Legal Alert – December 2013 – Cyber Security, Risks and Crimes

In this Issue:-

Introduction

Associated with the enormous benefits that the internet continues to bring to mankind, are numerous Risks which global governments are using legislation to ensure that public confidence in modern Commerce and Governance, over the internet, does not diminish, and or become ultimately eclipsed by criminal activities undertaken using the internet.

Escalating increments in economic crimes, some of which economic crimes are associated with terrorism, have brought about more urgency for cyber-security legislations and enforcement in Nigeria, as in other parts of the world.

What is Cyber Security?

Cyber security, which is more commonly referred to as cybercrime, has been described as the use of the internet to perpetuate, in time and space, the commission of criminal offences.

Some of the common cybercrimes, which are enumerated in the Nigerian Cybercrime Bill 2013, include:-

i. The unlawful access to a person's computer;
ii. The unlawful interference or interception with a computer system or network of systems, or with other electronic devices;
iii. The use of a computer or computer systems or networks to unlawfully produce, procure, distribute and promote child pornographic materials;
iv. The use of a computer, computer systems or networks to unlawfully impersonate and steal another person's identity;
v. Cyber-stalking – which is the unlawful, gross, offensive, menacing, indecent and or obscene use of a computer, computer systems or networks to annoy and inconvenience another person;
vi. Cyber-squatting – which is the intentional and unlawful acquisition and or use of another person's name, trademark, domain name or other word or phrase without that person's consent or authority;

vii. Cyber-terrorism – which is the unlawful use of a computer, computer systems or networks to promote any form of terrorism;
viii. Racist and xenophobic crimes – which entails the unlawful distribution of racist and xenophobic material using a computer, computer systems or networks.

Cyber Security Laws in Nigeria?

There is not presently in Nigeria, any Act of Parliament regulating cyber security or cybercrimes. This is despite several Bills on the subject, before the Nigerian National Assembly, awaiting enactment into Law.

It is therefore recommended that we consider the existing Laws that relate to cyber security or cybercrimes before considering at least one of the numerous Bills before the Nigerian National Assembly on the subject – i.e. the Cyber Security Bill, 2013, which is the most recent Executive Bill on the subject.

Criminal Code Act – Obtaining By False Pretences

Presently, the most common legislation for prosecuting cybercrimes in many of the Southern States of Nigeria are as stated in Sections 419, 419A, 419B, 420, 421, 422, and 423 of the Criminal Code Act.

The above-mentioned Sections of the Criminal Code Act provide in summary that where any person, by false pretence, and with the intent to defraud another person, obtains from that other person anything capable of being stolen, or advises any other person to deliver to any other person anything capable of being stolen, or obtains credit by false pretences or by some other kind of fraud, commits an offence and is liable on conviction to imprisonment for a term of three (3) years. Where the item concerned is of a value of ₦1000 (One Thousand Naira) or upwards, the term of imprisonment on conviction is seven (7) years.

The above statutory provisions and punishments also apply to cases of obtaining the execution of a security document by false pretences; cheating and conspiracy to defraud another person by deceit or other fraudulent means, etc are also criminal offences which carry fines and terms of imprisonment.

Advance Fee Fraud & Other Fraud Related Offences Act, 2006.

The Advance Fee Fraud & Other Fraud Related Offences Act, CAP A6, Laws of the Federation of Nigeria literally extended the felonious provisions of the Criminal Code Act, on false pretences,

to now include any person who by false pretence, and with the intent to defraud, obtains from any other person, whether in Nigeria or in any other country; or induces any other person in Nigeria or in any other country, to deliver to any person, any property, whether or not the property or its delivery is induced through the medium of a contract, which contract was itself induced by false pretence.

The penalty on conviction for committing any of the above false pretences offences is imprisonment for a term of not less than seven (7) years without the option of a fine, or imprisonment for a term of not more than twenty (20) years.

Other fraud related offences under this Law include:-

(a) Representing oneself as possessing the power of doubling or otherwise increasing any sum of money through any unorthodox method or methods, like currency colouration.

(b) Fraudulent invitation of a non-Nigerian to Nigeria under false pretences.

(c) Possession of fraudulent documents to commit a false pretence offence.

(d) Laundering of funds obtained through unlawful false pretences activity or activities.

Data Services Customers Registration.

As part of the global efforts to enhance cyber security, the Advance Fee Fraud and other Fraud Related Offences Act, provides in its Part II, Sections 12 and 13, the statutory mandatory requirement for all telecommunication companies in Nigeria to obtain from all their subscribers or customers, especially their data services subscribers or customers, the full names, residential or corporate copies of utility bills, certificates of incorporation or registration, etc of these subscribers or customers.

All telecommunications, internet and internet cafe service providers are also required to, in addition to registering their businesses with the Economic and Financial Crimes Commission ("EFCC"), maintain a register of all telecommunication lines in their networks. These service providers are further statutorily required to submit on demand to EFCC, such data and information as are necessary or expedient for giving full effect to the performance of the functions of EFCC under the Advance Fee Fraud and other Fraud Related Offences Act.

The failure by any customer or subscriber to any telecommunication service to register, or where the customer or subscriber registers with the intent to deceive, or supplies false

information, or conceals or disguises such false information, constitutes an offence which on conviction carries a term of imprisonment of not less than three (3) years or a fine of ₦100,000.

Economic and Financial Crimes Commission Act, 2004.

The Economic and Financial Crimes Commission (Establishment, ETC.) Act. CAP E1, Laws of the Federation of Nigeria 2004 ("EFCC Act") is the legislation which preceded the Advance Fee Fraud and other Fraud Related Offences Act, 2006.

