Jurisdictional Issues in Electronic Banking

Adeola A. Oluwabiyi*

Abstract
Globally Banks have changed their mode of transacting financial business in a bid to align with the current developments in banking practices. Banking transactions are gradually going paperless and electronic banking has become the order of the day. The central bank of Nigeria and other global financial controlling bodies have been responding to this new trend of development which is not without its challenges. The aim of this paper is to look critically into issues on jurisdiction which is one of the challenging areas in electronic banking and make relevant recommendations.

Keywords: *Legal Issues, Internet Jurisdiction, Electronic Banking*

Introduction

In the examination of cyber banking problems, a fundamental aspect poses serious difficulties. That is the problem of jurisdiction. The nature of the Internet is such that geographical and political boundaries are rendered irrelevant. A person with access to a computer and the Internet might be participating, attempting or planning a criminal act anywhere in the world. The question of which state's or Country's Laws control an internet relations is still developing. Internet in remote sense is analogous to the high seas. No own owns it yet people of all nations use it. This makes control of cyber crimes an international issue. The aim of this paper is to look into issues of jurisdiction as it relates to electronic banking and make recommendations as appropriate.

Internet Jurisdiction

To decide what laws apply in Cyberspace, those responsible for the creation of laws must first decide whether Cyberspace is a place, a means of communication, or a state of mind. It is submitted that

* Ph.D Senior Lecturer, Department of International Law, Faculty of Law, Obafemi Awolowo University, Ile-Ife, Nigeria.

the internet merely represents yet another means of communication along a continuum of technological developments that date back to the discovery of electricity. But that does not mean that these questions are easily answered.

Second, if this new means of conducting business is to fully succeed and be as efficient and economical as possible, commercial rules that are at least predictable, if not certain, must be developed. Predictability requires a legal infrastructure that allows the participants to an electronic transaction to consummate it without undue concern over the risk of repudiation, the means of enforcement or the rules of dispute resolution. Jurisdictional predictability for a business may suggest that the law of the country of origin should apply, while for a consumer, it will mean that the law of the country of destination should apply. Is there an easy compromise to these polar alternatives? The internet, unlike earlier forms of electronic communication, moves data in a widely diffused fashion, which raises questions about what laws, should apply to it.

The Problems of Regulating Cyberspace[1]

Cyberspace is radically different from any space that man has conquered. Virtually every territory occupied by mankind is regulated. The fact that cyberspace is a creation of computers of different shapes and sizes, made by different manufacturers and with different processing powers and in scattered locations across the globe, connected by cables, telephones (fixed and wireless - GSM and CDMA inclusive) fibre optic, on land, in the air or under the sea makes the governance of cyberspace a daunting task. The attempt to regulate cyberspace by some countries' governments has been referred to as King Canute's comeback[2]. In Nordic/ English history, King Canute was a king who was fond of making laws for territories outside his control. His subjects flattered him that his word was so powerful that even the waves of the sea would obey him. He moved his throne to the seaside and began to give

[1] See Generally Bernard Oluwafemi Jemilohun and Timothy Ifedayo Akomolede (2015), "Legislating for Cyberspace: Challenges for the Nigerian Legislature', *Journal of Law, Globalization and Policy*, Volume 38, *www. iiste.org*

[2] Graham Greenleaf, 'An Endnote on Regulating Cyberspace: Architecture vs. Law?*'* [1998] UNSWLJ 52

orders to the waves until he was almost washed into the sea by the oblivious waves. But one does not have to be pessimistic about rules and legislation for cyberspace. Even though no one sovereign can claim to have total control over cyberspace, it is not a lawless or ungoverned frontier because many of the actions in cyberspace are not only occasioned by real people, but they also have consequences in the real world.[3] In considering the challenges of regulating cyberspace, the following are some of the suggested outstanding issues for the Legislature to work on:

(1) Personal jurisdiction in cyberspace
(2) The Default state of anonymity
(3) The threat of cybercrime

The highlighted issues will now be considered.

