Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.38, 2015

Legislating for Cyberspace: Challenges for the Nigerian Legislature

Dr. Bernard Oluwafemi Jemilohun
Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria
bojemilohun@gmail.com

Prof. Timothy Ifedayo Akomolede
Faculty of Law, Ekiti State University, Ado-Ekiti, Nigeria

Abstract
The need to make proper legislations governing interactions in the world of technology is a contemporary issue and several nations across the globe have made serious efforts at legislating for cyberspace. Nigeria as an emerging international market and a continental leader is capable of profiting in cyberspace but has not made serious attempts at legislating for interactions therein, thus the possibility of abuse of the infrastructure is largely open. This article argues that the Nigerian legislature should make adequate legislations to govern interactions in cyberspace and attempts to point out the challenges that the legislature should advert its mind to in the course of doing same. It also attempts to draw lessons from some other jurisdictions. In discussing the challenges, this article considered issues like personal jurisdiction in cyberspace, the default state of anonymity, the constitutional guarantee of freedom of speech, the threat of cybercrime and the need to strike a balance between data protection and freedom of information. The article concludes that though legislating for cyberspace may not be easy, laws must be made to govern it since online interactions have impacts in the real world.

1. Introduction

Generally, laws are made for specific territories. That jurisdiction is fundamentally territorial is evidence in the location of lawmakers within a particular territory and adjudicators also been located in the same territory. However, the advancements in technology have foisted on humanity a sort of territorial limitlessness wherein humans can engage in transactions without geographical or physical limitations. The possibility of such freedom has also brought with it some negative consequences. Not only can people engage in consensual dealings across boundaries, people can also commit crimes across boundaries and without physical presence. In the language of the e-proponents, the world has become a global village.

When the computer came on board as a personal tool not many people envisaged the possibilities that could arise from its continual employment. The initial uses were largely mathematical and then private usage and business interests came in. But with the developments in technology has come multi-dimensional usage of the computer and its offshoots so much that little can be done in today's world without the use of the computer. From research institutions, to banks, to hospitals, to airports to the industrial/manufacturing sector, to the market place, to the private home, the computer has become a major tool for accomplishing tasks and doing all manner of things.

The computer would not have attracted much attention if not for the possibility of sharing the information and resources contained in any one system via the possibility of networking.[1] This capability has made it possible for information and resources to be shared between computers and in the advanced forms between diverse types of electronic devices via telephone lines (cable or wireless) satellite links, fibre optics and so on. Beyond this possibility of sharing information is the capacity to store large amount of information both on local systems and on distant located servers. Were there to exist no possibility of such stored information been accessed without authorisation, there would have been less problems.

But as some of the people that made the Internet happen said, the Internet has revolutionized the computer and communications world like nothing before. The invention of the telegraph, the telephone, the radio, and the computer set the stage for this unprecedented integration of capabilities. The Internet is at once a world-wide broadcasting capability, a mechanism for information dissemination, and a medium for collaboration and interaction between individuals and their computers without regard for geographic location[2].

---

*LL.B. (Hons) B.L., LL.M, Ph.D., Lecturer, Faculty of Law, Ekiti State University, Ado-Ekiti
**LL.B. (Hons) B.L., LL.M, M.Phil., Ph.D., Professor & Dean, Faculty of Law, Ekiti State University.
[1] The term networking refers to any form of interconnectivity between stations (radio or television) or computers or even human in the sense of building and maintaining relationships that could be of mutual advantage
[2] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff (2003). A Brief History of Internet available at http://www.isoc.org/internet/history/brief.shtml last accessed on 9th September 2011

The fact that the Internet (or in the social context cyberspace), which is the connection of all computers, has become a place where so much is stored and so much is done requires that laws be put in place to guide human behaviour, warn against abuse and improper use and stipulate enforceable punishment for offenders. This paper makes an attempt to look at some of the various components of cyberspace requiring legislation, consider some challenges that may be confronted while attempting to legislate for cyberspace and offer some suggestions in the light of efforts made by other nations and regional bodies.

