Comparative Study of Cybercrime Laws in Nigeria and China

(The Constraining Dynamics)[19]

Florence U Masajuwa

ABSTRACT

Cybercrime is a growing threat to security of life, property and transactions generally. The threat posed by cybercrime arises from the fact that criminals and fraudsters have realised the huge potentials of cyberspace and have consequently, replicated their nefarious activities in the physical world in ways that are unique to the cyberspace. To check aberrations arising from use of the cyberspace for criminal purposes, United Nations (UN) and various countries have made legislations to forestall criminal acts in the internet. It's against this foregoing background that this paper comparatively, appraised legal constraints that may hinder efforts with implementing principal laws enacted to curb cybercrimes in Nigeria and China. From an analysing primary secondary data, this paper identified the constraints as jurisdiction matters, law enforcement, applicable laws, issue of evidence, courts and human rights concerns among others. Findings of this paper indicate that these constraints are real. However, the level of success in addressing the constraints varies in the two countries under consideration. As a developing country whose cybercrime law was only enacted in 2015, Nigeria has not acquired solid experience in the application of its cybercrime law. This is unlike China, a developed economy whose principal cybercrime law not only dates back to 1957 but is robust and has been tested. Among the recommendations is that all cadres of personnel that will administer cybercrime laws be trained to be computer, information and communication technology literate especially in Nigeria.

Kew words: Constraints, cybercrime, law, 419 Scam, Advance Fee Fraud.

INTRODUCTION

The Nigerian government's reaction to cybercrime took a great turn when former President Goodluck Jonathan in May 2015, enacted a *Cybercrime (Prevention, Prohibition etc.) Act.* (Kumolu, 2015). Before, there were no specific laws for computer crimes. Laws relied upon were the *Criminal Code Act*, *Economic and Financial Crimes Commission Act 2004*, *Advance Fee Fraud and other Fraud Related Offences Act 2006* (Chawki, 2009). On the other hand, the main law regulating the cyber space in China is the *Regulation for the protection, security and Management of All Computer Information Networks*. The People's Republic of China (PRC) promulgated this regulation on December 30, 1957 for the protection, security and management of all computer information networks. Thus, *China's Computer Law* pre-dated the commission of computer-related crimes. This is because computer-related crimes emerged in China in mid-1980s and was punished according to provisions of the previously existing

legal framework (Li, 2015). However, specific regulation on cybercrime started in 1994 when the State Council promulgated the *Ordinance on Security Protection of Computer Information System* (State Council Decree No. 147, 1994), (Li, 2015).

From legal perspective, this paper found issues that may hinder application of cybercrime laws to include issues of jurisdiction, law enforcement, applicable laws, issue of evidence, courts and human rights concerns. This paper therefore sets out to examine these issues. The main objective of this paper is to appraise the nature and propensity of each of these challenges in a developing economy like Nigeria and a developed economy like China. The method of the paper is analytical legal research. An analytical research method involves analysis of both legal and other texts, statutes, delegated legislation, cases and so on (Jackson, 2003). Data were from primary (Focused group discussion) and secondary sources. The FGD had 8 discussants, consisting of two lawyers, four identified yahoo-yahoo undergraduates, one academic in computer science and a victim of cybercrime.

APPRAISAL OF CONSTRAINING DYNAMICS

Law enforcement in the Cyber-Space

It is evident that cybercrime has come to stay (Li, 2015). It is "big business" for the criminal entrepreneur with potentiality of making lots of money with minimal risks. At the same time the main areas which the FGD recognised as the contributory elements hindering law enforcement officers from prosecuting cybercrime offences include:

- Lack of up-to-date guidelines
- Lack of proper training
- Lack of funding

This finding is corroborated by Jahankhani & Amin Hosseinian-far, (2014) whom in their own study, found that law enforcement officers find it difficult to identify and apprehend cyber criminals. This may be due to the fact that perpetrators can use technology to conceal their identities and physical location, thereby frustrating law enforcement efforts to locate them (Chawki & Wahab, 2006). The traditional model of law enforcement assumes that the commission of an offence involves physical proximity between perpetrator and victim (Brenner, 2004, p.6). This assumption has shaped approaches to criminal investigation and prosecution (Oriola, 2005). Real-world criminal investigations focus on the crime scene as the best way to identify a perpetrator and link him to the crime. However, in automated or cybercrime there may either be no crime scene or there may be many crime scenes, with shredded evidence of the crime scattered throughout cyberspace (Chawki, 2009). In this respect Dana van der Merwe (2008, p.104) argues that:

"The true problem of the information and communication era seems to be to decide exactly how much value should be attached to a given piece of information, especially when that information is stored electronically and digitally. The only field of law which advertises itself as a specialist in the area of verifying facts is the law of evidence. Unfortunately, like all other fields of law this field sometimes finds itself struggling to adapt to a new world in which paper is being phased out of general commercial transactions and to decreasing contact between human beings and the information needed to conduct business."

Accordingly, identifying an electronic crime scene can be a daunting task when the perpetrator may have routed his communications with the victim through computers in three or four countries, with obscure networks that are inaccessible to investigators (Conn, 2002). To this end, the reactive model of law enforcement does not deal effectively with cybercrime because it is fluid and distributed in nature. Thus, as a lateral, pervasive phenomenon, cybercrime requires a lateral, pervasive solution. This solution must be proactive; that is, it must focus on preventing cybercrime because, as explained above, reacting to completed crimes is not a practicable means of dealing with cybercrime. The solution must also involve a collaborative approach that combines the efforts of civilians and law enforcement in order to address the fact that it is neither financially nor pragmatically possible to deploy enough officers to maintain order in cyberspace. A practical way to address cybercrime is to utilise the community policing model's concept of a proactive, collaborative approach to preventing crime (Vanguard, 2017).

It needs be noted that "communities" in cyberspace tend to be defined by interests, not by territory (Kollock & Smith, 1998). In the real-world, community policing succeeds because the civilians who participate want to ensure the security of the neighborhood in which they live. Before colonialism, most villages and towns in Nigeria had community police that maintained law and order in the communities. Colonial government jettisoned the community police and in its place, formed what is now known as Nigerian Police. Due to increasing crime in the society, especially during this democratic government, the idea of community police was re-visited. Thus, in recent times, community police are called vigilante group (Arase, 2013). Community policing has no special name in China, but then, the policing in China is essentially community policing (Zhong, 2009). In the cyber-world, the members of these interest-based "communities" may not be concerned about cybercrime because they lack the central, binding focus that a physical neighborhood provides. Considering the interests and communications that give rise to these communities, many of the participants may prefer the risk of cybercrime to the prospect of a law enforcement presence in their midst.

