British Journal of Arts and Social Sciences
ISSN: 2046-9578, Vol.5 No.2 (2012)

http://www.bjournal.co.uk/BJASS.aspx

The ICT Revolution and Commercial Sectors in Nigeria: Impacts and Legal Interventions

Adejoke O. Oyewunmi, PhD (Ife),
LL.M.I.P. (Piercelaw USA), LL.M. (Lagos),
Faculty of Law, University of Lagos.
E-Mail : adejoke21@yahoo.com
2348052081414

Abstract

This paper examines the impacts and challenges of information and communication technology in diverse aspects of commerce, banking and business activities in Nigeria. Against the background of international standards, the paper discusses emerging legal responses aimed at safeguarding the security and integrity of online transactions, and promoting certainty in the outcomes of dealings carried out through the medium. The paper concludes that while ongoing legislative interventions are desirable, the highly fragmented nature of emerging ICT laws and multi-layer regulatory institutions will unnecessarily complicate the legal and institutional landscape, and defeat the purpose of certainty and simplicity.

Keywords: ICT, Law, Nigeria, Business.

1.0. Introduction

Despite a rather late start, available statistics indicate that information and communication technology (ICT) is rapidly gaining ground in Nigeria. Due to its many possibilities, ICTs constitute veritable tools for socio-economic development, which makes the legal and regulatory environment for their application in developing countries critical. Among other impacts, ICTs have brought about significant changes in business practices with respect to banking transactions and, to some extent, the buying and selling of goods and services, through the possibilities of the medium to promote trade and commerce through wider access to prospective customers from anywhere on the globe for products and services. ICTs have thus transformed the business world, including the banking, trading and entertainment sectors, making the sectors more efficient and less limited by the barriers of time, distance and costs.ICTs also have the potential to contribute to poverty alleviation through websites promoting local products in international markets, and facilitating access to market information for competitive prices for locally produced crafts, clothing and farm produce.[1] The technology further offers an opportunity for the exploitation of foreign markets for cultural products, a market which continues to expand in line with increases in the African Diaspora eager for means to access local food, clothes, music, films and other aspects of their cultural identity and heritage.

On the negative side however, the technology has been accompanied by the emergence of new dimensions of crimes by those who, rather than exploiting the opportunities presented by ICT in legitimate ways for positive activities, rather do so for dubious or out rightly fraudulent acts. Thus, cyber crimes like child pornography, fraudulent electronic fund transfers, and unauthorised access to computer systems have become widespread. Tackling the problem of cyber crime and the attendant image nightmare to Nigeria poses legal and policy challenges, which result in efforts to stretch the laws in a bid to accommodate the new challenges.

The fact however, is that there is a limit to which laws, which were promulgated in a different technological and socio-economic context, can adequately cater for the new technological realities presented by ICTs. It thus becomes necessary for legal rules to be developed to tackle the issues and challenges brought about by ICTs, in order to promote public confidence, maximise the benefits of the technology and encourage wider acceptance and use by individuals as well as private and public organisations. This paper examines diverse aspects of commerce, banking and business generally, which have been impacted by ICTs, and against the background of international standards, discusses emerging legal responses under Nigerian law.

1.2. Operational Definition of ICT and an Overview of Internet Use in Nigeria

The term "information and communication technology" (ICT), describes the integration of two previously existing disciplines: computing and telecommunications.[2] ICT therefore refers to the convergence of audio-visual and telephone networks with computer networks, and the technology encompasses a wide range of activities, ranging from office data processing to remote control and monitoring of manufacturing robots.[3] It also covers the cabling infrastructure e.g. fibre optic cables, which carry voice, data and video communications.[4] A major offshoot of the convergence of information and communication technology is the emergence of the internet, which is a content distribution network comprising of a global system of interconnected computer networks through which data is interchanged. The technology consists of millions of private and public academic, business and government networks of both local and global scope which facilitates the dissemination and exchange of information, and makes diverse other forms of non-physical interaction the new reality.

From modest beginnings in the 1990s, internet penetration and use have continued to grow in Nigeria, [5] and apart from its impact in the banking and commercial sectors,[6] has become very popular as a means of communication, through the electronic mail system, as well as a means of accessing news and information generally. Also, in the health sector, it has impacted diverse aspects of medical care, including the provision of medical information, diagnosis and treatment as well as the training

of medical personnel.[7] Despite its positive aspects, ICT however, poses challenges for legal regulation in several important respects.

2.1. ICT and the Menace of Cyber Crime in Nigeria

As ICT access and use began to grow, so also did the menace of cyber crime. Cyber crime consists of a variety of criminal acts perpetrated through the Internet, and includes e-mail scams, child pornography, hacking, theft of data, identity theft, extortion and a wide array of other nefarious activities. Other ICT–related crimes include the counterfeit cashier's cheque scheme, which relies on the issuance of fraudulent cheques, and targets individuals that use Internet advertisements to sell merchandise. Another is the advance fee fraud, also known as the "419 scam", after the section of the Nigerian Criminal Code dealing with the crime of obtaining property by false pretences.[8] The 419 scam combines impersonation fraud with a variation of an advance fee scheme, and relies on letters, emails, or faxes to potential victims from individuals representing themselves as government officials, offering the recipient the "opportunity" to share in a percentage of millions of dollars, while soliciting for help in placing large sums of money in overseas bank accounts. [9]

The problem of cybercrime is a global one whose extent, magnitude and impact reverberate throughout various walks of life, leaving hitherto unimaginable damage in its wake. [10] Popularly referred to as the "yahoo yahoo syndrome" in Nigeria, these fraudulent activities are carried on by a recalcitrant few, but the impact is far reaching due to the world wide reach of the Internet. Cybercrime is not only an embarrassment, it also has negative implications for the positive deployment of ICT for socio-economic growth and development.