2. Cyberspace: An all-encompassing Phenomenon

The term cyberspace has come to represent an imaginary place in the realm of human interaction where computers and peripherals that make it the multi-functional tool that it is today, interact through cables, fibre optics and other wireless communication devices with real impact on the present world. In the language of William Gibson:

> *"Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children taught mathematical concepts… A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding…"*[1]

Or in the language of Donna Haraway,

> "*Cyberspace is a spatio-temporal figure of post modernity and its regimes of flexible accumulation. Like the genome, the other higher-order structures of cyberspace, which are displaced in counterintuitive ways from the perceptual assumptions of bodies in mundane space, are simultaneously fiercely material realities and imaginary zones. These are the zones that script the future, just as the new instruments of debt scheduling and financial mobility script the future of communities around the globe."*[2]

Thus, originally coined to describe data matrices existing in a dark distant future, the term cyberspace has entered the common lexicon. In other words, it has come to mean the information spaces created by the technology of digital networked computer systems, most of which ultimately connect with the mother of all networks, the internet. It follows that the meaning of cyberspace goes beyond the descriptive technological aspects such as the Transmission Control Protocol/Internet Protocol (TCP/IP) but also covers the social consequences of these technologies.

It follows that though an institution or an organisation may have its several computers and servers connected within its own network for its daily operations and business management; as long as those computers are linked together over the internet (and not limited to the organisation's intranet) the organisation actually has its dealings in cyberspace. A bank in Nigeria for instance may choose not to have direct transaction links with any bank in the United Kingdom, but once it is internet connected, the rules governing cyberspace (which may be unknown to the owners or operators or customers of the bank) govern the bank's dealings on the net. The resultant risk of this is that a computer hacker in the U.K. may access the bank's records without entering Nigeria's physical territorial space.

The possibility of wireless communication has made cyberspace more mysterious. In the early days when internet access was by telephone lines, the location of any user could be traceable by the telephone cables. But presently with the availability of mobile equipments via GSM[3] and other wireless forms, it has become more difficult tracing internet users. It is common knowledge that the default state in cyberspace is anonymity and as the popular adage created by Peter Steiner's cartoon says, "On the Internet, nobody knows you are a dog".[4] And today, Cyberspace has entered real space because, hardly is there any educated person living in real space that does not deal with or in cyberspace.

3. Some Considerations

It is common knowledge that the absence of regulatory framework in any human endeavour leads largely to unpredictable behaviour. That Nigeria is an emerging market[5] for information communication technology is obvious given rapid development in the telecommunication industry since the advent of GSM in 2001. Moreover, there are indigenous companies in Nigeria involved in the production of computers, both desktop and laptops[6]. This in itself is a sign of a growing market.

---

[1] The Neuromancer, (1984) New York: Ace Books
[2] Feminism and Technoscience, 1997.
[3] Global System for Mobile Communications
[4] This was the caption of a cartoon by Peter Steiner published in *The New Yorker* on July 5, 1993. It is available at en.wipedia.org/wiki_on_the_ internet_nobody_knows_you're_a_dog accessed on 4th September 2011
[5] A recent BBC post on www,bbc.com reads " Forget about oil and gas: Nigerians embrace communication technology
[6] Two prominent examples are *Zinox Computers* and *Omatek Computers*

Prior to the advent of GSM telecommunications, internet access in Nigeria was abysmally low as very few could afford broadband access and some of those that had telephone lines largely could not afford dial-up internet access. With the coming of the Global System for Mobile Telecommunications came several opportunities leading to the availability of handy modems that are quite affordable and give access almost anywhere a network signal is receivable. The resultant effect of this is that a larger percentage of the population, largely young people, now have unrestricted and uncensored access to the internet.

A report by the OpenNet Initiative on Internet filtering in Nigeria shows that from 80,000 Internet users in 2000 to 11,000,000 (eleven million) in 2008[1], Nigeria's online population has grown dramatically. Nigeria has over a hundred licensed Internet service Providers (though none holds a substantial share of the market) and traffic on the Internet in Nigeria is growing by the day. With this growing development comes the possibility of risky and unhealthy internet practices and usage. One is of the opinion that rather than avoid technology altogether because of the negative pictures borne out of some misuse, what Nigeria needs to do is to have a strong and result oriented legislative framework to regulate inter-relationships on the net and encourage full-scale development via technology. Technological development is an important issue in Nigeria. There is no way Nigeria can leapfrog from the backburner position it currently occupies except vigorous attempts are made to bridge the digital divide. One of the ways this should be done is via appropriate legislation.