Personal Jurisdiction in Cyberspace[4]

Simply speaking, personal jurisdiction concerns the power of a court to adjudicate on a matter between parties. In order for a court to exercise jurisdiction, there must be a statutory or common law jurisdiction which must not surpass or overreach the limitations imposed by the Constitution[5]. Historically, the law on personal jurisdiction has changed over the years, reflecting changes of a more mobile society. Initially, personal jurisdiction could only be found if the party was physically present in the forum state. But the courts have evolved different rules to bring a party within jurisdiction even where the party is not physically present within the state. One of such is the principle of submission. The challenge with jurisdiction in cyberspace inheres is the fact that the operators and actors (*netizens*[6]) are not limited by time and space. As was observed in the American case of *Reno v. American Civil Liberties*

[3] Companies often take action against anonymous abuses in cyberspace by trying to unveil the identity of the abuser. Law enforcement agencies have power to search and the courts can subpoena service providers to identify some anonymous misusers of cyberspace.
[4] Ibid.
[5] Jay Kesan, "Learning Cyberlaw in Cyberspace: Personal Jurisdiction in Cyberspac*e",* available at *http://www.cyberspacelaw.org/kesan/kesan1.html*
[6] Internet citizens Journal of Law, Policy and Globalization *www.iiste.org* ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) Vol. 38, 2015

Union,[7] cyberspace is characterized by a tremendous permeability of boundaries: physical, political and social.

The regulation of real-space depends quite a bit on the assumption that fences and rivers will not leave their locations and jump around. But that assumption does not hold up in cyberspace. Cyberspace is a truly global technology that is simultaneously nowhere and everywhere[8]. The importance of this is that the "inhabitants" of cyberspace can "move" from one legal jurisdiction to another, and "chose" the legal rules that may be applicable to them. The foregoing is further reinforced in the words of Professor Michael Froomkin, "the multinational nature of the internet makes it possible for users to engage in regulatory arbitrage to choose to evade disliked domestic regulations by communicating/transacting under regulatory regimes with different rules. Sometimes, this will mean gravitating to jurisdictions with more lenient rules, or perhaps no rules at all; sometimes it will mean choosing more stringent foreign regimes … when stricter rules are more congenial"[9]. The American courts have devised methods of regulating this phenomenon that simply cannot be defined or confined within state lines. The first way by which the American courts bring parties in cyberspace within jurisdiction is by the 'minimum contact' principle. This means that once a party has some contact with the territory by brief physical presence[10] the courts are clothed with jurisdiction. However, for a state to exercise personal jurisdiction over an out of state defendant, two requirements must be met. Firstly, the state must have statutory authority that grants the court jurisdiction and, secondly, the due Process clause of the constitution must be satisfied.

The second way by which the American courts have developed personal jurisdiction rules in extraterritorial matters is by the use of 'long arm statutes'. These statutes allow a state to exercise jurisdiction over an out of state defendant by reaching into another

---

[7] 521 U.S. 844 (1997

[8] Margaret Chon, "Learning Cyberlaw in Cyberspace: The Relation of Law to Cyberspace and of Cyberspace to Law" available at *http://www.cyber spacelaw.org/chon/index.html* accessed on 26th July 2011 at 8:35 pm

[9] BrianKahin & Charles, "The Internet as a Source of Regulatory Arbitrage in Borders in Cyberspace" Nesson, eds., (MIT Press, 1997)

[10] *Burnham v. Superior Court*, 495 U.S. 604, 110 S.Ct 2105 (1990)

state. One of the first long arm statutes was enacted in the state of Illinois in the United States. The statute in part reads: "Any person, whether or not a citizen or resident of this state, who in person or through an agent does any of the acts herein enumerated, thereby submits such person and if an individual his or her personal representative, to the jurisdiction of the courts of this State as to any cause of action arising from the doing of any of such acts…" Evidently Nigerian state legislatures will not find it easy enacting 'long arm' statutes. And where the ease of enactment is there, the difficulties in enforcement are another set of challenges altogether.[11] One can only hope that the federal legislature will enact laws meant to affect the whole country in matters of this nature as, after all, matters bothering on post, telegraph and telephones, trade and commerce and wireless broadcasting are contained in the Exclusive Legislative List.[12]