With a view to dealing with some of the problems occasioned by cybercrime, the Nigerian government has deployed some legal and enforcement tools, including the enlistment of the Economic and Financial Crimes Commission (EFCC)[11], the Nigerian Police Force, and other crime fighting bodies to tackle the problem. Unfortunately however, initial attempts to deal with the problem did not utilise a refined and technology savvy approach to detect and arrest perpetrators. Rather, law enforcement officers largely descended on cyber cafes, carrying out frequent raids, arrests, ban of overnight browsing and other activities. However, resort to cyber cafes for internet access has waned considerably, with more possibilities to access the internet through mobile phones and personal computers. This may be attributed to the deregulation of the telecommunications sector, which has afforded the public the benefit of competitive internet access options by telecommunications companies, thus making private internet more accessible and affordable.This modification in the location of use from cyber cafes to private offices and homes means that physical raids of cyber cafes and other public venues for internet access can no longer constitute a valid approach to tackling online criminal activities. Rather, use of technological means and seeking of relevant information from, and collaboration with Internet Service Providers (ISPS) have become inevitable. This on its part raises the need for proper training and adequate deployment of specialised police and other enforcement authorities.[12] Additionally, there is the issue of the security of stored customer data, which has been a concern in many developed countries, where servers holding millions of customer data have been hacked, and storage media such as compact discs holding data on millions of customers have been carelessly misplaced or lost in the post.[13]

Beyond these however, more effort should be made to refocus on the promotion of positive uses of ICT. In this regard, it is encouraging that Microsoft has partnered with an NGO (Paradigm Initiative Nigeria (PIN)) to tackle cyber crime through its Internet Safety, Security and Privacy Initiative for Nigeria (ISSPIN). [14] The programme essentially focuses on redirecting the energy of young Nigerians away from cyber crime and towards positive utilisation of cyber space for legitimate purposes.[15] Microsoft also aims at addressing the need for adequate training in information technology among young Nigerians by distributing free compact discs containing Microsoft's Digital Literacy Curriculum.[16] There is also the practical aspect of empowerment through training programmes designed to arm youths with marketable skills for legitimate business activities in the

online environment. As awareness continues to rise about the potentials of the technology, there is a corresponding need for the creation of local content online, establishment of websites for businesses, as well as online advertisements and marketing. Expertise and skills in these areas are therefore increasingly becoming more valuable, and a legal framework that deals with protection of creativity, prevention of misrepresentations and fraudulent acts become relevant. Hopefully, skill acquisition in these areas will not only reduce the tendency towards commission of cyber crimes, but also contribute to a reduction in the number of the unemployed in the country.

2.2. E-Contracts, E-Commerce and E-Banking

The ICT revolution also presents possibilities for the carrying on of commercial transactions, including buying and selling of goods and services, promotion of businesses and other related activities online. The new issues arising in this regard cut across the formation and validity of contracts, where questions may be raised about whether, for contracts which are in writing, e-mails and other means of electronic communication satisfy the requirements of writing and signing. Thus, the validity of ICT-related commercial transactions, their admissibility in evidence and options for dealing with conflict of laws issues arising where, as is often the case, these transactions are carried out between persons who are connected to different countries have been severally identified as some of the challenges posed by ICT.[17]

With regard to the buying and selling of goods, the law sets out the obligations of sellers and buyers in such contracts.[18] However, these legal provisions inadequately address concerns arising in the online environment. For example, under the law, the place of delivery of goods is deemed to be the seller's place of business.[19] However, in the case of e-commerce, the existence of a physical place of business cannot be assumed. Furthermore, even where such exists, it can no longer be presumed to be the place of delivery. Thus, there is a need for legislation which addresses concerns of buyers and consumers generally by specifying obligations of sellers in e-commerce, including the indication of a geographical address of the seller's place of business where complaints may be addressed, and terms of exercise of withdrawal options.[20] This is to preserve the buyer's right of examining the goods, and the presumption against acceptance of goods until the opportunity to examine has been given. [21] Other consumer protection provisions which ought to be put in place include disclosure of the full identity of the seller and cost of delivery. Options for achieving these objectives include the promulgation of a new law or the amendment of existing laws, such as the sale of goods law and the consumer protection law.[22]