The absence of any legislative framework is another serious consideration and thus this paper attempts to point out that which is necessary to note in the course of legislating for cyberspace. The Nigerian legal framework on most major contemporary issues is virtually non-existing. Most of our laws governing inter-relationships are relics from our colonial past[2] and it is necessary that laws are made to reflect the needs of a dynamic and ever-changing society. The information communication technology revolution is a heavy flood (though not negative) that is carrying everybody in its deluge and there is no nation that can go back. The best we can do is to design laws by which we can safely operate within it without injuring each other and our interests.

This paper attempts to show that there exists an urgent need for clear-cut legislation on cyberspace in Nigeria. It appears that over the years, Nigeria is content with borrowing laws from other territories and adapting the same to our use. Sometimes, some of these laws do not take into cognisance the realities of the Nigerian situation and thus do not meet up to expectation. This further compels judges to do a lot of judicial mechanics. An attempt to expand and develop the interpretation of existing legal provisions to take account of advances in technology may somewhat stretch the law to breaking point. As may be guessed, this was the situation in countries like the United Kingdom before relevant legislations were passed which adequately covered crimes of this specie[3].

Secondly, cyberspace which hitherto was relatively confined to a few computers on restricted networks in the United States[4] and a few other countries has become a world-wide accepted phenomenon. It is now known as the fifth realm. It will be sheer foolishness for Nigeria to believe that the laws enacted in the years before 1998 when the Internet became public stream will be adequate to govern transactions or prohibit certain acts and prescribe appropriate penalties for matters incidental to modern developments in cyberspace. As Oliver Wendell Holmes said, "it cannot be helped, it is as it should be, that the law is behind the times".[5] In other words, the law must change with the times.

Further in the process of lawmaking, lawmakers generally must be aware of the subject matter of the law. The Constitutional provisions[6] for the qualifications of people seeking election as lawmakers in Nigeria do not require any specialist knowledge on the part of the candidates. Thus the country may have the misfortune of having lawmakers in the two houses of the National Assembly who are ignorant of issues relating to information communications technology. There is the need to educate lawmakers and by extension policy makers of the necessity of a legal framework for this area and intimate them of the challenges involved. I am of the opinion that such needed service can be rendered through papers of this nature.

---

[1] International Telecommunications Union, "ITU Internet Indicators 2000" available at http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/Information Technology Public &RP_intYear2000&RP_intLanguageID=1; and" ITU Internet Indicators 2008"

[2] Examples are the Criminal Code Act, the Marriage Act, etc.

[3] See the speech of Lord Lane CJ in *R. v. Gold & Schifreen* [1987] QB 1116 at 1124 where he said "…that is not a criminal offence. If it is thought desirable to make it so, that is a matter for the legislature rather than the courts" In that case, an attempt to squeeze the activity of computer hacking into the framework of an inappropriate statute was treated with disdain by both the Court of Appeal and the House of Lords.

[4] The origins of the Internet in the Advanced Research Projects Agency Network (ARPANET) did not start as something for the public domain, rather it was a network of computers to prevent loss of data in military operations.

[5] Holmes, "Law and the Court" speech at a dinner of the Harvard Law School Association of New York on Feb 15, 1913 in Mark deWolfe Howe, ed., *The Occasional Speeches of Justice Oliver Wendell Holmes* (Cambridge, Mass.: Belknap Press 1962) 168. Also available at http://www.quoteland.com/author/Olover-Wendell-Holmes-Quotes/76/

[6] Sections 65 and 66 of the Constitution of the Federal Republic of Nigeria, 1999.

It is accepted generally that cyberspace cannot flourish without a proactive, favourable environment for the use of the internet by people in their various activities[1]. The importance of cyber legislation to the development of a modern information society cannot be over emphasized, thus active efforts by governments, the private sector and non-governmental organisations are essential for the establishment of the enabling environment needed for the appropriate use of cyberspace. Furthermore, the nascent nature of the information society in Nigeria requires appropriate legislative action in order to create an adequate enabling environment.
This paper is written with the assumption that the legislative duty and the legislative process are well understood by the body charged with making laws for the nation – the National Assembly[2]. An attempt will be made to look at the role of the legislature, and suggestions on making laws for this aspect will be made in line with lessons learnt from other jurisdictions.