Anonymity: The Default State in Cyberspace

It is widely accepted by internet users that as far as cyberspace is concerned, you are a dog. There is no physical means of directly ascertaining who the other party is. Cyberspace enables anyone without discrimination and with no possibility of identification[13] to communicate via text, sound or video to hundreds or thousands of people nearly instantaneously and at little or no cost. Due to the nature of the technology, identities in cyberspace are easily cloaked in anonymity and once a message sender's identity is anonymous, cyberspace provides the masses the means to perpetrate widespread criminal activity with little chance of apprehension. Anonymity has been classified into two kinds:[14] true anonymity and pseudo anonymity. True anonymous communication is untraceable and only coincidence or purposeful self-

[11] Bernard Oluwafemi Jemilohun and Timothy Ifedayo Akomolede (2015) Op. cit.

[12] Ibid.

[13] As Ron Dick, chief of the FBI's computer investigation section explained, "Until you get to the keyboard and Jurisdiction be identified, the sender herself may remain anonymous. "Biggest Cyber-attack Was Simple", NYTimes.com, Feb. 9, 2000, available at *http://www.nytimes.com*

[14]George du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 Mich. Telecomm. Tech. L. Rev. 2001 also available at *http://www.mttlr.org/volseven/duPont_art.html Journal of Law, Policy and Globalization www.iiste.org* ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online) Vol. 38, 2015

exposure will bring the identity of the mystery message sender to light. Because this is not easily discoverable, it has high potential for abuse because the message senders cannot be held accountable for their actions. Pseudo-anonymous communication on the other hand is inherently traceable. Though it may not be easily uncovered or readily available, it is still possible to discover the identity of the sender.

There are many different ways to communicate in cyberspace—email, chat, graphics, pictures, sound broadcasts or internet telephony, social network media[15], video, plain text, etc., and also there are many ways to communicate anonymously. For instance, with all the blocks placed on the web by internet based web mail providers[16], one can still open an email account without using one's true identity and the same applies to joining a social network like *Facebook* or *Netlog* or *Hi5*. Thus, a single individual can have as many web based email accounts as he wishes and since an email ID is the basic requirement for most online presence identification, he may choose to use some specific email account for anonymous social network interactions. It is common knowledge that people take nicknames in chat rooms to conceal their true identity from others[17]. The question that arises is whether it is in the overall interest of public good to legislate against anonymity. Over time, people have used anonymity as a cover for expressing dissent against unprofitable government policies or campaigning against repressive and dictatorial regimes. Quite a number of writers in history have used some form of anonymity or the other in presenting their ideas and thoughts to the world. The

[15]A reminder of the last days of President Yar'Adua, when some journalists were intimidated with prosecution over article suggesting the President was in poor health. See Reporters without Borders *http://www.rsf.org/Four-journalists-face-trialover, html* November 28, 2008.

[16]As at the year 2000, growing concern over the increased threat of cyber crime prompted the United States Department of Justice to request another $37 million the following year on top of the estimated $100 million already being spent to combat increasingly sophisticated computer criminals. Justice Department Wants More Funds to Fight Cyber Crime, CNN.com, Feb. 9, 2000, available at *http://www.cnn.com/2000/US/02109/cyber.crime.money/index.html* legislation.

[17] 3 COPPA 15 U.S. Code 6501 *Journal of Law, Policy and Globalization www.iiste.org* ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)Vol. 38, 2015 139

challenge for the lawmakers here is how to legislate against criminal anonymity without killing the spirit behind public-spirited and change-oriented anonymous messages.[18] Because cyberspace enables truly anonymous communication to flourish on a scale never before experienced, it also encourages anonymous unlawful acts. Since, the influence of cyberspace will increase in society, those acts are likely to become more persistent.