The EFCC Act describes an economic or a financial crime to be the non-violent and illicit activity committed with the objective of earning wealth illegally.

Some of the economic and financial crimes mentioned in the EFCC Act include any kind of fraud, drug trafficking, money laundering, embezzlement, bribery, looting and other corrupt practices, tax evasion, foreign exchange malpractices, theft of intellectual property and piracy, etc.

It is also an offence under the EFCC Act for any person to retain, conceal or remove from Nigeria the proceeds of any economic or financial crime; or to engage in the acquisition, possession or use of any property acquired from any economic or financial criminal activity.

It is equally a criminal offence for any person to engage in the concealment or disguising of the true nature, source, location, disposition, movement or rights to a property acquired through an economic or financial criminal activity.

The penalties for the various economic and financial crimes enumerated in the EFCC Act include terms of imprisonment for different number of years for each class of economic or financial offence; fines equivalent to 100 per cent of the value of the proceeds of the economic or financial crime; in addition to the forfeiture of such proceeds to the Federal Government of Nigeria; life imprisonment where the economic or financial crime is meant to aid, facilitate or participate in a terrorist activity; obtaining from a competent Court of record an order freezing the Bank accounts of a suspected economic or financial crime infringer.

Budapest International Convention on Cybercrime.

In the international platform, there is a Convention on Cybercrime, which is more commonly referred to as the Budapest Convention on Cybercrime. This is the first International Treaty that seeks to address internet and computer related crimes, by harmonising the legislations of signatory nations on cybercrimes, thereby

enhancing cooperation in the investigation and prosecution of such cybercrimes among nations.

Some of the criminalised cyber offences enumerated in the Budapest Convention on Cybercrimes include illegal access, illegal interception, data interference, system interference, misuse of computer and other internet devices, computer-related forgery, computer-related fraud, offences related to child pornography, copyright and neighbourhood rights.

There is no record that Nigeria has ratified this International Convention on Cybercrime. Some of the countries that have however ratified this Convention include the members of the European Union, the United States of America, Canada, Japan, the Republic of South Africa, Australia, the Dominican Republic, Mauritius, among other countries.

An additional Protocol to the Budapest Convention on Cybercrimes criminalised the publication of racist and xenophobic literature over the internet. Undergoing further review is the inclusion of cyber terrorism in the Budapest Convention on Cybercrime.

Nigerian Cybercrime Bill, 2013.

Numerous Bills on cybercrime prevention in Nigeria have remained unpassed by successive sessions of the Nigerian National Assembly. This is due in part to the lack of coordinated efforts by various interest groups presenting separate Cybercrime Bills to the Nigerian National Assembly; instead of a harmonised Cybercrime Bill.

Another reason for the non-passage of any Cybercrime legislation in Nigeria has been that no session of the National Assembly has been able to consider for passage any of the Cybercrime Bills before the tenure of that National Assembly elapsed, with the new Assembly considering all such Bills *de novo* – i.e. afresh.

Despite the above developments, one of the core objectives of the Cybercrime Bill, 2013 is the provision of "….. an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.

Some of the offences under this Bill include any unlawful access to any computer; any unauthorised modification of a computer data, which is also known as data forgery; any computer system interference; any misuse of any computer devices; any computer related fraud; any identity theft and impersonation; any child pornography and related offences; any cyber stalking, cyber terrorism, racist and xenophobic offences, attempt, conspiracy,

aiding and abetting in cybercrimes, etc. Penalties and fines apply for any commission of any of these cybercrimes.

Cybercrime Bill and International Cooperation

As Cybercrimes have no territorial boundaries, the Nigerian Cybercrime Bill 2013, like the previous Bills before it, has proposed that all offences under this legislation shall be extraditable offences under the Extradition Act, Cap. E25, Laws of the Federation of Nigeria, 2004.

Other areas of international cooperation, among different countries, on the matter of cybercrimes, include requests for mutual assistance in the singular or joint investigation or prosecution of cybercrimes, whether or not Nigeria has signed a bilateral or multilateral agreement on cybercrime prevention, investigation and prosecution with such country or countries from whom cybercrime prevention assistance is requested.

Conclusion

The existence of a very weak cybercrime prevention and enforcement structure in a country like Nigeria, with an estimated population of more than one hundred and fifty million people, most of whom are adolescents and juveniles, portends a clear and present danger to the structural and economic development of Nigeria, and the global economy.

While there is no enacted cybercrime specific legislation in Nigeria, the above-mentioned Laws criminalising obtaining any property under false pretences should serve as a start-off point for the successful prosecution of cybercrimes. Unfortunately, private and public sector corruption have changed dramatically the value structure which celebrates ill-gotten wealth with the result that cybercrime prosecution is in turn inhibited.

Multiplicity and under-funding of the numerous law enforcement and security agencies have not assisted in the prevention and prosecution of cybercrimes and other white collar crimes in Nigeria.

Equally inhibiting the prevention and prosecution of cybercrimes has been a weak and grossly underfunded judicial system.

Despite the above challenges, continuing enlightenment on the criminality and harm that cybercrimes cause to the development of any country will greatly assist Nigeria and other countries of the world in overcoming the menace of cybercrimes'.

DISCLAIMER NOTICE. This Legal Alert is a free educational material, for your general information and enlightenment

purpose ONLY. This Alert, by itself, does not create a Client/Attorney relationship between yourself and our Law Firm. Recipients are therefore advised to seek professional legal advice and counselling to their specific situations when they do arise.

COPYRIGHT NOTICE. This Legal Alert is protected by International Intellectual Property Law and Regulations. It may however be shared with other parties provided that our Authorship is always acknowledged and this Disclaimer Notice is attached.