In real world investigations, a set of interrogative pronouns, commonly known in the law enforcement field as the "5× WH + H" method—Who, What, When, Where, Why + How are often be put to good use" (Cook & Tattersall, 2010). This formula helps to organise the investigative information and to identify where there are knowledge gaps. For a cybercrime investigation this may look as follows: (Staniforth in Akhgar et al p.35)

• Who is the victim? – Victim details and why this victim?

• What happened? – Precise details on incident/occurrence

• When did it happen? – Chronological issues such as relevant times

• Where did it happen? – Geographic locations, national/international?

• Why did it happen? – Motivation for crime or terrorism

• How did it happen? – Precise modus operandi details

This information can then be developed into a useful investigative matrix which will help identify the gaps in information by setting out all the relevant details in a logical sequence which is easily understood. The snag however is that the matrix must be a living document, being regularly updated as the investigation progresses.

PRINCIPLES OF EVIDENCE AND THE CYBER-SPACE

The laws of evidence are certain established principles for production of evidence before courts of law. In a civil or criminal trial, a situation arises between the parties when they raise claim and counter-claim about the existence of a fact or facts. In such situation, the rule of evidence comes into play so as to enable the judge arrive at a rational conclusion about existence or non-existence of disputed fact or facts. The principles of the laws of evidence by and large are the same both for civil and criminal trials. Added to this is the fact that the definition of the term "proof" in the Nigerian Evidence Act does not make any distinction between civil and criminal. There is however, difference in impact a piece of evidence will make in civil or criminal matter (FGD, Lawyer). This difference in impact was succinctly explained in a decided Indian case *Emperor v. Janki.* (Singh, 2007)

In civil cases, there are two parties, plaintiff and defendant, who put forward their cases and try to prove them by adducing evidences. The court is bound by the law to decide the case one way or the other. It gives findings in favour of the party whose evidence is more probable. But this does not happen in a criminal trial. In a criminal trial there is no question of two parties proving their cases. In a criminal trial, the prosecution is one and the only party and it has to prove its case and that too beyond a reasonable doubt. In criminal cases no weight of preponderance of evidence is sufficient.

In civil cases, both have to prove their cases by placing their evidence before the court. If a party fails to prove his case, he would lose. In criminal trial it is the duty of the prosecution to bring all the evidence before the court to prove the charge and the opposite party, as a measure of defence, has to create just doubt in the prosecution evidences (ibid). Investigation of cybercrime is thus constrained by the type of evidence acceptable. Stephen Mason (2010, p.25) proffered an all- embracing definition of electronic evidence to cover both civil and criminal proceedings. According to him, electronic evidence is:

"Data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence."

This definition of Mason has three identifiable elements that highlight the nature of electronic evidence (Akhihiero, 2013). Firstly, it covers all forms of evidence that are created, manipulated or stored in a device that can be classified as a computer. Secondly, it aims to include the various forms of devices by which data can be stored or transmitted. This aspect is wide enough to include devices such as mobile phones, digital cameras, video recorders, ATM machines, satellite devices, car tracking devices etc. The third element involves the process of adjudication in the court. This part of the definition relates to the aspect of relevance and admissibility of the evidence.

The use and importance of digital evidence in judicial proceeding have increased tremendously due to rapid growth in the field of computer and internet in everyday transactions. Thus where real evidence is not available, admission of digital evidence becomes a veritable alternative (Singh, 2007).

Evidence in cybercrime is very peculiar and thus raises a challenge which arises from the difficult faced by a law officer investigating a cybercrime with regards to discovering and collecting evidences of crimes committed against, or by means of electronic devices. This is because the culprit can easily delete a file in a computer thereby making the data not available to any investigator for evidence. Unlike crimes that take place in the physical world, there may not be any tangible evidence available such as weapon, paper, records, etc. (Adams, 1996). But technically it is very difficult to remove the materials completely from the computer. This is because modern computer forensic scientists are now capable of restoring the evidences even after it was intentionally deleted (Singh, 2007).

The evidence concerning cybercrimes may be physical or logical. The media and the hardware components which contain the data are in the category of physical evidence. This physical side of computer forensic involves the process of search and seizure of computer evidences. On the other hand, the logical side of computer forensic deals with the extraction of raw data from the relevant source of information. The search operation is done by investigator through log files, searching the internet, retrieving data from a database, etc. (Odumesi, 2014). Understanding the evidences involved in cybercrimes is a matter of experience and expertise. This expertise and experience is very much used in China (Wang, 2008). This is however, lacking in Nigeria due to the very low level of computer literacy among most law enforcement officers (Odumesi, 2014).

How to preserve cybercrime evidence is another real challenge in the effort to curb cybercrimes. This is because the process of procuring and storing evidence of cybercrimes is a delicate and precise process. Improper or careless handling of cybercrime evidence may

result to destruction of the evidence. For example, the collection of finger prints after robbery or murder has taken place. (Martie, 2015).

The normal practice in the case of a cybercrime is that the computer forensic experts and criminal investigators conduct the recovery process by gathering of evidences and restore normal operation through a relatively smooth exercise. If computer forensic or trained investigator evidences entailed physically removing of the victim's computer by investigators so as to retrieve evidences preserved in the victim's hardware system for investigation (Martie, 2015). This is still the level police and other detectives in Nigeria operate. Most times, police detectives either in plain clothes or uniform accost passer- bys, especially young men carrying computer bags on their back and seek to see the contents of the bag. They often seize the computers and mobile phones of the young men and compel them to follow them (that is, the police detectives) to their police station. At the stations, the seized computers or mobile phones are searched by the police for any incriminating evidence (Daily Post, 2014).

