CYBERCRIMES (PROHIBITION, PREVENTION, ETC) ACT, 2015 NEWSLETTER

27-08-15

The explanatory memorandum of the Nigerian Cybercrimes Act 2015 states in summary that the purpose of the act is to provide a comprehensive legal frameworkfor the promotion of cyber security, protection of computer systems, programs, and networks, electronic communications, data, intellectual property and privacy rights, the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria and protection of critical national information infrastructure.

Some of the offences in the Nigerian Cybercrimes' Act 2015 include; Unlawful Access

EDITOR'S NOTE

In this quarter's newsletter we critically review the recently enacted Cyber Crime Act 2015, which signed into law on the 15th of May, 2015.

The said Act has long been expected, and Nigerians are optimistic as to the positive effect it will have in mitigating cybercrime in the country.

Consequently the Information Security Society of Africa –Nigeria is set to hold a stakeholders conference to enlighten Nigerians on the Act.

One of its key features is its provision on prohibition of infrastructure attacks (for instance an assault on a nation's power grid), which inevitably affects the wellbeing of the nation, individually and collectively.

Unfortunately the practice in some parts of Nigeria has been the incessant vandalism of infrastructure, such as telecommunications mast, therefore the Act under part III, particularly in section 5(1), provides amongst other things, that any person who with intent commits any offense punishable under the Act against any critical national information infrastructure is liable on conviction to imprisonment for a term of not more than 10 years without option of a fine.

Section 5(2) provides in summary that where that offence committed under subsection 1 results in grievous bodily harm, the offender is liable on conviction to 15 years imprisonment without an option of a fine, and lastly section 5 (3) says where the result of committing the offence is death, the offender is liable on conviction to life imprisonment.

The Act describes "critical national information infrastructure" as certain designated computer systems, networks, programs and traffic computer data, the destruction of which would have a debilitating impact on national security, national public health and safety, or a combination of these.

Another notable provision is section 44 (2) (a) which in summary states that a levy of 0.005 of all electronic transactions by businesses specifies in the Second Schedule to the Act. Those businesses are GSM Service providers and all telecommunication companies, internet service providers, Banks and other Financial Institutions, Insurance Companies and Nigerian Stock Exchange.

The above and many other provisions which shall be reviewed below are the reason why it is the writer's view that this law though seemingly rushed, will bring the much needed positive change in cyber and computer interactions in Nigeria.

The writer has noted however that crime associated with mobile phone internet interactions seem to be omitted in the Act, it is hoped that future amendments to the Act will incorporate the issues that arise in the use of mobile phones for cyber interactions and crime. Do have a pleasant read.

to Computers, Unlawful Operation of Cybercafés, System Interference, Intercepting Electronic Messages, Emails, E-money Transfer, Tampering with Critical Infrastructure, Computer related Forgery, Theft of Electronic Devices and Electronic Signatures, Child Pornography, Racism, Willful Misdirection of Electronic Messages, Unlawful Interceptions, Cyber Terrorism, Fraudulent issuance of e-instructions, Cyberstalking, Cybersquatting, Identity Theft and Impersonation, Breach of Confidence by Service Providers, Phishing, Spamming, Spreading of Computer Virus, Manipulation of ATM, Electronic cards related fraudand Xenophobic Offences.

<u>REVIEW OF THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT, 2015</u>

The above mentioned Act is divided into 8 parts and 2 Schedules which are;

1. Object and Application
2. Protection of critical national information infrastructure
3. Offences and Penalties
4. Duties of Financial Institutions
5. Administration and Enforcement
6. Arrest, Search, Seizure and Protection
7. Jurisdiction and International Co-operation
8. Miscellaneous.

1st Schedule- Members of the Cyber Crime Advisory Council

2nd Schedule- Businesses referred to in section 44(2) (a).

The provisions of the Act apply throughout the federation of Nigeria.

Notable provisions include the following;

- Section 7(1) (a) (b) states in summary that from the commencement of the Act, all cyber café operators must register as a business concern with "Computer Professionals Registration Council" in addition to a business name registration with the Corporate Affairs Commission, and maintain a register of users through a sign in register, which shall be made available to law enforcement personnel when needed.