4. Developments in Technology: Business possibilities and attendant problems

Business in today's world is different from what it was some 50 years ago. The possibilities of electronic communication and delivery systems have created new patterns of doing business and have raised new questions about the effectiveness of traditional laws governing business. In today's business climate, two or more people may do business without having to leave the shores of either country much less see each other. With the possibilities of communication via email, purchases on websites, the rapid growth of the Internet as a tool for commerce has brought a rapid shifting of common transactions from the marketplace to cyberspace. Unfortunately, this development has displaced millions of consumer purchases, plunging countless common consumers into arrangements made on the internet that often go sour[3].

In the familiar world of non-cyber transactions, the law has evolved over the years to serve multiple purposes. 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 metamorphosis, 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 where purchases are made via electronic documents like ATM Cards, MasterCards 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.

5. Computer crimes and related offences

The diverse possibilities brought about by the realities of cyberspace have brought more sophistication into crime. But it should be stated from the outset that not everything that is computer-related is cybercrime and not everything related to a computer is computer-crime. Some classifications of computer crimes include crimes against a computer system, crimes against computer programmes, crimes against computer data and crimes against computer devices.[4]

The use of computers as incidental to another offense is not cybercrime. Cybercrime may be defined as crime committed in cyberspace with computer as the target as well as the tool. Classifications of this include: crime related to persons like pornography, crimes related to consumer goods, crimes related to public sector e.g. attacks against public sector computer infrastructure and crimes related to information and electronic communication.

Since many financial institutions find it easier to operate electronically and customers and account operators can do money transfer, pay for goods and services, settle accounts from the comfort of their homes or offices or even on the road via mobile computing terminals, it has also become possible for criminals to hack into accounts to steal and commit all manners of unlawful and unauthorised transactions. This is the real problem

[1] See the Preamble to the Nigerian National Policy for Information Technology available at www.nitda.gov.ng
[2] This comprises the Senate and the House of Representatives. The Senate consists of 109 Senators, with three elected from each of the thirty-six states in the Federation and one from the Federal capital Territory. The House of Representatives on the other hand consists of 360 members elected from the 36 states but not by fixed members but more by near-equal geographical representation.
[3] Kenneth D. Crews, *Learning Law in Cyberspace – Electronic Commerce* available at http://www.cyberspacelaw,org/crews accessed on 17th November 2007 8:44 pm
[4] See however, Halder, D., & Jaishankar, K. (2011) Cybercrime and Victimization of Women: Laws, Rights and Regulations. Hershey, PA, USA: IGI Global

of identity theft – when someone other than the authorised owner gains access into a network by pretending to be the same as the real owner.

Cyberspace also brings together every service and facility imaginable to expedite money laundering. One can purchase anonymous credit cards, bank accounts, encrypted global mobile telephones, and false passports. From there one can pay professional advisors to set up IBCs (International Business Corporations, or corporations with anonymous ownership) or similar structures in OFCs (Offshore Financial Centres)[1]. Such advisors are loath to ask any penetrating questions about the wealth and activities of their clients, since the average fees criminals pay them to launder their money can be as much as 20 percent.

A direct manifestation of this form of crimes was the advanced fee fraud issue which was prevalent in Nigeria in the 90s. It commences with the receipt of an official-looking email usually purporting to be from the relative of a deceased government official seeking the victim's cooperation to retrieve funds belonging to the deceased but trapped in the bank. Despite the juicy rewards offered, the design is to defraud the respondents of as much money as possible. The difficulty in apprehending criminals of this sort is due to the fact that technology can be used to conceal the real identity and physical location of the perpetrators[2].

6. The Legal Framework for Computer crimes and Cybercrimes in Nigeria

Computer crimes by nature and by execution are sophisticated. The complex nature of the computer and the fact that computers speak to each other in languages that are unintelligible to the average mind makes it largely uneasy for the average person to detect much less curtail computer crimes. Initially, computer crimes were limited to crimes against computer systems and the owners and the common offences were: unauthorised access to information, distortion and outright damage to files and computer data via virus attacks, alteration of records on the computer etc. But with the deployment of the computer in the financial services sector the possibility and the incidents of fraud-related computer crimes became common place. The reality of the fact that the internet has made computer crimes transnational has added another dimension to the problem.

But it seems 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 include:

(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

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[3]. 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 be in place to at least 'regulate' the Nigerian cyberspace.

It is only the Advanced Fee Fraud and other Fraud 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 N100,000

[1] Johanna Granville "Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions," *Australian Journal of Politics and History*, vol. 49, no. 1. (Winter 2003), pp. 102-109.