The challenge for the legislature is how to legislate against anonymity that is geared towards crime or other forms of abuse without criminalising free speech that is ultimately to *Strict Sense* Information Transactions Act, the Uniform Electronic Transactions Act and the Millennium Digital Commerce Act of 1999.[19] Some of the states have also enacted laws governing some aspects of cyberspace as far as their territories are concerned. The American position is not different from the Canadian position. In the case of the United Kingdom, laws governing the Internet are made largely by the British Parliament. One is not aware of any law operating in Britain on any aspect of cyberspace that is not an enactment of parliament.[20] Starting from the Computer Misuse Act of 1990 to the most recent British law on cyberspace, all laws on this area are enacted by the parliament. It could be guessed this is largely because Britain is largely homogenous and has always operated a unitary Constitution.[21]

The experiences of countries like the United States, Canada, Britain other European countries and countries under the Economic and Social Commission for Western Asia have shown a greater need for cyber-laws. Firstly, countries legislated for cyberspace when it became clear that previous legal regimes and laws were not adequate to govern the resultant effect of interactions in cyberspace due the novel issues emanating therefrom. In older cases as *CompuServe Inc. v. Cyber Promotions Inc*[22], the court found it was not easy to use or apply existing doctrines to regulate new behaviour. In principle, the same crimes or acts considered illegal offline are equally illegal and punishable under criminal and/or civil laws related to the online world.

---

[18] Bernard Oluwafemi Jemilohun and Timothy Ifedayo Akomolede (2015) Op. cit
[19] id
[20] id
[21] id
[2222] 962 F. Supp. 1015 (S.D. Ohio 1997)

However, in cyberspace, illegal acts and crimes take different forms with regard to the nature of the offender and the proof of the crime or illegal act. As a consequence of this, legislators have had to instigate new laws and regulations aimed at controlling the use of computers and computer-related data and transactions made in cyberspace. Secondly, the United States specifically had to legislate to protect cyberspace because the government recognizes the interconnected information technology and the interdependent network of information technology infrastructures operating across this medium as part of the US National Critical Infrastructure. It will be recalled that the Internet began largely as a brain child of the Americans and it was primarily restricted to a specific target group, primarily military and intelligence. But with the release of the Internet to the public domain, comes much risk that cannot be left to open chance or without regulation.

Thirdly, some countries like those under the Economic and Social Commission for Western Asia[23] have come to the understanding that cyberspace in the region cannot flourish without a proactive, favourable environment for the use of the Internet by people in their various activities. An important factor for achieving the enabling environment for that sector is crafting cyberspace laws and adopting directives in the legislative, organizational and management domains. Enlargements in commerce and technological developments and breakthroughs in research have been largely assisted by the Internet. Keeping the progress on will require some measure of legislation. Fourthly, online crime, it is believed, grew with the evolution of the Internet and this in turn has resulted in the need to maintain a secure space where data and intangible money could be stored, shared and transferred legally, and where personal data could be shared securely. The possibility of crimes across boundaries with difficulties in tracing or detection abounds due to the nature of the Internet. While it may not be possible to totally prevent crime by legislation, at least there is certainty about what is legal and what is unlawful. Fifthly and within this context, legal protection had to cover all possible legal issues and aspects whether related to commerce, personal and human rights and procedural acts, with regard to the collection of

[23] Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syrian Arab Republic, United Arab Emirates and Yemen

evidence in electronic form, specifically electronic evidence and electronic signatures. Further, cyber crime can be combated in cases where offender have infringed on intellectual property rights, or have obtained money through electronic fraud or breach of security systems.

Cybercrime Threats and Cross Border Issues[24]

Cybercrime remains one of the most serious forms of crime in the world today with newer and more sophisticated patterns of execution yet with not much success in apprehension[25]. That cybercrime is a threat is not limited to Nigeria alone; it is a global phenomenon. While we have earlier pointed out that the legal framework for Computer crimes and cybercrimes in Nigeria is in need of legislative creativity, it must be pointed out that the threat of cybercrime calls for international cooperation among nations.