According to FGD (one of the Yahoo-yahoo boys) "Where incriminating evidence is found, the police hardly retrieve the evidence and return the computer or phone to the owner. They often "detain" the computer or phone for 'further investigations'." "Even where nothing incriminating is found in the seized electronic gadgets, the police also hardly return them to their owner. They also "detain" them until the owner "bail" his seized gadget! This is often a ploy to get the owner of the computer or mobile hand set to pay some bribe. The amount paid is determined by the sophistication or newness of the seized gadget and in some cases, the status of the owner" (Vanguard, 2017; Adeniran, 2008, p. 327).

The Nigerian scenario notwithstanding, the current trend is for the investigator to simply copy the evidence they need without disruption of person's or organisation's systems. No need to remove the compute at all. In China, the expertise has been properly developed. Services like electricity supply are constantly available to power the compromised computer while investigation or effort to retrieve evidence is continuing. The reverse is however, the case in Nigeria where electricity supply is primitively epileptic or out rightly unavailable. There is also the issue of corruption to contend with in Nigeria. There have been instances where officials assigned to investigate cybercrimes like the advanced fee fraud or 419 or yahoo-yahoo "runs" or "soft work" took bribes and allowed the cases to die natural death. (Adeniran, 2008, p.374). In China, the corruption attracts dire consequence including death penalty (Time in China, from www.timeinc.net, accessed 8th July, 2017).

ISSUE OF JURISDICTION

This has to do with the long-established view of jurisdiction and the new idea of Cyber-Jurisdiction. The expansiveness of the Internet, its borderlessness and easy reach has made it imperative that a new definition of the concept of statehood and sovereignty in terms of territoriality be redefined. A "state" consists of three features: territory, population and state authority or sovereignty (Shaw, 2003). A required condition is the presence of government

(Oppeinheim, 2006). That is its independence from any external authorities or forces: in other words, its sovereignty (Kelsen, 2002).

One may point to a wide range of indicators of state sovereignty. The most representative and uncontroversial are the exclusiveness of power over state territory and citizens, execution of foreign policy, the ability to make decisions or engaging in war or keeping peace, free recognition of states and governments, decisions concerning the creation of diplomatic relations and participation in military alliances and international organizations (Hinsely, 1986). Sovereignty therefore manifests itself in a number of activities performed by states at international level under competence vested by international law.

When analysing the jurisdictional of states, it should be noted that the something that is of interest to a state may not necessarily be within the said state but may be "physically" located outside the territory of the state, for instance, trust territories, individuals or persons. (Rosenn, 2001). The legitimacy of a state exercising laws with respect to events occurring abroad yet seriously affecting its territory is in no doubt. One of the first instances of acknowledging the jurisdictional powers of a state over events outside its territory is the resolution of the International Law Institute (ILI) which in 1879, stipulated the right of states to sanction acts committed outside their respective territories such as instances of breach of their criminal regulations by foreigners. This a state can do insofar as such acts pose a threat to the existence of a state and are not penalised under the laws of the state in which they were committed (Hall, 1904).

These state jurisdictional principles were confronted at the end of 1990s with a hail of claims resulting from inter-state interactions performed via the Internet. The first basic challenge that this brings however, is that of jurisdiction (Fraser, 2014). Cottim (2010, p.5) has identified five jurisdictional theories and approaches in this context, namely:-

1. Territoriality theory: The theory that jurisdiction is determined by the place where the offence is committed, in whole or in part. This "territoriality theory" has its roots in the Westphalia's Peace model of state sovereignty that has been in place since 1684 (Beaulac, 2004). This approach predicated on the presumption that the State has sovereignty over the territory under discussion, a presumption that is manifestly and easily rebuttable in most "cyberspace" cases.

2. Nationality (or active personality) theory: This is based primarily on the nationality of the person who committed the offence. In United *States of America v Jay Cohen* (2d Cir. July 31, 2001),World Sports Exchange, together with its President, were defendants in an FBI prosecution for conspiracy to use communications facilities to transmit wagers in interstate or foreign commerce. The defendants were charged with targeting customers in the United States inviting them to place bets with the company by toll-free telephone call or over the Internet. While the Antiguan Company was

beyond the jurisdiction of the court, the President was a US citizen and could, therefore, be brought before an American criminal court.

3. Passive personality theory: While the "nationality theory" deals with the nationality of the offender, the "passive personality theory" is concerned with the nationality of the victim. In what Cottim calls "the field of cybercriminology," a good example of this jurisdiction assumption can be seen in a case where a Russian citizen who lived in Chelyabinsk, Russia was sentenced by a court in Hartford Connecticut for hacking into computers in the United States.

4. Protective theory: Cottim's (2010) "protective theory" (also called "security principle" and "injured forum theory") deals with the national or international interest injured, assigning jurisdiction to the State that sees its interest—whether national or international—in jeopardy because of an offensive action. Cottim (2010) sees this rarely used theory as applying principally to crimes like counterfeiting of money and securities.

5. Universality theory: In his final theory, Cottim (2010) identifies the approach of universality based on the international character of the offence allowing (unlike the others) every State to claim of jurisdiction over offences, even if those offences have no direct effect on the asserting State. While this theory seems to have the most potential for applicability to cyberspace, there are two key constraints in the way it has been developed thus far. The first constraint is that the State assuming jurisdiction must have the defendant in custody; the second is that the crime is "particularly offensive to the international community." While this approach according to Cottim (2010) has been used for piracy and slave trafficking there is considerable practical difficulty in defining the parameters of the universality approach even in a conventional context and the possibility of extending it to cover cyberspace offences and activity is yet to beexplored (Fraser, 2014, p.4).

The first decisions pertaining to inter-state relations based on electronic contacts were issued in the second half of the 1990s. They were characterised by extreme discrepancies in the interpretation of inter-state jurisdictional principles. Many judges decided to apply the simplest analogy, disregarding the special, global nature of the medium they had to face (Kulesza, 2012). They decided to exercise their jurisdictional powers only if the effects of actions taken outside the state were noticeable within its territory. Most often the judges invoked the personal jurisdiction resulting from actions of the entity which is that the defendant, when producing effects within the forum territory, should have been aware of the responsibility he or she would bear within its area (ibid). The effects principle was also applied to criminal cases.