On its part, in the banking sector, the replacement of the age-old ledger system with computers linked to internet facilities has brought about a revolution in the sector. Online/e-banking allows customers to carry out a wide variety of banking and other financial activities online, through a website operated by the bank. A major benefit of internet banking is the ease and convenience of managing one's finances from a place and time of one's choosing. Thus, financial transactions including checking of account balance, monitoring transactions, payment of utility bills, transfer of funds and monitoring, confirmation and stoppage of cheques can be conveniently carried out from any location. A related development is the use of electronic devices such as magnetically encoded plastic cards that permit customers to make cash withdrawals and pay for transactions without visiting banking halls, through ATMs (Automated Teller Machines), POS (Point of Sale) and other online channels. The possibilities provided by e-banking, which reduces the need to carry cash on personal and business trips, while also affording ready 24-hour access and convenience for users represents one of the most obvious and potent impacts of ICT in Nigeria.[23]

However, despite the progress in the sector, there are certain challenges which need to be addressed to facilitate the carrying on of e-commerce and other on-line activities. In particular, the availability of effective payment mechanisms which enjoy acceptance in international circles to support cross-border online transactions need to be strengthened. This is mainly through addressing the negative perception of Nigeria as a haven where cybercrime thrives, and which is therefore a

risky country to carry out online commercial and financial transactions in. At the heart of this challenge is the need for suitable legal and regulatory framework to address the emergence of e-banking. This is with a view to promoting public trust and confidence in e-banking by providing mechanisms which effectively protect customers from the risk of hackers, fraudsters and other criminal acts in the online environment.

At present, there is a lacuna in the main Nigerian legislation regulating the banking sector, as this does not deal with e-banking.[24] Similarly, neither the Nigerian Criminal Code nor the common law principles which regulate the banker/customer relationship adequately address the problem of cyber crime and other critical issues arising in e-banking. There is therefore a need for legislation to tackle diverse issues such as responsibility for authentication and security, and the allocation of risks for losses arising from the carrying out of unauthorised transactions in e-banking, protection of personal information, jurisdictional issues, admissibility of electronic transactions in evidence and other issues peculiar to the ICT environment. Although to some extent, part of the issues are addressed by the Central Bank of Nigeria (CBN)'s Regulations on Electronic Banking, which deals with licensing, supervision and other regulatory roles of the CBN, the Regulations specifically note the absence of laws dealing with e-banking in Nigeria.[25]

A recent example of legal uncertainty regarding the admissibility of computer generated bank statement may be seen in the case of *Federal Republic of Nigeria V. Femi Fani Kayode*.[26] There, the trial judge had held that the computer generated statement of account of the accused person, Chief Fani-Kayode was inadmissible in evidence, for failure to comply with the provisions of Section 97 of the Evidence Act.[27] The ruling was however, reversed by the Court of Appeal, which held that the computer print out of the statements of transactions was admissible.[28]

2.3. Trade Marks, Domain Names and Cyber Squatting

Another area of impact of ICT in Nigeria is the intersection between domain names, which are the titles with which websites are identified and located, and trade mark law. A domain name is the internet equivalent of an online telephone directory,[29] and comprises different elements. These elements include a Top Level Domain (TLD), which appears as a suffix to the name of the site, [30] and Second Level Domains (SLD), which usually include or even mirror the trademark or business name of the registrant, thus facilitating the functioning of domain names as business identifiers in a manner similar to trademarks.[31] Domain names therefore, adequately identify the user, and enable consumers to perceive the requisite nexus between the enterprise and the site. The use of such trademarks as SLDs for entities other than the trade mark owner may therefore result in free riding and other forms of unfair competition, thus giving rise to the need for protection of trademarks in the ICT environment.[32]

Beyond free riding, such use may also border on public deception and fraud, as may be seen in the WIPO arbitration case of *Shell International Petroleum Co. v Allen Jones.*[33] Here, the domain name www.shell-nigeria.com was falsely registered in respect of a website. The false site copied information from the website of the well known Shell Oil Company and was sufficiently similar to the legitimate Shell Company's website as to be likely to cause confusion. Likewise, the domain name was deceptively similar to the legitimate www.shellnigeria.com. The WIPO panel had no difficulty deciding that the registered domain www.shell-nigeria.com infringed the trade name of the genuine Shell Company.

Even the educational sector is not immune from this misuse. A case in point is that of a fraudulent website purporting to be the web site of the University of Nigeria, Nsukka, falsely inviting applications into fake degrees with prospects of scholarships, and unlawfully soliciting for payments to secure admission into the University. The website used was www.universityofnigeria.com, while the genuine web address of the university is www.unn.edu.ng. A public disclaimer had to be issued to warn the public of the fraud. [34] A related issue is the problem of cyber squatting, whereby domain name speculators, in bad faith, intentionally register domain names corresponding to famous

personalities, trademarks or other identifiers, with a view to selling them off at a profit to the person or company with legitimate claim to the name at a later date.

These issues give rise to a need for law reform to protect the rights of trade marks and business name owners from unauthorised use of the name or mark as a domain name, and to prohibit cyber squatting.[35] This is imperative given the increasingly popular practice of creating web sites for individuals, businesses and government agencies and departments, and the need to protect unsuspecting members of the public from the fraudulent antics of tricksters. Additionally, the establishment of a registration authority within the country for the assignment and management of domain names within the country code top-level domain, and rules for dispute resolution, revocation, assignment and other issues need to be promptly addressed.

