AN EXAMINATION OF THE NIGERIAN CYBERCRIME BILL 2014

Adekola Tolulope Anthony LLB LLM BL

Department of Business Studies, Landmark University Omu Aran

Email-adekola.tolulope@lmu.edu.ng phone No- 07035843524

ABSTRACT

Nigeria recorded a milestone in October 2014, when the Cybercrime bill was passed by the Senate. The Bill will no doubt, speed up judicial processes on cyber criminality and as well boost e-Commerce activities in the country. It is an indisputable fact that a country without cyber laws is susceptible to all sorts of online attacks. The absence of cyber laws gives hackers the freedom to have unauthorized access to individual and corporate data banks and to steal or manipulate classified information. The perpetrators often get away with the crime in Nigeria, because there are no laws in place to prosecute offenders. Disturbed about the huge economic losses to cybercrime coupled with the dent on Nigeria's image in the international community and also the pressure from experts in the field of information and communications technology (ICT), the upper chambers of the Nigerian National Assembly has passed the cybercrime bill which will have the full force of law after the President signs same. In the light of this development, this paper will conduct an x-ray of the Cybercrime Bill with a view to preparing the minds of stakeholders in the ICT sector and the general public on the content of the proposed Law. This paper will also proffer necessary recommendations for the proper enforcement and implementation of the law.

Key words- Cybercrime, Cybersecurity, Law

AN OVERVIEW OF CYBERCRIME

Cybercrime refers to any crime that involves a computer and a network. The computer may have been used in the commission of the crime or it may be the target. Cybercrime has also been defined by Dr Debarati Halder and Dr K. Jaishankar (2011) as offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as internet (chat rooms , emails, notice boards and groups), and mobile phones(SMS/MMS).Such crimes may threaten nation's security and financial health. Issues surrounding these types of crime have become high- profile, particularly those surrounding cracking, copyright infringement, child pornography and child grooming. There are also problems of breaches of privacy, when confidential information is intercepted or disclosed lawfully or otherwise. Nigeria has the largest Internet population in Africa, estimated at about 56 million by Freedom House in Its 2013 Freedom on the Net report. 57.9% of the Internet traffic being via mobile phones and the latter is largely accountable for the surge in its penetration rate from 27% in 2011 to 33% in 2014. This buttresses the increasingly important role of the Internet across societal sector and the indispensible need for the provision of a legal

framework to wit -the Cyber Crime Bill 2014-for the prohibition and punishment of electronic fraud and cybercrime whilst promoting e-government services, electronic communications and transactions between public and private bodies as well as institutions and individuals.

ANTECEDENT AND OBJECTIVES OF THE CYBER CRIME BILL 2014

The plenary session of the Senate on Thursday, 23 October 2014 witnessed the passage into law of "A Bill for an Act to Provide for the Prohibition, Prevention, Detection, Response, Investigation and Prosecution of Cyber Crimes and for Other Related Matters, 2014". The passage of the bill was sequel to the presentation of Senate Committee on Judiciary, Human Rights and Legal Matters' Report on the Cyber Crime Bill referred to it for further legislative work by the Chamber. The Chairman of the Committee, Senator Umaru Dahiru, presented the report before the Senate for clause by clause consideration and passage. According to Sen. Dahiru, the bill seeks to provide a legal framework for the implementation and evaluation of response and preventive measures in the fight against Cyber Crime as well as other related frauds in line with international best practices. It also provides a legal framework for the prohibition and punishment of electronic fraud and cybercrime whilst promoting e-government services, electronic communications and transactions between public and private bodies as well as institutions and individuals. The bill seeks to criminalize certain acts and omissions in line with regional and international best practices and provide procedural guidelines for the investigation of such offences. The legislation also intends to define the liability of service providers and ensure that national interest of Nigeria is not compromised by the use of electronic communications. Sen. Dahiru noted that during the bill's public hearing, stakeholders and the general public made some important contributions to the bill which specifically seeks to secure computer equipment against unauthorized access and modification, as well as against misuse in the following areas: (1) Unauthorized access or modification of computer. (2) Unauthorized access with intent to commit or facilitate commission of further offences. (3) Unauthorized access to computer or misuse of electronic devices.