In the case *United States* v. *Thomas*, (1996) which involved an operator of e-bulletin distributing, *inter alia*, to Tennessee, pornographic materials forbidden therein, the Sixth District Court held that "the effects of the Defendants' criminal conduct reached the Western

District of Tennessee, and that district was suitable for accurate fact-finding" (ibid). Similarly, in the first international case concerning trademark infringement online, *Playboy Enterprises, Inc.* v. *Chuckleberry Publishing, Inc (2012)* the New York court recognised its jurisdiction to hear the case based on the availability of services provided online in the US directly from Italy, yet it also consciously held that:

"The Internet is a world-wide phenomenon, accessible from every corner of the globe. [The defendant] cannot be prohibited from operating its Internet site merely because the site is accessible from within one country in which its product is banned. To hold otherwise 'would be tantamount to a declaration that this Court, and every other court throughout the world, may assert jurisdiction overall information providers on the global World Wide Web" (Kulesza, 2012).

Wherever it is, constitutional lawyers around the world have contended with the possibility applying their countries' legislation to the virtual world of the Internet. In effect, the application of "analog" territorial laws to the extensive digital boundaries of the vast global communications network is, it seems, a big challenge to mankind's conventional legal systems. When it comes to interpreting and applying law across administrative jurisdictional boundaries, an established body of internationally agreed principles, behavior, and jurisprudence has developed over time. Some attempts have been made to apply these legal norms to cyberspace. For example, the International Covenant on Civil and Political Rights sets out some key obligations of signatory states (Gibbons, 1997).

MANIFESTATIONS OF JURISDICTIONAL CHALLENGE

Spammers and other online scammers currently ignore national borders, sending solicitations emails to potential victims in a host of countries. The transnational nature of cybercrime challenges traditional conceptualisations of criminal jurisdictions because conduct no longer necessarily occurs entirely within a territory of a single sovereign. A cybercriminal operating out of the US can attack victims in a host of countries-USA, Nigeria, Japan, China and so on with equal ease. Thus cyberspace and computer technology make geographical location irrelevant. This has several consequences for criminal jurisdiction (Brenner, 2007). Among the consequences are:

1. Jurisdiction may be completely lacking that is, non-existent.
2. Jurisdiction may exist but be impossible to assert. For example, Chinese law may not frown at the offence but Nigerian law could, so that Nigeria may wish to prosecute but China will not agree to turn in the criminal.

Jurisdiction means a government's general power to exercise authority over persons and things (Black's Law Dictionary, 2004). This general power encompasses 3 distinct concepts: jurisdiction to prescribe, jurisdiction to adjudicate and jurisdiction to enforce (American Law, Reinstatement, 1987). Jurisdiction may be claimed simultaneously by more than one country.

This would mean for example, Nigeria, China or Ghana etc. assert jurisdiction to prosecute the hypothesised cybercriminal. Here the problem is one of establishing priorities, of deciding which country should be given the first opportunity to prosecute him, which should be given the next chance etc.

The principles that govern a sovereign exercise of jurisdiction to prohibit conduct and to sanction those who violate such prohibitions are well established as to conduct occurring in real physical world. These principles evolved over the last several millennia, as law increased in sophistication and life become more complex. A physical world crime is almost exclusively a local phenomenon; the perpetrator and victims are all physically present at a specific geographical point when a crime is committed. This is therefore predicated on the assumption that 'crime' is a territorial phenomenon. Cybercrime makes these principles problematic in varying ways and varying degrees. Unlike real world crimes, it is not physically grounded; cybercrime increasingly tends not to occur in a single sovereign territory.

A cybercriminal's attack may physically occur in country 'A' while victim is in country B, C or D etc. The perpetrators may further complicate matters by routing his attacks on victims in country B through computers in countries F and G. The result of these and other cybercrimes scenario is that the cyber is not committed in the territory of a single sovereign state. Instead, 'pieces' of the cybercrime occur in a territory claimed by several different sovereigns (Brenner, 2007). In Nigeria, internet fraudsters in their continued quest to carry out their illegal transactions incognito, constantly upgrade their style of operations using the anonymity of transactions in the cyber space. (Ajayi, 2015). For example, they now by register email addresses with an **internet protocol (IP)** that indicate that they are resident in another country or location entirely different from their exact location. With this email, they send fraudulent messages or business ideas to unsuspecting individuals mostly outside their real country or location of domicile. Corroborating the assertion above, a participant in an eight-member focused group discussion (FGD) organised to generate primary data for this paper said:

"To be able to change your location, you will need to install an application called CYBER GHOST or ZENMATE. Once it is installed, you can log into the application and choose any country of your choice then the IP Address and location of your system will automatically change so that your exact location cannot be tracked by the anti-cybercrime authorities."

They also open social media accounts with the illicit e-mail address and add or become friends on platforms like Face Book. Another FGD, a "yahoo-yahoo" or "soft work" unemployed graduate explained to me extensively on their modus operandi. According to him, they don't use their real photographs as profile pictures on the social media accounts. Instead they use those of nationals of other countries, preferably whites, Asians or black Americans. Where the profile picture and name used is female, the yahoo-yahoo young man explained, their target victims are males and vice versa (http://www.telegraph.co.uk, Accessed Saturday, 30 September, 2017).

Sometimes, they use pictures of prominent personalities like presidents, ministers, legislators, governors etc. In this instance, their target victims are the friends of the important dignity whose picture and name he is flaunting. They stalk on the friends and engage them in chats as soon as these friends come online. They also use other devices to hack into bank accounts (https://www.youtube.com/watch?v=1y6TAuulbR0. Accessed, Saturday, 9 September, 2017).