3.0. International Legal Responses

In view of the increasing number of transactions in international trade which are carried out through electronic means, coupled with the borderless nature of electronic transactions, it has since been recognised that there is a need for some level of uniformity and harmonisation of legal norms which respond to the new technology. In this regard, international bodies like the International Telecommunications Union (ITU) and the United Nations Commission on International Trade Law (UNCITRAL) responded to some of the issues through the putting in place of model laws and Declarations which deal with different aspects of the challenges for legal regulation.

One of the notable responses is the adoption, in 1996, of the UNCITRAL Model Law on Electronic Commerce.[36] The Model Law sets out rules which aim at facilitating the use of electronic means of communication and storage of information as an alternative to paper-based methods of communication and storage of information. To this end, the Model Law provides for the legal recognition of data messages, which are also, in the absence of a contrary agreement, deemed to fulfil the requirements of writing, signature and original documents.[37] With regard to the formation of contracts in the electronic environment, the Model Law specifically provides that valid offers and acceptances can take place through data messages.[38] Admissibility in evidence and evidential weight of data messages are also guaranteed under the provisions. [39]

Also, in 2001, the UNCITRAL Model Law on Electronic Signatures (MLES) was adopted to build on the principles underlying the adoption of the Model Law on E-Commerce with respect to the fulfilment of the signature function in the electronic environment. [40] The underlying objective of the MLES, as may be deduced from the provisions, is the creation of functional legal equivalence between traditional means of signing or authenticating documents and electronic techniques. In furtherance of this objective, the MLES provides for equal treatment of signature technologies, regardless of the geographical location where such was issued, provided such signature is as reliable as appropriate for the data generated or communicated.[41] To ensure integrity, the MLES imposes duties on signatories, [42] certification authorities,[43] and relying parties, [44] with a view to striking the right balance among participants and ensuring the integrity of e-transactions. [45]

Another international organisation which has contributed to the ICT discourse, notably from a development perspective, is the International Telecommunications Union. It has done this especially through the fora of the two World Summits on the Information Society (WSIS) which took place in 2003 and 2005.[46] The 2003 summit facilitated the adoption of a Declaration titled "Building the Information Society: A Global Challenge in the New Millennium". [47] The Declaration emphasised the need to build a people-centred, inclusive and development-oriented Information Society, which facilitates the use of ICT to promote the development goals of the Millennium Declaration, including the eradication of poverty.[48] On its part, the 2005 Tunis Agenda focused on the importance of internet governance, cyber security- related issues such as privacy and data protection,[49] cyber crime,[50] consumer protection, [51] and ICT for e-governance.[52]

3.2. Existing and Emerging Legal, Policy and Institutional Responses to ICT in Nigeria

At present, Nigeria is in the process of updating its laws with a view to responding to the challenges of ICT both generally, and in the particular context of commerce and business. Government has also put in place a policy on information technology, while setting up a regulatory body to deal with ICT-related issues.

3.2.a. National Policy on Information Technology and NITDA

In 2001, the government put in place a National Policy on Information Technology. The policy targets the effective utilisation of information technology for the promotion of efficient national development, including for wealth creation and the encouragement of participation by Nigerians in software and IT development.[53] Responsibility for the implementation of the policy lies with the National Information Technology Development Agency (NITDA), whose main mandate is that of addressing the challenges and harnessing the opportunities presented by ICT.[54] To this end, Section 6 of the NITDA Act provides for the creation of a frame work for the planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of IT practices, activities and systems in Nigeria. This extends also, to the provision of universal access for IT penetration including rural, urban and underserved areas.[55]

However, the effective implementation of NITDA's mandate is conditional on government's ability to address one of the major challenges to universal access, i.e. stabilising and upgrading the power sector to ensure uninterrupted electricity supply. In the absence of this, reliance will continue to be placed on private sources of electricity, and the attendant high cost will further push up the cost of telecommunication services, thus making the goal of universal access a mirage.

Another mandate of NITDA is to consult with, and advice government at all levels on the need to have strategies in place for adoption and use of IT to enhance service delivery to the citizenry, as well as to businesses in the country. ICT is of particular importance in promoting efficient and accelerated service delivery for the enhancement of business and technological development, including foreign investment. Its use in land registries, Trademarks, Patents and Designs Registry,and Corporate Affairs Commission can facilitate registration, submission of statutory reports and online inspection and monitoring of compliance with regulations in convenient, timely, efficient and cost effective manner. Also, the putting in place of functional web sites with up-to-date information can facilitate access to business and regulatory information within and outside the country, while also promoting good governance and accountability.