[2] 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

[3] The provision on advanced fee fraud will only be relevant to computer crime or cybercrime if the transaction was initiated via email or other electronic means of communication.

(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 N100,000 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[1]. 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, Nigeria has a lot to do in providing an effective and all encompassing legal framework. Piecemeal attempts at legislation may not go a long way.

7. Informational Privacy in Cyberspace

Traditionally speaking, the Constitutional approach to the study of privacy involves thinking in terms of certain protected zones or spheres of activity like the home, reading, sexual life, reproduction, health etc. In part, this approach is due to the precedent nature of our legal system. The established pattern of fixing legal concepts in 'pigeon holes' has somewhat restricted our ability to think outside the box. The Nigerian Constitutional guarantee of the protection of privacy[2] of the citizens, their homes, correspondence, telephone conversations and telegraphic communications has always been seen as protection against government intrusion. It is not within the perspective of the average Nigerian that protection of privacy is freedom from misuse of personal information by other individuals, corporations or non-governmental organisations.

But, privacy is one of the most contentious issues in cyberspace. Just as in the actual world, privacy is of extreme importance not only to the individual internet 'citizens' but also corporations and Governments[3]. The fast rate at which identity theft occurs as a global crime calls for serious attention. The prevalence of identity theft has been attributed to about four reasons[4], namely:

- Huge margins for little effort and risk on the part of criminals
- Inadequate legislation or punishment to deter identity thieves
- Organisations not deploying appropriate security measures
- People not being aware of the value of their personal information

Nigeria does not presently have any definite legislation on data protection,[5] yet there is a lot of information gathering in digital form. For example, the last general elections were prepared for by digital voters' registration. No one is particularly sure of the safety of all the volumes of data captured by INEC's DDC[6] machines. The DDC machine operates biometric database software that captures bio-data of a person and stores them in the backend database. It also has the ability to capture photographic data and fingerprints.

It is true that Nigeria needs a biometric database for the citizenry for a myriad of reasons like security, national development, economic planning, educational policy formulation, elections, crime prevention etc, but if there is no legal framework for data protection, the courts will soon be inundated with suits on abuse within a short while. A few years back, the GSM service providers embarked on SIM[7] registration exercises under the directive of the Nigerian Communications Commission and again biometric data are being collected at the registration centres. There is no guarantee that this will not be subjected to abuse sooner than later. For this and many more other reasons, Nigeria needs an appropriate legislative framework to regulate cyberspace.

8. The Legislative duty of Lawmaking

The lawmaking role of the Legislature is predicated on the phrase "power to make laws for the peace, order and good government of the Federation or any part thereof". It follows therefore that the power to make laws is not endowed on the legislature for the purpose of their members but for the benefit of the inhabitants wherein the

[1] 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.
[2] Section 37, Constitution of the Federal Republic of Nigeria, 1999.
[3] Pavan Duggal: Privacy in Cyberspace *http://www.cyberlaws.net/cyberindia/privacy1.htm* visited at 08:43:50pm on 11/17/2007
[4] Franklin F. Akinsuyi: Data Protection Legislation for Nigeria, The Time is Now *http://www.nigerianmuse.com/20071004075550zg*
[5] 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.
[6] Direct Data Capture
[7] Subscriber Identity Module

legislature serves.[1] It then behoves the legislature to be acquainted with the dynamic nature of the society and aspire to meet up with the changes and render quality service in lawmaking to the populace by legislating to cover modern issues. It is important that the legislature is abreast of current global trends and the futility of applying outdated legislations to govern modern transactions.

The lawmaking duty of the Nigerian legislature is performed by two bodies jointly known as the National Assembly. As far as making laws for the whole nation is concerned, the Constitution creates an Exclusive Legislative list governing matters that the component states legislative houses do not have any part in. The Exclusive List largely contains matters that affect the entirety of the Nigerian nation and not just individual component states. Relative to cyberspace on the Exclusive legislative List are:

(i) Item 46 Posts, telegraphs and telephones
(ii) Item 62 Trade and Commerce
(iii) Item 66 Wireless, broadcasting and television other than broadcasting and television provided by the Government of a State; allocation of wavelengths for wireless, broadcasting and television transmission.