As soon as any of their numerous social media accounts "hammers" that is such account has been used successfully to swindle a victim, such account is quickly deactivated and the victim will no longer see his or her "chat" mate any longer! The soft workers or yahoo boys also have different mobile lines and use these lines to send sms messages to unsuspecting members of the public. The commonest of these scam sms are those purporting to have been sent by the bankers of the targeted victim of the yahoo scam to the effect that the bank accounts of the victim with the said bank have some problems. The scammer then provides online links for the victim to click on to "rectify" the so-called identified anomaly in his account. If the unsuspecting victim clicks the supplied link, he or she often clicks away all his money in that account to that of the yahoo-yahoo scammer! (Thisdaylive, Available at https://www.thisdaylive.com (Accessed Saturday, September 30, 2017). A female participant in the FGD recounted her personal experience which was also reported in some local newspapers in Nigeria. According to her she received a message that had the following content:

"Dear Customer, According to our records this month, your registration for our Guaranteed Trust Customer Digest monthly bulletin has been processed and this comes with a monthly charge of N11, 450:00. "As your opinion is important to us, we would like you to confirm your registration through this link:
https://ibank.gtbank.com/ibank3/confirm_customer_digest_monthly_bulletin/

If you wish to reject the registration request, follow the cancel reference below:
https://ibank.gtbank.com/ibank3/cancel_customer_digest_monthly_bulletin_request/

"NOTE: If you do not respond within 12 hours of this notice, you would receive a successful debit alert on your account confirming your registration. You would have to confirm you are an active account holder with us by following the procedures from your GTBank Internet banking account. Thank you for choosing Guaranty Trust Bank plc." at https://www.thisdaylive.com (Accessed Saturday, September 30, 2017)

These scammers also operate in China. But unlike Nigeria, China easily detects change in strategy of cyber scammers and have the resources and facilities to deters them before they do monumental harms in the society (Hu, Li. Et al., 2013). In Nigeria, fraudsters and even kidnappers keep several mobile lines and use these devices regularly to send sms or make calls to defraud their numerous victims without detection by the law enforcement bodies or even the mobile network provider (Daily Trust Newspaper, Oct 26 2015. Available at

https://www.dailytrust.com.ng/news/general/mtn-fined-n1-4tr-over-unregistered-users/116634.html, Accessed, Saturday, 30 September, 2017)

This position was corroborated by some participants in the focused group discussion (FGD). According to them,

"We often buy many lines from the network providers. In fact, they specifically produce some lines for people engaged in yahoo-yahoo deals. We pay very high amount of money to get these special lines. We don't register the lines. Even with the heavy fine Federal Government imposed on one of the major network providers has not stopped them from selling special lines to us." (FGD, 12 July, 2017, Benin-City)

Scenarios like the above have created situations whereby lawyers to internet scammers exploit the jurisdictional differences to reduce the level of the sanction or the extent of their liability of their clients. An example in the United States (US) is Klemis *v Government of the United States of America* [2013, All ER (D) 287) where the UK defendant allegedly sold heroin to two men in Illinois, USA. One of the men subsequently died and raised questions at the point of sentencing as to how the different legislatures in the two jurisdictions had set the requirements for the relevant actus reus (criminal act) and the mens rea (culpable state of mind) differently.

Another example of trans-jurisdictional friction is *Bloy and Anor v Motor Insurers' Bureau* (2013, EWCA, Civ1543). In this case, a road traffic collision in the, United Kingdom had been caused by a Lithuanian national who had been uninsured at the time. The Motor Insurers' Bureau is the UK compensation body for the purposes of the relevant EU Directive and was obliged to pay compensation where a UK resident had been injured in a collision in another Member State caused by an uninsured driver. In such cases, the Directive enabled the Bureau to claim reimbursement from the respective compensatory body in the other Member State. However, under the domestic law of Lithuania the liability of the compensatory body was capped at €500 k. The Bureau argued that its liability to pay the victim should be capped by Lithuanian domestic law even though the collision happened on an English road (Fraser, 2014).

CHOICE OF LAW

Arising from the contentious issue of jurisdiction in cybercrime is the choice of law to apply in disputes arising from crimes committed over the internet. International law, or more specifically public international law, is the body of law that governs interactions among nations. The study of the law of foreign countries is not international law but comparative law. The international nature of the Internet makes both international law and comparative law important (Schwabach, 2005).

International law is either conventional (law made by treaties and other international agreements) or customary (normative expectations based on state practice undertaken out of a sense of legal obligation). The difficulty associated with determining the laws that should apply in the trial of a cybercrime was explained by Akomolade (2008, p.87) as follows: "The question of choice of law is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data and geographically dispersed processing activities, several connecting factors could occur in a computer involving elements of legal novelty."

"There are still more difficulties with regulation of cyberspace by the laws of a single jurisdiction. It is not just that national law is difficult to apply and enforce given the inherently transnational nature of the internet. It is also sometimes impossible to discern what country's laws would be most appropriately applied" (Edwards &Waelde, 1997).

Once a court has the jurisdiction to hear a case, in the absence of a choice of law by the parties to the dispute, the next step is for the court to determine which law will govern the dispute. When a contract has a foreign factor, the laws of several different countries may all be related to the contract or dispute.

COMPUTER INFORMATION COMMUNICATION AND TECHNOLOGY (ICT) KNOWLEDGE CONCERNS.

Cybercrime is crime that is carried out mainly through the computers and ICT. For anyone to circumvent the use of computers for nefarious ends, that person must be highly literate in computer and ICT. It suffices to say that those who will pursue and apply necessary laws in the prosecution of cybercriminals must also be proficient in computer and ICT knowledge. This is hardly the case, especially in Nigeria. There is no serious effort to evolve a national computer literacy policy. Thus, many schools- primary, secondary and even tertiary institutions do not have computers. Schools that teach computers at all teach only the theory and not the practical because such schools have no computers (Mabayoje, Isah, Bajeh, & Oyekunle, 2016).

Law enforcement officials who will apply the cybercrime laws are recruited from graduates of schools where computers are taught poorly or not taught at all. Consequently, these officials get onto their jobs lacking even basic knowledge of the main tools of their jobs. The opposite is the case with cybercriminals. Cybercriminals are computer and ICT savvy. They also have money to keep reinventing their knowledge of the computer and ICT (Ajayi, 2016). This difference in computer and ICT knowledge between law enforcement officials and cyber scammers is a challenge to the application of cybercrime law. This situation is more perverse in Nigeria than in China.

HUMAN RIGHTS AND PROTECTION OF PRIVACY CONCERNS

The form the human rights protection system should take is one of the most controversial issues in contemporary public international law. The roots of this controversy lie in cultural diversity among nations resulting from their social, historical and political backgrounds (Olomojobi, 2016). The development of an age of borderless cyberspace and the popularity of the internet that now reaches over one-third of the world population prove that a global consensus among cultures and policies on the limits of human rights is indispensable (Kulesza, 2012). Methods used by states to enforce national laws on freedom of speech or protect state secrets, for example, are no longer there for their nation only. This fact is reflected directly in the human rights debate and raises serious questions about the shape and scope of a global human rights catalogue fit for the twenty-first century.