On receipt of the report, the Senate resolved into the Committee of the Whole and considered and approved clauses 1 to 48 with the exception of clauses 7, 13, 14, 28 and 39 which were deleted and substituted. Thereafter, the Chairman rendered progress report and the Senate Leader moved that the bill be read the third time and was seconded by the Senate Minority Leader. The Deputy Senate President, Ike Ekweremadu, who presided over the day's sitting put the question on the bill and it sailed through third reading and passed. Sen. Ekweremadu thereafter congratulated distinguished Senators for achieving a major landmark by passing the very important bill that not only seek to fight corruption to standstill but boost the image of the country within and outside it as well as reduce to the barest minimum the rate of cyber-crime in Nigeria.

PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

The Bill in its interpretation section defines "critical national information infrastructure" to include assets, systems and networks, whether physical or virtual, so vital to the security, defence or international relations of Nigeria; the provisions of service directly related to

communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure or the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services.
According to the Bill, the President may on the recommendation of the National Security Adviser, by Order published in the Federal Gazette, designate certain computer systems, networks and information infrastructure vital to the national security of Nigeria or the economic and social wellbeing of its citizens, as constituting Critical National Information Infrastructure.
The Presidential Order may also prescribe minimum standards, guidelines, rules or procedure in **respect of:**

(a) the protection or preservation of critical information infrastructure;
(b) the general management of critical information infrastructure;
(c) access to, transfer and control of data in any critical information infrastructure;
(d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any critical national information infrastructure;
(e) the storage or archiving of data or information regarded critical I national information infrastructure;
(f) recovery plans in the event of disaster or loss of the critical national information infrastructure or any part of it; and
(g) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.

Administration And Enforcement of the Cyber Crime bill 2014

The proposed Act provides that the National Security Adviser shall be the co-coordinating authority for all security and enforcement agencies under the Act and shall:

(a) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria;
(b) ensure the effective formulation and implementation of a comprehensive cyber security strategy for Nigeria; and
(c) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies.

Furthermore the Attorney - General of the Federation shall be the coordinating Minister for the effective implementation and administration of the proposed Act; and shall strengthen and enhance the existing legal framework to:

(a) ensure conformity of Nigeria's cybercrime and cybersecurity laws and policies with intemational standards and the African Union Conventions on Cybersecurity;
(b) maintain international co-operation required for preventing, combating cybercrimes and promoting cybersecurity;
(c) provide appropriate legal framework, guidelines and mechanism for the blocking of offensive or inappropriate web-sites; and
(d) ensure the effective prosecution of cybercrimes and cybersecurity matters.

Also all the law enforcement, security and intelligence agencies are to develop requisite institutional capacity for the effective implementation of the provisions of the proposed Act and also shall in collaboration with the National Security Adviser, initiate, develop or organize training programmes nationally or internationally for officers charged with the responsibility of the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

Establishment Of The Cybercrime Advisory Council

The passed bill establishes, a Cybercrime Advisory Council (referred to as "the Council") which shall comprise of a representative each of the Ministries and Agencies listed below:

1. Federal Ministry of Justice;
2. Federal Ministry of finance:
3. Ministry of Foreign Affairs;
4. **Federal Ministry** of Industry, **Trade and Investment:**
5. **Federal Ministry** of' Communicauon Technology:
6. Federal Ministry of Information;
7. Federal Ministry of Youth Development;
8. Federal Ministry of Science and Technology;
9. Central Bank of Nigeria,
10. National Broadcasting Commission,
11. National Security Adviser;
12. State Security Service;
13. Nigeria Police Force;
14. Economic and Financial Crimes Commission;
15. Independent Corrupt Practices Commission;
16. National intelligence Agency;
17. Nigerian Security and Civil Defence Corps;
18. Defence Intelligence Agency;
19. National Agency for the Prohibition of' Traffic in Persons;
20. Nigeria Customs Service;
21. Nigeria Immigration Service;
22. Nigerian Financial Intelligence Unit;
23. National Information Technology Development Agency; and
24. Nigerian Communications Commission.

The proposed bill states that a representative appointed shall be an officer not below the Directorate Cadre in the Public Service or its equivalent.

The Council has the duty to create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and will also provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria. The Bill provides that the Council will meet at least four times in a year and whenever it is convened by the National Security Adviser who presides over such meetings

Function of The Council

The Council by the provisions of the Bill has the following functions:

(a) formulate and provide general policy guidelines for the effective implementation of the provisions of the proposed Act; and.
(b) advice appropriate authorities on measures to prevent and combat computer related offences, cybercrirnes, threats to national cyberspace and other cyber security related issues.
(c) promote cyber security and the coordinate efforts to prohibit, prevent and combat cybercrimes in Nigeria;

(d) ensure the identification and inclusion of the critical national information infrastructure for protection and preservation;
(e) ensure the effective monitoring and control of the use of ICT against abuse; and
(f) do such other acts or things that are reasonably necessary for the effective implementation of the provisions of the Act**.**

The Council by the provisions of the proposed Act has the power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.

REVIEW OF OFFENCES AND PENALTIES

Offences Against Critical National Information Infrastructure

By the provisions of the Bill any person who commits any offence punishable under the Act against any critical national information infrastructure designated is liable on conviction to imprisonment for a term of not less than fifteen years without an option of fine.

Unlawful Access A Computer

A term of not less than two years or a fine of not less than N5,000,000 or to both fine and imprisonment is prescribed for any person, who without authorization or in excess of authorization, intentionally accesses in whole or in part, a computer system or network.

Unlawful Interception Of Communication

The Bill also prescribed that any person, who intentionally. and without authorization or in excess of authority: intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

Unauthorized Modification Of Computer Data

The Bill stipulates a term of not less than 3 years or a fine of not less than N7,000,000.00 or to both fine and imprisonment to anyone who directly or indirectly does an act without authority and with intent to cause an unauthorized modification of any data held in.any computer system or network.

Also the practice of engaging in the act of damaging, deletion, deteriorating, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a computer system by any person without authority or in excess of authority will attracts the punishment of a term not less than three years or an option of fine of not less than N7,000,000.00 or to both fine and imprisonment.

Unlawful Interception Of Communications

The relevant provision of the Bill on unlawful interception of communications stipulates that any person, who intentionally. and without authorization or in excess of authority: intercepts by technical means, transmissions of non-public computer data, content data or traffic data, including electromagnetic emissions or signals from a computer, computer system or network carrying or emitting signals, to or from a computer, computer system or connected system or network; commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both fine and imprisonment.

System Interference

The Bill prescribes that any person who without authority or in excess of authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference in the computer system, which prevents the computer system or any part thereof, from functioning in accordance with its intended purpose, commits an offence and liable on conviction to imprisonment for a term of not less than two years or to a fine of not less than N5,000,000.00 or to both tine and imprisonment.

Misuse of Device

On the misuse of device the Bill provides that any person, who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available:

(a) any devices, including a computer program or a component designed or adapted for the purpose of committing an offence;
(b) a computer password, access code or similar data by which the whole any part of a computer, computer system or network is capable of being accessed for the purpose of committing an offence; or
(c) any device designed primarily to overcome security measures in any computer, computer system or network with the intent that the devices be utilized for the purpose of violating any provision of the bill, commits an offence and should be liable on conviction to imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both imprisonment and fine.

Computer Related Forgery

A term of not less than three years imprisonment or to a fine of not less than N7, 000,000.00 is prescribed by the Bill against any person who knowingly accesses any computer or network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible.

Computer Related Fraud Identity Then And Impersonation

The Bill provides that any person who knowingly and without authority or in excess of authority causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any computer, whether or not for the purpose of conferring any economic benefits for himself or another person, commits an offence and is liable on conviction to imprisonment for a term **of** not less than three years or to a fine of not less than N7,000,000.00 or to both **fine and imprisonment.**

Identity And Theft Impersonation

The Bill provides that **any** person who in the course of using a computer, computer system or network:

(a) knowingly obtains or possesses another person's or entity's identity information with the intent to deceive or defraud; or

(b) fraudulently impersonates another entity or person, living or dead, with intent to:

(i) gain advantage for himself or another person;

(ii) obtain any property or an interest in any property;

(iii) cause disadvantage to the entity or person being impersonated or another person; or will be liable to an imprisonment for a term of not less than three years or a fine of not less than N7,000,000.00 or to both fine and imprisonment

Child Pornography

For the purpose of the Bill, the term "child pornography" is said to include pornographic material that visually depicts:

(a) a minor engaged in sexually explicit conduct;

(b) a person appearing to be a minor engaged in sexually explicit conduct; and

(c) realistic images representing a minor engaged in sexually explicit conduct.

Also the bill defines the term "child" or "minor" to mean a person below 18 years of age.

"Sexually explicit conduct" was provided to include at least the following real or simulated acts:

(a) sexual intercourse, including genital-genital, oral-genital, anal genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex;

(b) besliality;

(c) masturbation;
(d) sadistic or masochistic abuse in a sexual context: or
(e) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated; and

The Bill provides further that any person who intentionally uses any computer or network system in or for:

(a) producing child pornography for the purpose of its distribution;
(b) offering or making available child pornography;
(c) distributing or transmitting child pornography;
(d) procuring childpornography for oneself or for another person;
(e) possessing child pornography in a computer system or on a computer-data storage medium; commits an offence and is liable on conviction an imprisonment for a term of ten years or a fine of not less than N20,000,000.00 or to both fine and imprisonment.

Cyber Squatting

The Bill provides that any person who, intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Governments in Nigeria, on the internet or any other computer network, without authority or right, or for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence and is liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment.

Cyber Terrorism

Life imprisonment is the penalty for any person that accesses or causes to be accessed any computer or computer system or network for purposes of terrorism.

Racist, Gender And *Xenophobic*

The Bill, provides that anyone who distributes or otherwise makes available, any racist, gender or offences xenophobic material to the public through a computer system or network; and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ten million naira or to both fine and imprisonment.

Also anyone who distributes or otherwise makes available, through a computer system to the public, material which denies, approves or justifies acts constituting genocide or crimes against humanity, as defined under the Rome Statute of the International Criminal Court, 1998; commits an offence and shall be liable on conviction to imprisonment for a term of not less than five years or to a fine of not less than ten million naira or to both fine and imprisonment.

Corporate Liability

A body corporate that commits an offence under the proposed Act is to be liable on conviction to a fine of not less than N 10,000,000.00 and any person who at the time of the commission of

the offence was a chief executive officer, director, secretary, manager or other similar officer of the body corporate or was purporting to act in any such capacity shall be liable on conviction to imprisonment for a term of not less than two years or a fine of not less than N5,000,000.00 or to both fine and imprisonment;

Duties Of Service Providers

The Bill provides that a service provider shall keep all traffic data and subscriber information as may be prescribed by the relevant authority for the time being responsible for the regulation of communication services in Nigeria.

A service provider shall also, at the request of the relevant authority or any law enforcement agency: preserve, hold or retain any traffic data, subscriber information or related content, or release any information required to be kept.

Interception Of Electronic Communication

Where there are reasonable grounds to suspect that the content of any electronic communication is reasonably required for the purposes of a criminal investigation or proceedings, a Judge may on the basis of information on oath:

(a) order a service provider, through the application of technical means to collect, record, permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or

(b) authorize a law enforcement officer to collect or record such data through application of technical means.

Failure Of** Service **Provider To Perform Certain Duties

It is the duty of every service provider in Nigeria to comply with all the provisions of the proposed Act and disclose any information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding in the court of law.

The proposed Act also provides that a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards:

(a) the identification, apprehension and prosecution of offenders;

(b) the identification, tracking and tracing of proceeds of any offence **or any property, equipment** or device **used in the commission** of any **offence; or**

(c) the freezing, removal, erasure Of cancellation of the services of the offender which enables the offender to either commit the offence or hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

(3) Any service provider who contravenes the provisions of subsection (I) and (2) of this section, commits an offence and shall be liable on conviction to a fine of not less than N I0,000,000.00.

Jurisdiction of Court

The Federal High Court located in any part of Nigeria regardless of the location where the offence is committed or High Court of Federal Capital Territory shall have jurisdiction to try offences under this Act **committed:**

(a) in Nigeria;
(b) on a ship or aircraft registered in Nigeria; or
(c) by a Nigerian outside Nigeria if the person's conduct would also constitute an offence under a 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.

Also the Bill states that the Attorney-General of the Federation shall prosecute offences under the Act subject to the provisions of the Constitution of the Federal Republic of Nigeria, 1999.

THE CYBER CRIME BILL 2014 AFTER ITS PASSAGE BY THE SENATE

After the Senate has passed the Cybercrime Bill 2014 the next urgent step is for the lower Legislative Chamber, the House of Representatives, to concur to its passage, before the President of Nigeria will eventually sign it into law for proper implementation.

As at the time of revising this paper, the cybercrime bill had already been passed by both chambers of the National Assembly (NASS). However, there are fears that the bill may not be signed into law before the present dispensation of President Goodluck Jonathan's administration winds up.

Stakeholders had expressed concerns that if the bill is not signed into law during this present dispensation, the implication is that the entire process would start afresh by the time a new government is sworn in by May 29, 2015.

The good news is however that the next parliament can rely on the effort of the present National Assembly and ensure that the contents of the Cyber Crime Bill 2014 becomes a reality by passing same into law within a reasonable time in no distant time in the interest of the Nation.

CHALLENGES TO PROPER IMPLEMENTATION THE PROPOSED ACT

The Bill, when it eventually becomes Law, whether in the present democratic dispensation or the next, may become a pawn on the cheese board of the numerous law enforcement, intelligence and security agencies detailed to be members of the Council. This may bring about bureaucratic bottlenecks in the implementation of the provisions of the proposed Act.

The low awareness of the general public particularly users of the internet may hamper the progress and implementation of the provisions of the Act. Although ignorance of law is not an excuse, however, cybercrime having been encoded in the “DNA” of a large percentage of

Nigerian youths, the government will have to educate the public on the criminality of some conducts Nigerians may have seen a not criminal in the past.

Also, the private sector from the provision of the Bill was not represented in the Cybercrime advisory committee. It is important to note that the non-inclusion of Associations of service providers and ICT professional bodies may pose a great threat to the legitimacy and indeed the effective enforcement of the provisions of the bill

Lack of integration of public –private sector stakeholders in the process of the law making, due largely to distrust of government by the private sector, as well as sectored infighting may also be a great challenge the implementation of the Act will be confronted with.

While it is obvious that an effective cyber security environment is needed, the efforts must ensure legal compliance, technical competence and other required organizational measures, such as, capacity building and cooperation for it to be effective. It is only when this is done that proper growth can be achieved, and citizens' rights not threatened

CONCLUSION

This paper at best, leads to expansion of knowledge, the outcome of which is intended for direct practical application to existing problems or future problems in the cyber sector of Nigeria. As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. Nigeria is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world.

This paper calls on all – citizens, media, businesses and governments – who value Nigerian citizens' rights to use the Internet without fear and risk, to join in partnership and advocacy of ensuring that the Cybercrime Bill 2014 sees the light of the day be it in this democratic dispensation or that which is to come. Stakeholders in the ICT sector should plan a range of activities to improve awareness across the public, political and business spaces to mobilize pressure on the legislature and executive to fast-track the passage of the 'Cybercrime Bill, 2014'.

REFERENCES

Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

Warren G. Kruse, Jay G. Heiser (2002). *Computer forensics: incident response essentials*. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

T.G. George-Maria Tyendezwa (2014) Legislation On Cybercrime In Nigeria:Imperatives And Challenges

www.nassnig.org/nass/legislation.php?id=2064 *(cybercrime bill 2014)*

http://pinigeria.org

Adebusuyi, A. (2008): *The Internet and Emergence of Yahooboys sub-Culture in Nigeria,* International Journal Of Cyber-Criminology, 0794-2891, Vol.2(2) 368-381, July-December

Longe, O. B, Chiemeke, S. (2008): *Cyber Crime and Criminality In Nigeria – What Roles Are Internet Access Points In Playing?,* European *Journal Of Social Sciences – Volume 6, Number 4*

Major General G. G UMO (2010): *Cyber Threats: Implications For Nigeria's National Interest,*

Mohsin, A. (2006): *Cyber Crimes And Solutions*,

Okonigene, R. E., Adekanle, B. (2009): *Cybercrime In Nigeria,* Business Intelligence Journal,