The carrying out of this mandate does not however, appear to enjoy the desired degree of attention and success, in view of the fact that, with the exception of companies and business names registry which has been computerised, most other services still require physical presence and submission of paper documents. Even at the companies' registry, equipment has been known to breakdown, thus causing unnecessary delay, and threatening certainty and predictability in interactions with the registry. Ten years after the adoption of Nigeria's IT policy, there is a need for better commitment towards actualising the ideals of the policy in all its ramifications, to promote efficiency and convenience in government service delivery.[56]

3.2.b. The Cyber Security and Data Protection Agency Bill

At present, a Cyber Security and Data Protection Agency Bill is awaiting promulgation into law.[57] The Bill proposes the establishment of a body to be known as the Cyber Security and Information Protection Agency, to be charged with the duties of investigation of all cyber crimes, adoption of measures to eradicate the commission of cyber crimes, registration and regulation of service providers in Nigeria, and organisation of campaigns and other activities to create public awareness on the nature and forms of cyber crimes.[58]

Beyond these, the Bill also contains a number of provisions criminalising unlawful access to computers, unauthorised disclosure of access information or passwords, sending of fraudulent electronic mail messages and spamming, system interference and other forms of computer fraud and

data forgery. Subsumed within this body of provisions is a single clause criminalising the use of computers to violate any intellectual property rights protected under any law or treaty applicable in Nigeria, and making such punishable upon conviction, by payment of a fine of not less than one million naira or imprisonment for a term of not less than five years or to both such fine and imprisonment.[59] Similarly, any person who, on the Internet, intentionally takes or makes use of a name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or government agency without authority or right, or for the purpose of interfering with their use on the Internet by the owner, registrant or legitimate prior user, commits an offence, punishable on conviction by payment of a fine and/or term of imprisonment.[60]

The Bill is a welcome initiative which addresses some of the issues relevant to legal protection of intellectual property in the ICT environment. However, the criminalisation of such acts may not be sufficient to provide succour to right holders, who may be more interested in civil remedies which afford the opportunity of pecuniary relief and compensation to the wronged party.

3.2.c. The Nigerian Communications Commission's Guidelines for the Provision of Internet Service

One of the agencies whose work is related to ICT in Nigeria is the Nigerian Communications Commission, established under the Nigerian Communications Act, and charged with the responsibility of regulation of the communications sector in Nigeria, with a view to the provision of efficient and qualitative telecommunications services in the country.[61] In furtherance of its mandate, the Commission has put in place Guidelines for the Provision of Internet Service,[62] which apply to all Internet Service Providers (ISPs), i.e. providers of Internet access services or any other Internet Protocol based telecommunication services.[63]

Very relevantly, the Guidelines require ISPs to ensure that users are informed of any statements of cyber crime prevention or acceptable Internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution.[64] This is a very important provision which is capable of raising awareness about acceptable uses of the internet. ISPs are further required to cooperate with enforcement and regulatory agencies investigating cyber crime or other illegal activity, and must provide any service related information requested by the Commission or any other legal authority.[65] These include information regarding particular users and the content of their communications, while also contacting the Commission, in the event they become aware of any complaint or activity indicating Internet use for the commission of an offence.[66] While of vital importance, the possibility of encroachment on the fundamental right to privacy necessitates the putting in place of laws, rather than mere guidelines, which strike the right balance between law enforcement and protection of human rights.

3.2.d. The Prohibition of Electronic-Fraud Bill[67]

This Bill targets the prohibition of unauthorised access to computers, electronic manipulation of credit or ATM cards, trafficking in passwords and other forms of fraud in electronic transactions in Nigeria, including with regard to e-banking.[68] It provides for the registration of cyber cafes and requires them to maintain a register of users which shall be made available to law enforcement personnel whenever needed.[69] The Bill further prohibits the commission of crimes of unauthorised access;[70] computer manipulation;[71] sending of obscene or pornographic electronic messages;[72] sending of misleading electronic instructions regarding money or promissory notes and other forms of manipulation or falsification of e-data.[73] Financial institutions and their employees are criminally liable if they directly or indirectly engage in, or authorise the unlawful diversion of electronic mails, and they are also required to render monthly reports of attempted electronic fraud to the appropriate security agencies.[74] Furthermore, computer phishing, spamming, use of credit or debit cards and other access devices to defraud, as well as the manipulation of an ATM machine or Point of Sales

terminals with intent to defraud are all prohibited acts which are punishable by imprisonment terms and/or payment of fines.[75]

Beyond the above provisions however, legislative provisions needed to respond to the emergence of e-banking include that which covers liability and risk allocation between financial institutions and consumers, in the event of fraudulent withdrawals and transfers, particularly where the perpetrator cannot be traced. Thus, the responsibilities and liabilities concerning the degree of care in using ATMs and other forms of e-payment and e-banking services need to be clarified, and effective, accessible institutional mechanisms for responding to customer grievances need to be put in place, with back up reporting systems. All these are required to promote confidence in e-banking.

3.2.e. The Electronic Commerce (Provision of Legal Recognition) Bill

The Electronic Commerce (Provision of Legal Recognition) Bill of 2008 incorporates some of the provisions of the UNCITRAL Model Law on E-Commerce and E- Signatures. The Bill provides for the legal recognition of electronic commercial transactions where parties have, either expressly or by conduct, accepted to contract through electronic means.[76] Where there is such consent, the Bill provides that in the formation of contracts, the communication, acceptance and revocation of proposals may be expressed by electronic messages. [77] It also provides that the requirements of writing, signature and affixation of seals are deemed to be complied with when done electronically. [78]

This is a laudable provision which gives legal backing to the use of ICT for commercial transactions. However, to further adapt the law to the level of awareness and development in Nigeria, there is need to include adequate provisions on consumer protection, particularly in business to consumer transactions and even in business to business contracts as well. Thus, requirements concerning the disclosure of the physical address of the seller of goods, where complaints may be addressed, and the mechanisms for addressing grievances relating to non-performance, defective performance and other customer complaints need to be put in place. Where possible, a verifying/certification body also needs to be set up to protect ensure consumer protection is safeguarded from the possibilities of non-existent sellers with no physical existence beyond the online address or website.

3.2.f. The Electronic Communications and Transactions Bill

The Electronic Communications and Transactions Bill,[79] aims broadly at promoting the use of ICT for business, governance, and other activities.[80] To this end, the Bill contains a number of provisions aimed at the elimination of legal and operational barriers to e-transactions, including the admissibility and evidential weight of data messages;[81] promoting e-government services;[82] consumer protection, including in sale of goods transactions;[83] limitation of the liability of service providers;[84] and generally ensuring that e-transactions in Nigeria conform to international best practices by the development of a safe, effective and secure environment for all stakeholders including businesses, consumers and government.

4.0. Conclusion and Recommendations

This paper has examined some of the legal issues raised by the impact of ICT in commercial sectors in Nigeria. It has identified areas of impact in banking and business, domain name and trademarks, and the emergence of new crimes and metamorphosis of old crimes into new forms. Ongoing efforts by Nigeria to respond to some of these new legal issues have also been examined, and are largely commendable. This is because the full benefits of the ICT revolution cannot be fully enjoyed where there is no confidence in the validity, security and integrity of the medium, and transactions carried out thereon. A major way of achieving this is through up-to-date laws, to provide for certainty in the outcome of transactions carried out utilising this medium. In this regard, the unduly slow pace of legislation is regrettable, as these bills are yet to see the light of day several

years after their initial introduction and consideration by the National Assembly. One hopes that efforts will be made to address this delay, with a view to ensuring that laws are in place to deal with the different issues raised by ICTs in the commercial and other sectors.

While hoping for speedy promulgation however, it must be noted that the potpourri of upcoming laws still leaves untouched certain vital concerns, including the protection of public interest particularly as regards the safeguarding of constitutional rights to privacy. Also, the objective of simplicity and legal certainty may be defeated where there is a complex array of laws dealing with different aspects of the same issue. Thus, it is necessary to streamline and harmonise some of these evolving laws. In this regard, lessons may be learned from other jurisdictions which seem to favour a more unified and holistic legislative approach. Examples on the continent include South Africa, Zambia and Ghana, which all have in place legislation dealing holistically with diverse aspects of electronic transactions, quite unlike the highly fragmented emerging ICT laws in Nigeria.[85]

Also, with regard to administration and enforcement, the proposed creation of the Cyber Security and Data Protection Agency would further add yet another layer to the regulatory environment, where the the Nigerian Communications Commission, the National Information Technology Development Agency and the Economic & Financial Crimes Commission are already key operators. The question is whether there is need for such duplication, and whether government's scarce resources might not be better off being deployed to strengthen and train operators within the existing institutions. This is especially so, given the fact that there will be considerable overlapping between the functions of the agencies, which might further complicate the legal and institutional landscape.

Ultimately however, beyond the mere promulgation of laws, it is the actual implementation of the laws that will help to ensure the achievement of the desired results of protection, safety and integrity in ICT-related transactions. Thus, institutions need to be strengthened to become more proactive, while public awareness needs to be stepped up, with a view to seeing Nigeria and the continent on the path of socio-economic development and growth, riding on the wheels of new opportunities presented by the ICT revolution.

End Notes

[1] See for example, http://www.alibaba.com/countrysearch/NG/craft-supplier.html, where diverse local businesses promote and market their artwork, craft, African textiles, beads and other wares. For examples of projects facilitating the deployment of ICTs for agricultural development and entrepreneurship in Africa, see Gakuru M, Winters K & Stepman F, "Inventory on Innovative Farmer Advisory Services Using ICTs", (Forum for Agricultural Research in Africa, 2009) online at http://www.fara-africa.org/media/uploads/File/NSF2/RAILS/Innovative_Farmer_Advisory_Systems.pdf, last accessed 10th October, 2011.

[2] The term which is largely synonymous with information technology (IT)-See Edwards C. and Savage N., *Information Technology and the Law*, 2nd Ed. (Macmillan, 1990), p.1.

[3] Ibid.

[4] Ibid.

[5] According to latest internet usage statistics for Africa, as at 31st March, 2011, Nigeria had 43, 982,200 internet users, representing 28% of the population in Nigeria. The figure constitutes 37% of users in Africa. See Internet World Stats: Usage and Population Statistics, online at http://www.internetworldstats.com/stats1.htm, last accessed on 25th October, 2011.

[6] Discussed below

[7] See Vanguard News Report- "LUTH Begins Tele-Medicine Services", Reported in the Vanguard Newspapers of 17th February, 2009.

[8] Section 419 of the Nigerian Criminal Code, Cap C38, Laws of the Federation of Nigeria, 2004, which provides: "Any person who by any false pretence, and with intent to defraud, obtains from any other person anything capable of being stolen, or induces any other person to deliver to any person anything capable of being stolen, is guilty of a felony, and is liable to imprisonment for three years..."

[9]See the International Crime Complaint (IC3) Centre, online at http://www.ic3.gov/crimeschemes.aspx#item-13, last accessed 15th October, 2011

[10] According to the Internet Crime Report (2010), released by the Internet Crime Complaint Centre (IC3), over three hundred thousand complaints of online fraud were lodged with the centre in 2010 , making it the year with the second highest number of internet complaints since the establishment of the centre about ten years before. The report may be viewed at the IC3 website at http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf, last accessed on 15th October, 2011.

[11] See the Economic and Financial Crimes Commission (Establishment) Act (No 1) of 2004, Cap E1, LFN 2004. Among other functions, the EFCC is responsible for the investigation of all financial crimes including advance fee fraud, money laundering, counterfeiting, illegal charge transfers, futures market fraud, fraudulent encashment of negotiable instruments, computer credit card fraud, contract scam, etc. See generally, Section 6 of the EFCC Act. The EFCC is the Nigerian equivalent of the Serious Fraud Office in the UK, (see http://www.sfo.gov.uk/), and the

[12] Already, some training is being provided for the Economic and Financial Crimes Commission (EFCC), to equip it with skills to curb the menace of cybercrime, through the government itself, as well as through the efforts of some ICT companies like Microsoft, which is collaborating with these agencies with a view to sharing technical knowledge and best practices. Such collaborative efforts will contribute positively to the creation of a legal environment that encourages ICT business development in the country.

[13]See for e.g. http://www.timesonline.co.uk/tol/news/uk/article2907495.ece, and Bruce Schneier , Inside Risks, 179, Communications of the ACM, Vol. 48, No. 5, May 2005 online at http://www.schneier.com/essay-128.html

[14] See Report titled "Curbing Cybercrime in Nigeria: Microsoft Enlists Nigeria's Youth to Tackle Cybercrime," online at Microsoft Africa website at http://www.microsoft.com/africa/stories/curbing_cybercrime.mspx, last accessed December 15 2010.
[15] Ibid.
[16] ibid.
[17] See Bamodu G, " Information and Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian legal System and Judiciary", 2 (2004)*The Journal of Information, Law and Technology*, online at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/bamodu/, accessed 25th July, 2010
[18] See for example, the Sales of Goods Law, Cap S2, Laws of Lagos State of Nigeria, 2005
[19] See Section 30 Ibid.
[20] Another alternative is to upgrade the existing consumer protection law, i.e. the Consumer Protection Council Act, Cap C23,LFN 2004, to deal with these concerns.
[21] See Section 35 of the Sale of Goods Law, Lagos State.
[22] See the Consumer Protection Council Act, Cap C23, LFN 2004
[23] Recently, the Central Bank of Nigeria (CBN) issued a circular banning cash withdrawals exceeding N150,000 for individuals, and N1million for corporate bodies. See Thisday Newspapers of 29th April, 2011, online at http://www.thisdaylive.com/articles/cbn-limits-daily-cash-withdrawals-to-n150-000/90464/. See also the CBN website at http://www.cenbank.org/Out/2011/pressrelease/gvd/Revised%20QnA%20on%20CBN%20POLICY%20ON%20CASH%20WITHDRAWAL%20LIMIT.pdf, accessed, 21st October, 2011.
[24] Banks and other Financial Institutions Act (as amended), Cap B3, LFN 2004.
[25] See Par 3(b) of the CBN Guidelines on Electronic Banking in Nigeria, 2003.
[26] Unreported Suit No FHC/L/523C/08 of the Federal High Court Sitting in Lagos.
[27] Cap E14, Laws of the Federation of Nigeria, 2004.
[28] The newly promulgated Evidence (Amendment)Act, 2011 has however, now clarified the law by providing for admissibility of computer generated evidence.
[29] See Carolina R & Stokes S, *Encyclopaedia of E-Commerce Law*, (Thompson, Sweet & Maxwell, 2006) at par. 8-41
[30] Examples include "uk", "ng" or .com, which are often generally used by a large number of registrants.
[31] Encyclopedia of E-Commerce Law, op. cit.
[32] See generally, Halpern M & Mehrotra A, "From International Treaties to Internet Norms: The Evolution of International Trademark Disputes in the Internet Age", 21(2000), *U.Pa. J.of Int'l Econ. L*, 523 at 526-528.
[33] WIPO Arbitration Case No D2003-0821, available online at http://www.wipo.int/amc/en/domains/decisions/html/2003/d2003-0821.html, accessed 17th August, 2009
[34] See the disclaimer of the Nigerian Consulate _General in New York, online at http://www.nigeria-consulate-ny.org/News/re-fraudulent.htm. Notwithstanding that, as at the date of the last search on 22nd April, 2011, there was still a fake website of the university at http://unn.org.ng/, co-existing with the genuine web site is at http://www.unn.edu.ng/
[35] The US responded through the Anti-Cybersquatting Consumer Protection Act, 15 U.S.C., S1125(d) which was promulgated in 1999 to provide relief from these negative acts.
[36] The Model law is accessible at the website of the United Nations Commission on International Trade Law, at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html
[37] See Arts 5-8 of the Model law.
[38] See Art 11.