Freedom of speech online is one of the most pressing issues that need to be resolved at international level. Since there is no strict global standard for free speech (Kulesza, 2012) initially states attempted to regulate electronic content available within their borders by enforcing their national laws with traditional judicial means. The current approach to regulating electronic content is filtering. Since practically no state allows freedom of speech to be exercised without any limitations, state authorities attempt to exercise their legislative restrictions also over online forms of expression. Therefore, most of them perform some sort of censorship "internet filtering" for different social, political or security reasons (Open initiative, 2005), which results in limiting access. The record of countries violating the right to free speech through filtering presented by OpenNetInitiative includes over 40 entries (ibid: 46).However, next to the filtering policies that clearly violate the present human rights standards of free speech by excessively restricting access to certain content are those forms of filtering that leave much more room for controversy. The scope of internet censorship is growing not only in countries recognised as autocratic, but also in model democracies (Ndionewese, *Techpoint,* available at www.techpoint.ng, accessed June 26, 2017). One could mention filtering done in libraries or schools for the protection of morality or child rights (Article *3,UN Convention on Rights of the Child, 1990*). The common national practice in Europe allowing local ISPs to block sites with child-pornography for example, might be recognised as one of such actions (Deiberte, 2010).

When discussing freedom of Internet access, human rights organisations oppose on-line censorship (Freedom House Country Report: Nigeria, 2017). At the same time state authorities propose the opposite opinion, attempting to protect their communities, both on and offline. However, blocking of electronic content is rarely initiated directly by law makers or executive authorities (Kumolu, 2015), even though, as an exception, it may also be carried out by a judicial decision.

In democratic states blocking content is a voluntary activity by the Internet service providers (ISPs) (Kulesza, 2012). Even in China, which is famous for its restrictive policy on the freedom of speech online, the burden of responsibilities, and what follows, the selection of methods and manner of restricting the access to specific content, rests with Internet service

providers, though the legal obligation to control content is stipulated by both statutes and extra-legal "codes of conduct" (Kulesza, 2012; Li, 2015).

PRTOECTION OF THE RIGHT TO PRIVACY AND NIGERIAN CYBERCRIME ACT

The *Cybercrimes (Prevention, Prohibition etc.) Act 2015* (hereinafter to be referred to as *the Act*), is a commendable development in Nigeria's legal and commercial jurisprudence. To start with, one of the many objectives of the Act is to confer on the Nigerian Communications Commission (NCC) (the regulatory body with respect to the communications sector) and security agencies the unrestricted powers to intrude into private communications of Nigerians such as telephone calls, email messages and such other electronic exchange of information like short messaging service (SMS) and multimedia applications with a view to enhancing national security, preventing crime and facilitating criminal investigations. It is pertinent to state here that provisions of the Act mandating the Nigerian Communications Commission as the relevant authority to authorise the service provider to keep certain subscriber information and then make disclosure when required, raises a whole lot of concerns and issues in respect of the human rights of individuals especially the right to privacy (Ojo, 2015).

In order to have a clearer understanding of relationship between the Act and the privacy concerns of the people, this paper, like Ojo did in a previous study (Ojo, 2015) asked the following questions: whether the emergence of the Act will mean that the private correspondence of all persons would be intruded upon without legal implications? Does it mean that the security agencies will have the licence to interfere with the privacy of an individual in the course of investigations? Does it mean that no private information and details shared by an individual with a social network can remain confidential? Does it indicate that no hitherto confidential information is really confidential in the real sense of the word? Does it imply that the right to privacy guaranteed under the Nigerian Constitution 1999 (as amended) could be reasonably trampled upon in reasonable circumstances as provided in this Act under consideration?

Like I argued elsewhere in the this paper, police simply confiscate the computer or mobile handset of a person they suspect as having incriminating data in his or her system. Most times they do this without any search warrant. The network providers claim to have registered all their subscribers, yet individuals buy and use unregistered lines to make calls that violate the cybercrime law (Premium Time, 8 March, 2016, available at https://www.premiumtimesng.com, accessed 18 September, 2017). This act by the police violates the 1999 Constitution.

The *1999 Constitution of the Federal Republic of Nigeria (as amended)* has sufficient provisions in relation to the privacy of citizens and *section 37* thereof states that "the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic

communications is hereby guaranteed and protected." After the enactment of the Cybercrime Act in 2015, the police now hinge their act of confiscating and searching of peoples electronic gadgets on section 38 (1) of the Act. According to that section of the Act, law enforcement officials have power to monitor electronic communications. It further empowers the officials to carry out lawful interception on suspected electronic communications. This is notwithstanding the fact that the Act in question under Section 38 (5) provides for the right to privacy. Thus, the Act enjoins anyone exercising any function under this section to have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria. It further provides that appropriate measures must be taken to safeguard the confidentiality of the data retained, processed, or retrieved for the purpose of law enforcement.

This paper submits that these provisions are contradictory and violate the provisions of the Constitution regarding protection of citizen's privacy. The Black's Law Dictionary (1990) defines the right to privacy as: "right to be let alone; the right of a person to be free from unwarranted publicity; and the right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned. "Protection of privacy entails prevention of governmental interference in intimate personal relationships or activities, freedoms of individuals to make fundamental choices involving himself, his family, and his relationship with others." (FGD, Lawyer).

The provisions of the Act allows for the retention by internet network providers of subscriber information, interception of electronic communications and then disclosure of such to the government or law enforcement agencies. Disclosure of such information will no doubt amount to a breach on the privacy policy and confidentiality agreement. This paper further submits that this provision enhances criminality as service providers in Nigeria hide under this provision to allow kidnappers and yahoo -yahoo boys to make calls to their victims without detection (Premium Time, available at https://www.premiumtimesng.com, Accessed 30, September, 2017)

We proposed that proper balance be struck between the rights of persons to be protected from undue interference with their private communications and the interest of the government to protect people from grossly offensive communication and forestall perceived breach of security. The right of privacy of persons is a sacrosanct right entrenched in the 1999 Constitution. However, it is subject to the constitutional restriction and reasonable derogation clause contained under section 45 of the 1999 Constitution (as amended). Section 45 of the 1999 constitution states that:
"Nothing in sections 37, 38, 39, 40 and 41 of this Constitution shall invalidate any law that is reasonably justifiable in a democratic society:

(a) In the interest of defence, public safety, public order, public morality or public health; or
(b) For the purpose of protecting the rights and freedoms of other persons".