Nigerian lawmakers and by extension policy makers must get acquainted with the different treaties and conventions been made against cybercrime and get in so that we can benefit. The cross border nature of cybercrime makes it an exercise in futility for any nation to attempt to handle it all by itself. It is also important that our lawmakers get acquainted with the different aspects of cybercrime and the various modalities by which criminals violate cyberspace. This is the age of information and for legislation to be meaningful and effective in this age, it must be informed. Again, it is time the Computer Security and Critical Information Infrastructure Protection Bill be passed into law after relevant additions and amendments in the light of global trends have been made to the Bill.

The introduction of e-money raises issues relating to the legal treatment of cross-border e-money payments[26]. For example cross border concerns could arise from the fact that the schemes might

[24] See Chawki, M. 'Nigeria Tackles Advanced Fee Fraud', 2009 (1) *Journal of Information Law & Technology (JILT), http://go.warwick.ac.uk/jilt/2009_1/ chawki* published 28 May 2009.

[25] As at the year 2000, growing concern over the increased threat of cyber crime prompted the United States Department of Justice to request another $37 million the following year on top of the estimated $100 million already being spent to combat increasingly sophisticated computer criminals. Justice Department Wants More Funds to Fight Cyber Crime, CNN.com, Feb. 9, 2000, available at *http://www.cnn.com/2000/US/02109/cyber.crime.money/ index.html*

[26] See C.E. Agene, Electronic Banking in Nigeria: Concept, Policy Issues and Supervisory Framework.

offer e-money in more than one currency, which might make it difficult for central banks to measure accurately the stock of e-money denominated in the home currency, banks accepting foreign currencies in payment of electronic money may be subject to market risks because of movements in foreign exchange rates. Many e-money schemes are being developed on the basis of technology or procedures developed in foreign currencies by for example, large international payment cards and companies. A concern may be how public authorities can obtain detailed and precise information about the products or schemes being promoted in their country by foreign vendors' attention to assessing, and how they might be able to influence individual schemes in the light of their particular domestic concerns. Cross border risks may be more complex than the usual risks bank face within their home country. Hence, banks and supervisors may need to devote added attention to controlling and monitoring operational legal and other risks arising from cross border electronic banking and e-money activities.

An Assessment of the Legal Frame work of Electronic Banking in Nigeria

In the familiar world of non-cyber transactions, the law has evolved over the years to serve multiple purposes.[27] As transactions move to a computer networked environment, though the objectives of the law have remained, the law has found it hard to fulfil them. Most times, the law falls short of fulfilling its goals when applied to electronic transactions. It is not as though the goods or the prices or the parties have witnessed any meta-morphosis, it is just that because the parties are removed from each other and the transactions are concluded in the remote realm of cyberspace, the new medium demands new approach by the law, lawyers and judges. If in the real world, the average consumer does not have an enduring protective regime as far as the laws are concerned, one can imagine the plight of the consumer of goods and services procured via electronic means.

While the possibility of contracting on the web is very real, there is no certainty that the person one assumes he is dealing with online is the same as one may encounter in the real world. In cases

[27] Bernard Oluwafemi Jemilohun and Timothy Ifedayo Akomolede (2015) Op. cit

where purchases are made via electronic documents like ATM Cards, Master Cards and co, an innocent business merchant may find out the identity of the user of the master card is not the same as that of the true owner. The law on electronic documents and computer generated evidence in Nigeria is not yet in line with the realities of online commerce when compared with the US and other developed countries. The Nigerian legislature has serious work to do here. Nigeria has not woken up to the reality of all this because the laws on ground are not adequate in the light of modern developments. Some of the laws on ground are laws used to regulate paper based transactions and these include:[28]

(a) The Criminal Code Act
(b) The Economic and Financial Crimes Commission Act, 2004
(c) Advanced Fee Fraud and other Fraud Related Offences Act, 2006
(d) The Computer Security and Critical Information Infrastructure Protection Bill, 2005
(e) Banks and Other Financial Institutions Act, 1991

The Criminal Code is a colonial legacy which predates the internet age, and as such does not directly address any type of cybercrime or even computer crime. The only provisions that may be relevant will be those dealing with obtaining by false pretence under Section 419 of the Act. Aside from this, I am not sure of any section under the Act that deals directly with cybercrime. The Economic and Financial Crimes Commission Act does not add anything worthy of note in this regard.

The Computer Security and Critical Information Infrastructure Protection Bill was presented to the National Assembly in 2005. Among other things, the Bill aims to '*secure computer systems and networks and protect critical information infrastructure in Nigeria by prohibiting certain computer based activities'* and to impose liabilities for global crimes committed over the internet. But till date, the Bill has not been passed into law. While the Bill may have certain deficiencies and imperfections, it is hoped that whatever correction necessary be put in place so that an appropriate law can be in place to at least 'regulate' the Nigerian cyberspace. It is only the Advanced Fee Fraud and other Fraud

[28] Bernard Oluwafemi Jemilohun and Timothy Ifedayo Akomolede (2015) Op. cit

Related Offences Act that really deal with electronic fraud on the internet. The Act provides as follows:

Section 12 (1) "Any person or entity providing an electronic communication service or remote computing service either by email or any other form shall be required to obtain from the customer or subscriber:

(a) Full names
(b) Residential address, in the case of an individual
(c) Corporate address, in the case of corporate bodies

(2) Any customer or subscriber who –

(a) fails to furnish, the information specified in subsection (1) of this section; or
(b) with the intent to deceive, supplies false information or conceals or disguises the information required under this section, commits an offence and is liable on conviction to imprisonment for a term of not less than three years or a fine of ₦100,000.

(3) Any person or entity providing the electronic communication service or remote computing service either by email or any other form who fails to comply with the provisions of subsection (1) of this section, commits an offence and is liable on conviction to a fine of ₦100,000 and forfeiture of the equipment or facility used in providing the service".

This provision shifts the burden of surveillance away from the government and vests the responsibility in industry players like Internet Service Providers and Cybercafé operators[29]. An attempt is made here to remove anonymity from users of internet services as cybercafés operators and ISPs will henceforth monitor the use of their systems and keep records of users' transactions. Laudable as this effort may be, one is of the opinion that due to the territorial limitlessness of cyberspace and the fact that information communication technologies are increasingly being made available to much private use.

[29] See Chawki, M. 'Nigeria Tackles Advanced Fee Fraud', 2009 (1) *Journal of Information Law & Technology (JILT), http://go.warwick.ac.uk/jilt/2009_1/chawki* published 28 May 2009.

Also, apart from the Central Bank of Nigeria's Guidelines on Electronic Banking, 2003 which has also been criticized severally to lack the potency to regulate issues on electronic banking, not to talk of internet jurisdiction on such; some other bills have also been put before the Nigerian National assembly. The relevant bills are the Electronic Transactions Bill and the Nigerian Bill on Cyber Crimes. The Electronic Transaction Bill provides for the validity of contracts, matters of Evidence, Electronic signatures, and payment systems among other issues. The draft Bill on Cyber crimes provides the legal and institutional framework for combating cybercrime in Nigeria and for ensuring cyber security. Provisions are also made for payment of compensation to victims of cyber crimes. Unfortunately these bills are yet to become laws. Nigeria does not also presently have any definite legislation on data protection[30]. There is also the absence of the Data Communication Act in Nigeria.

Nigeria obviously has a lot to do in providing an effective and all-encompassing legal framework. Piecemeal attempts at legislation may not go a long way.

Conclusion and Recommendations

The resolution of the jurisdictional legal uncertainties created by electronic commerce will be a function of the reconciliation of a wide variety of factors and national and state interests. The following recommendations will however be helpful for Nigeria and other countries in regulating cyber space banking transactions and in coming up with appropriate laws in determining cyber jurisdictions;

(1) Since no one state or nation can bring about predictability and certainty in global electronic commerce, a multi-national Global Online Standards Commission ("GOSC") should be established to study jurisdiction issues and develop uniform principles and global protocol standards. The GOSC's charter should require it to complete its work by a specific sunset date and to work in conjunction with other international bodies considering similar issues. The

[30] The best that Nigeria has at the moment are the Draft Guidelines on Data Protection published by the National Information Technology Development Agency pursuant to Sections 6, 17 and 18 of the NITDA Act

agenda of the GOSC should include the points discussed below.