It is not really surprising that the Schedule does not particularly mention cyberspace as an item for which only the National Assembly could make laws. The truth is that Nigerian governments successively have never paid much attention to this area. But it is possible that laws for this realm could be made under the items mentioned above as a combination of the impact of telephones and wireless broadcasting is what is known as cyberspace today.

9. The Problems of Regulating Cyberspace

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 others 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. Constitutional guarantee of freedom of speech and expression
4. The threat of cybercrime
5. Data Protection versus Freedom of Information

9.1 Personal Jurisdiction in Cyberspace

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[4]. 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 in the fact that the operators and actors (*netizens*[5])

[1] See B. Femi Jemilohun, *The Role of the State Legislature as Enshrined in the Nigerian Constitution* The Jurist Consult, Vol. 8, 121-133, University of Ado-Ekiti.2010
[2] Graham Greenleaf, *An Endnote on Regulating Cyberspace: Architecture vs. Law?* [1998] UNSWLJ 52
[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] Jay Kesan, *Learning Cyberlaw in Cyberspace: Personal Jurisdiction in Cyberspace* available at http://www.cyberspacelaw.org/kesan/kesan1.html
[5] Internet citizens

are not limited by time and space. As was observed in the American case of *Reno v. American Civil Liberties Union*,[1] 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[2]. The import 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 Prof 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"[3].

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[4] 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[5].

The second way by which the American courts have developed personal jurisdiction rules in extra-territorial 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 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. 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.

9.2 Anonymity: the Default State in Cyberspace

It is widely accepted by internet users that as far as cyberspace is concerned, you are a dog[6]. There is no physical means of directly ascertaining who the other party is. Cyberspace enables anyone without discrimination and with no possibility of identification[7] 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:[8] true anonymity and pseudo anonymity. True anonymous communication is untraceable and only coincidence or purposeful self-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.

---

[1] 521 U.S. 844 (1997)
[2] Margaret Chon, Learning Cyberlaw in Cyberspace: The Relation of Law to Cyberspace and of Cyberspace to Law available at http://www.cyberspacelaw.org/chon/index.html accessed on 26th July 2011 at 8:35 pm
[3] The Internet as a Source of Regulatory Arbitrage in Borders in Cyberspace (Brian Kahin & Charles Nesson, eds) (MIT Press, 1997)
[4] *Burnham v. Superior Court*, 495 U.S. 604, 110 S.Ct 2105 (1990)
[5] Jay Kesan, *op cit.*
[6] *Supra* footnote 6 above
[7] As Ron Dick, chief of the FBI's computer investigation section explained, "Until you get to the keyboard being utilized [by an anonymous message sender], you don't know what you're dealing with." In other words, even if the sender's computer can be identified, the sender herself may remain anonymous. "Biggest Cyber-attack Was Simple" , NYTimes.com, Feb. 9, 2000, available at http://www.nytimes.com
[8] 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

There are many different ways to communicate in cyberspace: email, chat, graphics, pictures, sound broadcasts or internet telephony, social network media[1], 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[2], one can still open an e-mail 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 chose 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[3].

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[4]. The challenge for the lawmakers here is how to legislate against criminal anonymity without killing the spirit behind public-spirited and change-oriented anonymous messages. Because cyberspace enables truly anonymous communication to flourish on a scale never before experienced, it also encourages anonymous unlawful acts[5]. 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 the advantage of the society.

9.3 Freedom of Speech and Expression

This, in most countries is a guaranteed right that is commonly called a fundamental human right[6]. It is one of the inalienable rights of man and anywhere it is not upheld or respected, such government is branded a dictatorial or oppressive regime[7]. The right to freedom of speech and expression under the Nigerian Constitution is called freedom of expression and the press[8]. The Constitution provides that:

Section 39 (1) "Every person shall be entitled to freedom of expression, including freedom to hold opinions and to receive and impart ideas and information without interference.

(2) Without prejudice to the generality of subsection (1) of this section, every person shall be entitled to own, establish and operate any medium for the dissemination of information, ideas and opinions

Provided that no person, other than the Government of the Federation or of a State or any other person authorised by the President on the fulfilment of conditions laid down by an Act of the National Assembly shall own, establish or operate a television or wireless broadcasting station for any purpose whatsoever.