Unlike the Nigeria Cybercrime Act which permits mobile network providers to reveal communication records of subscribers when requested by security agents, China's cybercrime law *Regulation for the protection, security and management of All Computer information Networks 1957 as amended*, provided for the protection of privacy and freedom of computer network users without giving network providers the freedom to reveal communication records of subscribers (Wang, 2008). No individual or unit may, therefore, use the internet to violate the freedom and privacy of network users in violation of these regulations. This was the position of the law before China opened its economy for investors from outside to come in. In a recent civil case, *Ms Zhu Ye v. Baidu*, the Chinese court ruled that the use of cookies by internet service providers, and accordingly delivering targeted advertising, does not violate the right of privacy of Chinese citizens. This court judgment has been read by the press as a judgment in favour of the 'new economy.' The evolving efforts at protecting privacy rights in the cyber space were further explained by Dong (2016, p.92) thus:

'The Tort Liability Law, which became effective 1 July 2010, includes many provisions that specifically or generally relate to the protection of personal data, and in particular, in Article 2, defines the 'civil rights and interests' protected under the Law, specifically listing 18 types of right and including the right of privacy. This is the first time under PRC law that the right of privacy has been treated as an independent type of civil right, and no longer attached to the right of reputation. Under the Tort Liability Law, the violation of the right of privacy and other personal and property rights and interests is clearly provided as constituting a tort. An injured party can seek redress against such an injuring party."

Under a new cyber-security law enacted in 2016, network providers are mandated to protect subscriber's personal information in the custody of the network providers. For example, network operators may not disclose, tamper with, or damage citizens' personal information that they have collected, and they are obligated to delete unlawfully collected information and to amend incorrect information. Moreover, they may not provide citizens' personal information to others without consent. Irrespective of the time and space in China's economic evolution, its goals against online activities regarded as harmful, are more targeted at maintaining state security than anything else (Covington 2016).

CONCLUSION

Nigeria and China have surfeits of laws to regulate misuse of the cyber space generally. This paper examined factors that constrain the application of cybercrime laws in Nigeria and China. The essence was to appraise the magnitude of these factors in the fight against cybercrimes in a developing economy and a developed economy. Factors identified were issue of jurisdiction, choice of law, issue of evidence and human rights concerns from the perspective of privacy of citizens. The effects of each of the factors varied in the two countries studied. There is poor level of computer and ICT knowledge by security personnel who constitutionally have the mandate to apply the cybercrime law. This is more prevalent in Nigeria than China. In Nigeria, the security officials are recruited from the populace. Majority

of the citizens are not computer literate. It follows that many of the security personnel recruited are also not computer literate. These officials are put through series of in-house computer and ICT training so as to equip them for their duties. This is different from the situation in China; where the officials at recruitment are already computer literate. Early exposure of its citizens to computer and ICT education is a state education policy in China. This is not so in Nigeria, though there is a national computer education policy. In line with the national computer education policy, many primary and secondary schools in Nigeria have a subject titled 'computer studies' in their curriculum, the teaching and learning is however, more theoretical than practical. This is because of absence of computer pcs in these schools.

Cyber criminals keep coming up with sophisticated methods of using the computers and the ICT to execute their nefarious activities, but same cannot be said about security officials whose knowledge and dexterity in the use of computers often lag behind, especially in Nigeria. Overcoming the identified challenges in the use of cybercrime laws to tackle cybercrimes entails not only equipping officials charged with applying the laws with both knowledge and materials to keep them ahead of cybercriminals, but also a profound political will on the part of the government.

RECOMMENDATIONS

Government at all levels especially in Nigeria should make computer literacy mandatory for all Nigerians. This should be done in phases. Recruitment of enforcement officers and other officials who administer laws like cybercrime Act should be based on computer and ICT literacy. Rule of evidence should be harmonised. International community should design a framework specifying the standard.

Mobile Network providers should balance business interests with overall need for security of life and property. Calls by subscribers like those made by kidnappers to relations of victims in the kidnapper's custody must be quickly intercepted or frustrated. This can be done by redirecting such calls to the police or other law enforcement agencies, telling them exactly the location and spot where the calls are being made from.

Lawyers appearing for anyone accused of engaging in cybercrime should eschew hammering on technicalities. Overriding public interest should guide such trials. Quick trial and dispensing of cybercrimes by the courts will strengthen transactions in the cyberspace as well as protect transactions in the cyber space.

References

Adams, J.M. (1996). Controlling cyberspace: Applying the Computer Fraud and Abuse Act to the Internet. *Santa Clara Computer and High Technology Law Journal, 12*, 403–434. Available at http://www.lexis-nexis.com. (Accessed October 27, 2015, 5pm).

Adeniran, A. I. (2008). The internet and emergence of yahoo-boys sub-culture in Nigeria. *International Journal of Cyber Criminology 2, (2),* 368-381.

Akhihiero, P.A. (2013). Admissibility of electronic evidence in criminal trials: How practicable?
A paper presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State Branch held on Tuesday, 23rd of July, 2013.

Akomolede, T.I. (2008). Contemporary legal issues in electronic commerce in Nigeria. *Potchefstroomse Elektroniese Regsblad 11 (3*), 80-100

American Law Institute. (1987). Restatement of Foreign Relations Law of the United States, *Section 401*

Beech, H. (2016). This is how much money you can take in bribes before Chinese Authorities execute you. Time. Available at www.timeinc.net. (Accessed, Saturday, July 8, 2017)

Black's Law Dictionary, "Jurisdiction."(8th edition, 2004).

Brenner, S. (2004). Cybercrime metrics: Old wine, new bottles. *Virginia Journal of Law and Technology, 9*, 13-13

Brenner, S.W. (2007). *Cybercrime jurisdiction.* London: Springer Publishers.

Charles Kumolu, (2015, December 9). Social Media Bill: Before the fatal blow is unleashed. *The Vanguard*,

Chawki, M & Wahab M. (2006).Identity theft in cyberspace: Issues and solutions. *Lex Electronica. 11* (1), 1-41

Chawki, M. (2009). Nigeria tackles advance fee fraud. *Journal of Information, Law and Technology*, 1(1), 1–20.