(2) Technology should be used to solve the issues that it creates. There is no need to impose the burden upon consumers to read and negotiate the jurisdictional terms of their electronic commerce experience on a global basis. Intelligent electronic agents can be programmed to electronically communicate jurisdiction information and rules (including rules relating to taxation), enabling such preprogrammed agents to facilitate the user's or sponsor's automated decision to do business with each other. Similar software products have been deployed to allow consumers to use such electronic agents to monitor their journey through Cyberspace and warn them when they are entering a site whose privacy policies do not match their preferences. Businesses and/or nations of the world must, however, agree on the rules and standards under which such agents will operate.

(3) Cyberspace needs new forms of dispute resolution to reduce transaction costs for small value disputes and to erect structures that work well across national boundaries. Voluntary industry councils and cyber-tribunals should be encouraged by governmental regimes to develop private sector mechanisms to resolve electronic commerce disputes. Government-sponsored online cross-border dispute resolution systems may also be useful to complement these private sector approaches.

(4) Self-regulatory regimes should be encouraged to forge workable codes of conduct, rules and standards among a broad spectrum of electronic commerce participants to provide an efficient and cost effective jurisdictional model that governments can adopt and embrace.

(5) Personal or prescriptive jurisdiction should not be asserted based solely on the accessibility of a passive web site.

(6) Good faith efforts to prevent access by users to a site or service through the use of disclosures, disclaimers, software and other technological blocking or screening mechanisms should insulate the sponsor from assertions of jurisdiction.

(a) Users (purchasers) and sponsors (sellers) should be encouraged to identify, with adequate prominence and specificity, the state in which they habitually reside, so that jurisdictional con-sequences will not be a surprise to either party.

(7) Safe harbor agreements, such as the one negotiated between the United States and the European Union in the context of personal data protection should be encouraged to resolve jurisdictional conflicts in Cyberspace. They should include a public law framework of minimum standards, back-up governmental enforcement and the opportunity for a multiplicity of private, self-regulatory regimes that can establish their own distinctive dispute resolution and enforcement rules.
(8) Global regulatory authorities of highly regulated industries, such as banking and securities, should be encouraged to reach agreement regarding how laws will be applied to financial products and services offered in a global electronic environment.
(9) Any use of intermediaries ("choke points") in the flow of electronic information, commerce and money, such as Internet Service Providers and payments systems, to regulate commercial behaviour and to enforce juris-dictional principles impose significant, new legal burdens on those private entities which require careful exploration before being proposed for adoption.

In addition to the provision of the Model laws on the admissibility of electronic generated evidence and confidentiality of customer's data and information the following suggestions will also be instructive. Most of the suggestions are coined from case –laws i.e. court decisions.

Since 1995, Nigeria developed a National Policy on Information Technology that has not moved out of the paper cover till date. It is time the Federal Government commits itself to the policy without an adequate legislative framework, there can not be enough reason to motivate foreigners to invest in Nigeria. There must be a form of legal protection for privacy. The European Union has expressly forbidden the transfer of data from any of its member-nations into any nation that does not have adequate data protection laws. As a matter of urgency, Nigeria must update its

national policy on cyberspace by keeping abreast of the various sources of emerging cyber-security threats and preparing to counter them before they manifest. For instance, the phenomenon of terrorism has gone beyond attacks on people and physical infrastructure to attack on cyber-infrastructure. It is common knowledge that information has become the backbone of development and since information for development is now kept in cyberspace, terrorists have somewhat shifted attacks to the Internet. Nigeria must not wait to experience cyber-terrorism before enacting proactive legislation in this regard. The Computer Security and Critical Information Infrastructure Protection Bill should also be passed into law with the needed amendments without further delay. It is unfortunate that fourteen years since the turn of the new millennium, Nigeria is yet to have single comprehensive cyber legislation. No aspect of cyberspace is adequately covered by legislation in Nigeria. It is time for Nigeria to have adequate legislations to govern cyberspace.