[39] See Art 9.
[40] See generally, the Preamble to the MLES. The Model law may be downloaded at the United Nations Commission on International Trade Law website at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html
[41] Reliability in this context, requires exclusive linkage of the signature data to the signatory, as well as the availability of safeguards to detect alteration or interference, and generally to ensure the integrity of the electronic signature-See Art 5&6 of the MLES.
[42] The main requirement here is the exercise of reasonable care to avoid unauthorized use of the signature creation data, and where this has been compromised, to expeditiously utilize reasonable efforts and means to notify possible relying parties. See Art 8
[43] Certification service providers, as intermediaries between signatories and relying parties, are required to exercise reasonable care to ensure that signature creation data was valid at or before the time when the certificate was issued-See Art 9.
[44] Relying parties are to take reasonable steps to verify the reliability of an electronic signature.See Art 10.
[45] See also the UN Convention on the Use of Electronic Communications in International Contracts of 2007.
[46] In Geneva and Tunis respectively. This work focuses mainly on the first phase of the summit, held in Geneva where issues such as the public domain and access to knowledge, including the role of intellectual property were discussed. The second phase, i.e., the Tunis summit, mainly tackled the issues of financial mechanisms and internet governance, and resulted in the Tunis Commitment of 18 November, 2005, online at http://www.itu.int/wsis/docs2/tunis/off/7.pdf; as well as the Tunis Agenda for the Information Society, online at http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf. The Civil Society Statement titled "Much More Could Have Been Achieved", is available online at http://www.worldsummit2005.de/download_en/WSIS-CS-summit-statement-18-12-2005-en.pdf, last accessed May 23, 2009.
[47] Document WSIS-03/GENEVA/DOC/4-E. The Declaration is available on the website of the International Telecommunications Union at http://www.itu.int/wsis/docs/geneva/official/dop.html, last accessed on the 13th of May, 2010.
[48] Par. 2.
[49] Par 39 of the Tunis Agenda
[50] Par. 40
[51] Par. 47
[52] Par. 48
[53] See Pars 3 & 4 of the Policy. The Policy is available online at http://www.nitda.gov.ng/document/nigeriaitpolicy.pdf
[54] See the NITDA website at http://nitda.gov.ng/, as well as the National Information Technology Development Agency Act, 2007
[55] See Section 6(a) of the NITDA Act.
[56] NITDA has however made some progress in the facilitation of access to digital works in Nigerian universities, through its Virtual Library Project. For further discussion on ICT and education, see, Oyewunmi A.O., "Digital Technology and the Educational Sector- A Perspective from Nigeria", Paper presented at the Annual Conference of the Association for the Advancement of Teaching and Research in Intellectual Property", hosted by the Faculty of Law, University of Stockholm, Sockholm, Sweden 23-26th May, 2010. (Upcoming for Publication)
[57] Titled "A Bill for an Act to Provide for the Establishment of the Cyber Security and Information Protection Agency Charged with the Responsibility to Secure Computer Systems and Networks and Liason with the Relevant Law Enforcement Agency for the Enforcement of Cyber Crime Laws, and for Related Matters" (2008).

[58] See generally Clause 4 of the Bill.
[59] See Clause 21 of the Bill.
[60] See Clause 19.
[61] Section 3 of the Nigerian Communications Commission Act, Cap N97, Laws of the Federation of Nigeria, 2004
[62] The Guidelines are published pursuant to Section 70(2) of the Nigerian Communications Act, and may be accessed on the NCC website at http://www.ncc.gov.ng/
[63] See the Opening Paragraph of the Guidelines.
[64] See Para 5 of the Guidelines. Other authorities, in the context of the Guidelines, would include the Economic and Financial Crimes Commission and the Central Bank of Nigeria.
[65] Para 6 of the Guidelines.
[66] Ibid. On-going efforts to put in place a registration scheme for owners of telephone lines, internet subscribers and other users of the ICT media who act through the medium of ISPs will enhance the efficacy of these provisions, particularly where there is a need to trace perpetrators of illegal acts carried out online.
[67] Of 2008
[68] See Clause 1 of the Bill.
[69] Clause 4
[70] Clauses 1-3
[71] Computer manipulation includes unauthorised destruction, abortion or misdirection of electronic mails involving conveyance of money or valuable information- See Clauses 7&8
[72] Clause 16
[73] Clause 18
[74] Clauses 25-28
[75] Clauses 39-41
[76] See Clause 2 of the Bill
[77] See Clause 5.
[78] Clauses 6&7 of the Bill.
[79] Of 2009
[80] See Clause 2
[81] See generally, Part II, Clauses 4-19 of the Bill.
[82] Clauses 20-21
[83] See Part IV, Clauses 22-28
[84] Clauses 29-32
[85] See the South African Electronic Communications and Transactions Act No 25 of 2002, the Zambian Electronic Communications and Transactions Act of 2009 and the Ghanaian Electronic Transactions Act No 772 of 2008, as amended by the Electronic Communications Amendment Act, No 786.