Conn, K. (2002). *The Internet and the law: what educators need to know*? (Alexandria, Virginia:
Association for Supervision and Curriculum Development, ASCD.

Cook, T & Tattersall, A. (2010). *Blackstone's senior investigating officers' handbook*, (2nd ed.).Oxford, UK: Oxford University Press.

Cottim, A. (2010). Cybercrime, cyber- terrorism and jurisdiction: An analysis of article 22 of the COE convention on cybercrime. *Eur. J. Leg. Stud. 2 (3*), 1-10.

Covington. (2016). China Passes New Cybersecurity Law. Available at https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf . (Accessed Saturday, September 30, 2017)

Deibert, R. J, Palfrey, J.G, Rohozinski, R & Zittrain, J. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace.* Cambridge, Mass.: MIT Press.

Dong, M. (2016). China's privacy, data protection and cybersecurity law: Overview. *The Privacy Data protection and Cybersecurity Law Review*. Edition 3, 89-99

Edwards L. (1997). Introduction to the law and internet. In Edwards L and Waelde C (Ed) *Law and the Internet*. Oxford: Hart Publishing.

Egbe, R. (2017). Three docked for defrauding Lagos speaker of N9.1m. The *Nation Newspaper.*

Fraser, S. (2014). Cyberspace: The new frontier for policing? In Babak Akhgar Andrew Staniforth and Francesca Bosco. (eds.). *Cybercrime and cyber terrorism: Investigator's handbook (p.1-10).* Oxford: Syngress Publisher.

Freedom House, *Freedom on the net: Country Report: Nigeria*. Available at www.freedomhouse.org. (Accessed Monday, June 26, 2017, 5 am)

Hall, W.E. (1904). *A treatise on international law*. Oxford, UK: Oxford University Press.

Hu, Y; Li, C.T; Wang, Y and Liu, B. (2015).An improved fingerprinting algorithm for detection
of video frame duplicating forgery.International Law. *291 Recueil des Cours*.

Jahankhani, H, & Hosseinian-far, A. (2014). Digital forensics education, training and awareness.

In Akhgar, B, Staniforth, A & Bosco, F (Eds.), *Cyber crime and cyber Terrorism: Investigator's handbook (p.91-100.)* Oxford, UK: Syngress.

Kelsen, H. (2002). *Principles of international law.* New Jersey: The Law book Exchange, Ltd.

Hinsley, F.H. (1986). *Sovereignty*, (2nd ed.). (London: Cambridge University Press.

Kobrin, S. J. (2001). Territoriality and the governance of cyberspace. *Journal of International Business Studies*, *32*(4), 687-704.

Kollock, P. &. Smith, M.A (1998). Communities in cyberspace.In Marc A. Smith & Peter Kollock, (Ed.) *Communities in Cyberspace*, 3-28

Kulesza, J. (2012). *International internet law*. New York, NY: USA: Rutledge.

Li, C. T. (Ed.). (2015). *Emerging digital forensics applications for crime detection, prevention, and security*. Hershy, PA: IGI Global Publishers.

Li, X. (2015). Regulation of cyber space: An analysis of Chinese law on cyber crime. *International Journal of Cyber Criminology*, *9*(2), 185-204

Mabayoje, M. A., Isah, A., Bajeh, A. O., & Oyekunle, R. A. (2016). An Assessment of ICT Literacy among Secondary School Students in a Rural Area of Kwara State, Nigeria: A Community Advocacy Approach. *Covenant Journal of Informatics and Communication Technology*, *3*(1), 40-59.

Martie, G. (2015).The need for digital evidence standardization. In Li, C. T. (Ed.). *Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security*. (Hershy, PA: IGI Global Publishers.

Mason, S & Seng D. (2016). *Electronic Evidence*, (3rd ed.). London: Lexis Nexis, Butterworths.

Ndioewese, I. (2017). *Censorship and social media: Resolving the dilemma between dictatorship and anarchy, Techpoint.* Available at www.techpoint.ng. (Accessed, M onday, June 26, 2017)

Ojo, O. V. (2015). *An x-ray of the Nigeria cybercrimes act 2015 vis-à-vis right of privacy in Nigeria.* Lagos, Nigeria: Lagos State University Press. Available at: https://works.bepress.com/oluwaseun_ojo/8/. 30 July, 2015.

Oppenheim, L. (2006). *International law: A treatise*. New Jersey, NY: The Law book Exchange, Ltd.

Oriola, T. (2005). Advance fee fraud on the Internet: Nigeria's regulatory response. *Computer Law and Security Review*, 21(3), 237-248

Schwabach, A. (2005). *Internet and the Law: Technology, Society, and Compromises*. Santa Barbara, CA: ABC-CLIO, Inc.

Shaw, M. N. (2003). *International law.* (5th ed.). Cambridge: Cambridge University Press.

Singh, P.Kr (2007). *Laws on Cyber Crimes: Along with IT, ICT and relevant Rules.* (Jaipur India: Book Enclave). Book Enclave. Available at www.enclavepublishing.com.

Staniforth, A. (2014). Police investigation processes: practical tools and techniques for tackling cybercrimes. in Akhgar, B; Andrew Staniforth, A and Bosco F. (eds.), *Cyber Crime and Cyber Terrorism: Investigator's Handbook* (Oxford: Syngress, 2014), 31-41.Thisdaylive, "Customers Raise the Alarm on 'GTBank' Scam Emails." Available at https://www.thisdaylive.com (Accessed Saturday, September 30, 2017)

Van der Merwe, D & Roos. (2008). A T Pistorius, en S. Eiselen. *Information and Communications Technology Law*, (Durban, South Africa: LexisNexis)

Vanguard, Osibanjo, eminent Nigerians canvas new policing system at Arase's book Launch. Available at www.vanguardngr.com (Accessed Thursday, July 6, 2017, 10 am)

Wang, M. (2008). Electronic evidence in China. *Digital evidence and electronic signature law review*, 5, 45. (Available at www.deaesir.org/Google scholar. accessed on Wednesday, July 5, 2017)

Zhong Y. L. (2009). Community policing in China: Old wine in new bottles. *Police practice and research*, 10 (2), 157-169.