(3) Nothing in this section shall invalidate any law that is reasonably justifiable in a democratic society –

(a) for the purpose of preventing the disclosure of information received in confidence, maintaining the independence and authority of courts or regulating telephony, wireless broadcasting, television or the exhibition of cinematograph films; or

(b) imposing restrictions upon persons holding office under the Government of the Federation or of a State, members of the armed forces of the Federation or members of the Nigeria Police Force or other Government security services or agencies established by law."

The American courts have decided that communication in cyberspace is a form of speech and thus any attempt to regulate it must not violate the First Amendment. For the larger part, legislations made by States in the United States have been largely unenforceable because they have been found to breach the spirit of the First Amendment. In the popular case of *Reno v American Civil Liberties Union*[9], the Supreme Court ruled that that the Communications Decency Act violated the First Amendment. Passed in 1996 as part of the Telecommunications Act, the CDA provided criminal penalties for knowingly transmitting indecent material to

[1] Examples are *Facebook, LinkedIn, Twitter, Netlog, Flixster, Hi5, Badoo, 2go*, etc

[2] Examples are *Yahoo mail, Hotmail and Gmail*. To create an account in any of these, there are questions to be answered and one may sometimes be required to re-write some words in a box to ensure that it is not an automated system that is creating the email address. None of these restrictions can ensure that the person before the computer is actually who he claims to be as there are no means of verification.

[3] *Supra* note 48

[4] Mark Twain (Samuel Langhorne Clemens), O. Henry (William Sydney Porter), Voltaire (Francois Marie Arouet), George Sand (Amandine Aurore Lucie Dupin), George Eliot (Mary Ann Evans), Charles Lamb (sometimes wrote as "Elia"), Charles Dickens (sometimes wrote as "Boz"), and Benjamin Franklin (employed numerous different pseudonyms) all cloaked their identities with various levels of anonymity. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 342 n.4 (1995).

[5] George DuPont, *op cit.*

[6] It is contained in Chapter 4 of the Nigerian Constitution under the heading "Human Rights"

[7] An example of such is the dismantled Apartheid regime of South Africa.

[8] Section 39, Constitution of the Federal Republic of Nigeria 1999

[9] *Supra*

minors over the Internet. Recognizing the vastness of the Internet as an information source, the Court held that it was protected by the Constitution to at least the same degree as print media.

Our Constitution also gives freedom of speech and till date, there have not been reported cases of undue censorship of the Internet in Nigeria. However, in the past, relationship between the government and the media has never been too smooth[1] and sometimes newspapers have been temporarily closed down due to some reasons.

While the Constitution provides some instances of derogation of the right to freedom of expression and of the press, it is hoped that our lawmakers will learn to address specific issues without passing an umbrella legislation that will be seen as an abrogation of free speech.

9.4 The Threat of Cybercrime

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[2]. 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.

9.5 Data Protection versus Freedom of Information

One of the challenges of legislating for cyberspace is striking a balance between the right to informational privacy and the right to freedom of information for governmental use. As earlier pointed out, the average Nigerian (or even African) does not see data protection or privacy rights as a serious issue and that is why there has been no legal challenge to the directive of the Nigerian Communication Commission to GSM service providers to register all SIM card owners. Beyond this, the suggestions that service providers will retain user data has not been met with any reaction either in the courts of law or the courts of public opinion.

The legislature must strive to strike a balance between the need for protection of private data and the need to make public information accessible.

10. Experiences of other developing and developed countries

The United States operates a federal system of government like Nigeria with components states. However matters surrounding cyberspace are not placed in the exclusive preserve of the Congress. The States have the liberty to make laws governing various aspects of the Internet. In the United States, some of the laws made to regulate transactions and interactions in cyberspace include the Communications Decency Act, the Children's Online Privacy protection Act[3], the Personal Data privacy and Security Act, 2005, Uniform Computer Information Transactions Act, the Uniform Electronic Transactions Act and the Millennium Digital Commerce Act of 1999. 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. I am not aware of any law operating in Britain on any aspect of cyberspace that is not an enactment of parliament. 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. One guesses this is largely because Britain is largely homogenous and has always operated a unitary Constitution.

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-

[1] 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-trial-over,html November 28, 2008.

[2] 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

[3] COPPA 15 U.S. Code 6501

legislation.

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. CyberPromotions Inc*[1], 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. 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[2] 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 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.