The above section will make it easy to track perpetrators of online fraud, as the register serves as a database of all persons who have used the internet service provided by the Internet Service Provider in question in any given cyber café.

- Section 7(2) (3) states that it is an offence to commit online fraud using a cyber café and makes the perpetrator liable on conviction to a fine of either 341,000,000.00 or a 3 years prison term or both, and if it is proven that there was connivance by the cyber café owners, the latter will be guilty of an offence and liable upon conviction to a fine of $42.000, 000, 00 or 3 year prison term.

It is noteworthy that there seems to be a typographical error, and therefore it would appear that what the drafts man intended has not been expressed. It is the writers submission that the fine intended for committing online fraud via a cyber café is N41,000,000.00 while connivance by a cyber café owner attracts a possible fine of N42, 000,000.00.

- Section 14 provides for the offence of computer related fraud, it states in summary, that a person who knowingly 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 on himself or another person commits an offence and on conviction liable to either a fine of not less than N7,000,000.00 or not less than a 3 year prison term or both, while anyone who with an intent to defraud sends an electronic message in

Members of the Cyber crime Advisory Council are representatives of the following Ministries, Agencies and Departments; Federal Ministry of Justice, Federal Ministry of Finance, Ministry of Foreign Affairs, Federal Ministry of Trade and Investment, Central Bank of Nigeria: Office of the National Security Adviser, Department of State Services, Nigeria Police Force, Economic and Financial Crimes Commission, Independent Corrupt Practices Commission, National Intelligence Agency, Defence Headquarters, National Agencyfor the Prohibition of Traffic in persons, Nigeria Customs Service, Nigeria Immigration Service, National Space Management Agency, Nigerian

which they materially misrepresent any fact, upon which reliance is made, thereby causing the recipient or another person to suffer any damage or loss commits an offence and liable upon conviction to either a fine of N10,000,000.00 or not less than a 5 year term or both.

The above provision is highly welcome and it is hoped that its enforcement will drastically reduce the incidence of Online Advanced Fee Fraud also known in Nigeria as '419' or 'yahoo yahoo'.

- Section 15 provides for the offence of theft of electronic devices, it states in summary that a person who steals the Infrastructure terminal owned by either the government or a financial institution is liable on conviction to either 3 years imprisonment or a N1, 000,000.00 fine or both. While one who steals an Automated Teller Machine (ATM) is liable on conviction to amongst others, either 7 years imprisonment or a fine of not more than N10, 000,000.00 or both.

It is worth noting that the above provision also makes it a criminal offence to "attempt" to steal an ATM, and such a thief is liable on conviction to 1 year imprisonment or a fine of not more than N1,000,000.00 or both.

- Section 17 provides that the Electronic Signatures used in respect to contracts for purchase of goods and services shall be binding generally except in the following contractual transactions; The creation and execution of wills, codicils and other testamentary documents, death certificate, birth certificate, family law matters such as marriage, divorce, adoption, and other related issues, issuance of court orders, affidavits, pleadings, motions, notices, and other judicial documents, any document issued by an empowered authority, ordering the withdrawal of drugs or other chemical on the grounds that they are expired, fake and dangerous to the environment or people.

The above provision shows the difficulty in the use of electronic signature across board in all transactions in Nigeria.

- Section 18 provides for the offence of Cyber Terrorism, and a person will be liable on conviction to life imprisonment.

- Section 22 provides for the offence of Identity Theft and Impersonation stating that a person who commits such offence will be liable on conviction to a 7 year imprisonment term or a N5, 000,000.00 fine or both.

- Section 23 provides for the offence of Child Pornography and other related offences, whose penalties range from 1 to 15 years imprisonment or fine ranging from N250, 000.00 to N25, 000,000.

- Sections 24 and 25 provide for the offence of Cyberstalking and Cybersquatting respectively stating that one is liable upon conviction to fine ranging from N7, 000,000.00 to N25, 000,000.00 in the case of the former, and a fine N5, 000,000.00 in the case of the latter or a prison term of 3 to 5 years in the former and 2 years in the latter or both penalty in each case.

Cyberstalking is described in the Act as when a person sends a message via computer that is grossly offensive, menacing, obscenely indecent, criminally

Information Technology Development Agency, Nigerian Communications Commission, Galaxy Backbone, National Identity Management Commission, Nigeria Prisons Service and One representative each from Association of Telecommunications Companies of Nigeria, Internet Service Providers Association of Nigeria, Nigeria Bankers Committee, Nigeria Insurance Association, Nigerian Stock Exchange and Non-Governmental Organization with focus on Cyber Security and any other Ministry, Department, Agency or

intimidating, or false with the aim of causing needless anxiety, insult, danger, obstruction, threat to kidnap/request for ransom/ kidnapping, hatred, harassment, bullying, violence, bodily harm or death.

While Cybersquatting is described in the Act as when a person intentionally makes use of a name, business name, trademark, domain name or any other word or phrase that is registered owned or in use by any individual , body corporate or belonging to either the federal, state or local government via the internet without authority for the purpose of interfering with their use by the owner, registrant or legitimate prior user, or for the purpose of obtaining compensation in any form for the release to the rightful owner the use of its name/business name/trademark/domain name.

- Section 26 provides for the offence of racism and Xenophobic offences, stating that one who distributes or makes available any racist or xenophobic material to the public via a computer network, or abuses or threatens others because they are of a certain race, ethnic origin, or religion, or distributes material that justifies genocide or crimes against humanity is liable on conviction to either 5 years imprisonment or a fine of not more than N10, 000,000.00 or both.

The above section is very relevant in the light of recent xenophobic acts carried out by some South Africans in South Africa against Nigerians. Since the Act gives the Federal High Court in Nigeria exclusive jurisdiction in a matter in which the victim is a citizen or resident of Nigeria, even though the offence has taken place outside Nigeria, the perpetrators can be extradited under the Extradition Act in other to ensure justice is done.

- Section 27 provides for the offence of attempting to commit an offence under the Act, Conspiracy, Aiding and Abetting in the commission of an offence under the Act. One is liable on conviction, as regards being an employee of a financial institution who commits fraud using a computer network, to not more than 7 years imprisonment and shall in addition, refund the stolen money, or forfeit any property to which it has been converted.

- Section 31 provides for the offence of manipulation of an ATM or Point of Sale (POS) terminal and provides that one is liable on conviction to 5 years imprisonment of a fine of N5, 000,000.00 or both. It states further that an employee of a financial institution who connives with others to perpetrate fraud using an ATM or POS terminal is liable on conviction to 7 years imprisonment without an option of a fine.

There appears to be two “section 31”, with the second providing for an “Employees Responsibility” upon disengagement from employment, in that whether he/she is working in the private or public sector, he /she must surrender all codes and access rights to his/her employer, refusal to relinquish and continuing to hold unto such access code without lawful reason will him/her liable on conviction to either a 3 year prison term or a fine of N1, 000,000.00 or both.

"Speedy resolution of legal issues is the hallmark of G.O Sodipo and Co"- Barrister B.V Enwesi,LL.B,BL,LL.M(E-commerce Law)

- Section 32 provides for the offence of Phishing, Spamming and Spreading of Computer Virus. Stating that a person who intentionally engages in any one of such acts is liable on conviction to a 3 year prison term or a fine of N1, 000,000.00 or both.
-

In the above provision, it would appear that subsection 1 refers to the offence of phishing, subsection 2 refers to Spamming, while the last subsection 3, refers to Spreading Computer Virus.

- Section 33 provides for the offence of **Electronic Cards Related Fraud**. It states that one who with an intent to defraud, uses a credit, debit or other type of financial card to obtain cash, credit, goods or service is liable on conviction to a prison term of not more than 7 years or a fine of not more than N5,000,000.00 or both. It further states that one who steals an electronic card is liable on conviction to a prison term of not more than 3 years or a fine of not more than N1, 000,000.00 in addition to being liable to repay in monetary terms the value of loss sustained by the true card owner or forfeit the goods acquired with the funds.

The above provision contains 16 subsections with fines varying from N5, 000,000.00 to N10, 000,000.00. Section 34 and 35 relate to card offences, with the latter specifically providing for the offence of the **Purchase or Sale of another's card**, stating that one would be liable on summary conviction to a fine of N500, 000.00 and to pay in monetary terms the value of loss sustained by the card owner or forfeit the goods acquired with the funds from the account of the true card owner.

- Section 36 provides for the offence of the use with an intent to defraud of any device, attachment, email or website to obtain the details of a card holder, stating that one who engages in such is liable on conviction to a 3 year prison term or a fine of N1, 000,000.00 or both. The same penalty is meted out in subsection 2, to one who fraudulently re-directs funds transfer instructions electronically during transmissions over an authorized communication path or device.

- Section 37 and 38 provide for the **duty of financial institutions**, stating in summary that they shall obtain personal details of their customers by applying the principle of 'Know your Customer", failure to do this will make such financial institution liable on conviction to a fine of N5, 000,000.00. In addition Section 38 provides for the duty of s service provider to retain records and protect traffic data for a period of 2 years, having due regard to the individual's **right to privacy** under the 1999 Constitution of the Federal Republic of Nigeria, contravention of this section's provision makes one liable on conviction to a prison term of not more than 3 years or a fine of not more than N7, 000,000.00 or both.

Section 37(3) is noteworthy as it states that a financial institution that makes an unauthorized debit on a customer's account shall upon a written notification by the customer provide clear legal authorization for such debit to the customer or reverse such debit within 72 hours, failure to reverse such debit within 72 hours results in liability upon conviction to restitution of the debit and a fine of N5, 000,000.00.

- Section 39 provides that where there is reasonable grounds to believe that the content of an electronic communication is required for criminal investigation or proceeding, a judge has the power to make an order, on the basis of information on oath, permitting a service provider to use technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data/traffic data associated with electronic communication, or communications transmitted by means of a computer system.

The above section appears to necessitate the procurement by either the service provider or other competent authorities, such as a law enforcement officer, of a court order prior to legal interception of an electronic communication.

- Section 40 provides for certain duties that must be carried out by service providers failure of which will make them liable on conviction to a fine of not more than N10, 000,000.00. The duties in summary are that a service provider shall either at the request of any law enforcement agency or on its own initiative provide assistance towards; the identification, apprehension, and prosecution of offenders; the identification, tracking and tracing of proceeds of any offence, or any property, equipment, or device used in the commission of any offence; freezing, removal, erasure or cancellation of the services of the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

Subsection 4 goes further to state that subject to section 20 of the Act, each Director, Manager or Officer of the service provider is liable on conviction to a prison term of not more than 3 years or a fine of not more than N7,000,000.00 or both.

- Section 41 provides for Administration, Co-ordination and Enforcement procedures to be carried out by the National Security Adviser and the Attorney- General of the Federation. It states that the office of the National Security Adviser shall be the coordinating body for all the security and enforcement agencies under the Act. It states it's duties to include; formulation and effective implementation of a comprehensive cyber security strategy and national cyber security policy; Establishing and maintaining a National Computer Emergency Response Team (CERT) Co-ordination Centre responsible for managing cyber incidences in Nigeria; Establish and maintain a National Computer Forensic laboratory and so-ordinate its utilization by all law enforcement, intelligence and security agencies; Establish appropriate platforms for public private partnership; Co-ordinate Nigeria's involvement in international cyber security co-operation to ensure Nigeria's integration into the global frameworks on Cyber Security.

  While the Attorney General of the Federation shall ensure conformity of the existing legal framework of Nigeria's cybercrime and cyber security laws and policies with regional and international standards; Effectively prosecute cybercrimes.

Subsection 3 of the above provision states that all law enforcement, security and intelligence agencies shall develop requisite institutional capacity by in collaboration with the National Security Adviser initiating, developing and organizing international and national training programs.

- Section 42 provides for the Establishment of the Cybercrime Advisory Council, whose members consist of a representative each of the ministries and agencies listed under the first schedule to the Act. Their meetings shall be presided over by the National Security Adviser, and they shall meet at least four times in a year. Section 43 provides for the functions of Cybercrime Advisory Council.

It is worthy to note that a member of the Cybercrime Advisory Council shall cease to be a member if the President of Nigeria is satisfied that it is not in the public interest for the person to be a member.

- Section 44 provides for the establishment of the National Cyber Security Fund, stating that it shall be domiciled in the Central Bank of Nigeria

- Section 45 provides for the power of arrest, search and seizure to be granted by a judge to a law enforcement officer upon an ex-parte application for the purpose of obtaining electronic evidence in relation to a criminal investigation.

- Section 46 provides that anyone who willfully obstructs any law enforcement officer in the exercise of his duty will be liable on conviction to 2 year prison term or a fine of not more than N500, 000.00 or both. While Section 47 provides that law enforcement agencies shall have power to prosecute under this Act, but must obtain the Attorney General's approval in the case of an offence provided for under section 19 and 21 of the Act

- Section 48 provides that a court may order that a convicted person forfeit to the Federal Government of Nigeria any proceeds of such offence, and such convicted person shall have his International passport cancelled and in the case of a foreigner his passport shall be withheld and only returned after he has served the sentence or paid the fines imposed on him.

- **Section 50** provides for **jurisdiction** and international co-operation, stating that the Federal High Court located in any part of Nigeria regardless of the location where the offence is committed shall have jurisdiction to try offences under this Act if the offence is committed in Nigeria, by a resident or citizen of Nigeria, in a ship or aircraft registered in Nigeria, the victim of the offence is a citizen or resident of Nigeria and if the alleged offender is in Nigeria and has not been extradited to another country for prosecution. In addition the Court shall give all matters brought before it by the Council accelerated hearing. Furthermore subject to the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of all criminal matters brought under this Act shall not be entertained until judgment is delivered.

- Section 51 provides for that offences under the Act shall be extraditable under the Extradition Act.

- Section 52 provides that the Attorney General may request for assistance from any agency of a foreign state in the investigation and prosecution of offences under the Act, whether or not any bilateral or multi-lateral agreement exists between Nigeria and the country to which the request is made.

- Section 53 provides for the procedure in authenticating evidence gathered pursuant to requests made under section 52, it states that all such evidence shall be authenticated by either ; certification by a judge, magistrate or notary public of the foreign state; sworn to under oath or affirmation of a witness or sealed with an official or public seal; or if it emanates from a ministry or department of the Government of the foreign state, or from a person administering the government of a foreign territory, protectorate, or colony.

- Section 56 provides that in order to provide immediate assistance for international co-operation, the office of the National Security Adviser shall maintain a contact point available 24 hours a day and 7 days a week.

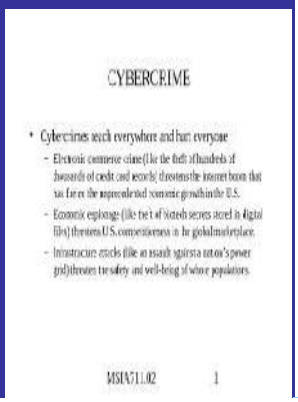
- Section 58 is the definition section.

In conclusion the above provisions are just a few of the salient provisions of the Act.

E-mail: b.sodipo@gosodipo.com

G.O SODIPO & CO
Tel: 08023198641

E-mail:b.sodipo@gosodipo.com
We're on the Web!
www.gosodipo.com



CYBERCRIME

- Cybercrimes seech everywhere and hurt everyone
  - Electronic commerce crime(Like the theft of hundreds of thousands of credit card records) threatens the internet boom that has fuelled the unprecedented economic growth in the U.S.
  - Economic espionage (like theft of Nateeh secrets stored in digital files) threatens U.S. competitiveness in the global marketplace.
  - Infrastructure attacks (like an assault against a nation's power grid) threaten the safety and well-being of whole populations.

MSIA711.02 1

G.O SODIPO & CO
Tel: 08023198641

We're on the Web!
www.gosodipo.com