11. Conclusions and Recommendations.

Legislating for cyberspace may not be an easy task for the Nigerian legislature, but we must have laws because as we have seen, interactions in cyberspace have real effects in the offline world. As earlier pointed out, cyberspace is as real as any other realm occupied by man and it has permeated every aspect of our lives. If there is any need for legislation to govern and moderate human interactions, then there must be laws to govern dealings in the online world because online transactions have offline effects in the real world.

As far back as 1995, Nigeria developed a National Policy on Information Technology that has not moved out of the paper cover till date. One strongly feels that it is time the Federal Government commits itself to the policy. We have pointed out that without an adequate legislative framework, there can't 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.

It cannot be over-emphasized that the Computer Security and Critical Information Infrastructure Protection Bill should 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 one single comprehensive cyber-legislation. No aspect of cyberspace is adequately covered by legislation in Nigeria. It is time for Nigeria to have

[1] 962 F. Supp. 1015 (S.D. Ohio 1997)
[2] Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, Syrian Arab Republic, United Arab Emirates and Yemen

adequate legislations to govern cyberspace.

References

Leiner, B.M. et al. (2003). A Brief History of Internet available at http://www.isoc.org/internet/history/brief.shtml (September 9, 2011)

Gibson, W., (1984) The Neuromancer. New York: Ace Books

Haraway, D., (1997) Feminism and Technoscience.

Holmes, (1913) "Law and the Court" in Howe, M. D.,ed., *The Occasional Speeches of Justice Oliver Wendell Holmes* (Cambridge, Mass.: Belknap Press (1962) 168. Also available at http://www.quoteland.com/author/Olover-Wendell-Holmes-Quotes/76/

Crews,K. D., (2007) *Learning Law in Cyberspace – Electronic Commerce* available at http://www.cyberspacelaw,org/crews accessed on 17th November 2007 8:44 pm

Halder, D., & Jaishankar, K. (2011) Cybercrime and Victimization of Women: Laws, Rights and Regulations. Hershey, PA, USA: IGI Global

Granville, J., (2003) "Dot.Con: The Dangers of Cyber Crime and a Call for Proactive Solutions," *Australian Journal of Politics and History*, vol. 49, no. 1. (Winter, pp. 102-109.

Chawki, M., (2009) 'Nigeria Tackles Advanced Fee Fraud' , (1) Journal of Information Law & Technology (JILT), http://go.warwick.ac.uk/jilt/2009_1/chawki

Duggal, P., (2007) Privacy in Cyberspace *http://www.cyberlaws.net/cyberindia/privacy1.htm (November* 17 2007

Akinsuyi, F. F., Data Protection Legislation for Nigeria, The Time is Now *http://www.nigerianmuse.com/20071004075550zg*

Jemilohun, B. O., (2010) *The Role of the State Legislature as Enshrined in the Nigerian Constitution* The Jurist Consult, Vol. 8, 121-133, University of Ado-Ekiti.

Greenleaf, G., (1998) *An Endnote on Regulating Cyberspace: Architecture vs. Law?* UNSWLJ 52

Kesan, J., *Learning Cyberlaw in Cyberspace: Personal Jurisdiction in Cyberspace* available at http://www.cyberspacelaw.org/kesan/kesan1.html

Chon, M., Learning Cyberlaw in Cyberspace: The Relation of Law to Cyberspace and of Cyberspace to Law available at http://www.cyberspacelaw.org/chon/index.html accessed on 26th July 2011 at 8:35 pm

Kahin, B. & Nesson C., (1997) The Internet as a Source of Regulatory Arbitrage in Borders in Cyberspace (MIT Press,)

Du Pont, G., (2001) *The Criminalization of True Anonymity in Cyberspace,* 7 Mich. Telecomm. Tech. L. Rev.

The IISTE is a pioneer in the Open-Access hosting service and academic event management. The aim of the firm is Accelerating Global Knowledge Sharing.

More information about the firm can be found on the homepage:
http://www.iiste.org

CALL FOR JOURNAL PAPERS

There are more than 30 peer-reviewed academic journals hosted under the hosting platform.

Prospective authors of journals can find the submission instruction on the following page: http://www.iiste.org/journals/ All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Paper version of the journals is also available upon request of readers and authors.

MORE RESOURCES

Book publication information: http://www.iiste.org/book/

Academic conference: http://www.iiste.org/conference/upcoming-conferences-call-for-paper/

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar