International Journal of Business & Law Research 3(2):110-123, April-June 2015

© SEAHI PUBLICATIONS, 2015 **www.seahipaj.org** **ISSN: 2360-8986**

INFORMATION TECHNOLOGY AND THE CHALLENGES FACING THE LEGAL PROFESSION IN NIGERIA[1]

ODOH, Ben. Uruchi

ABSTRACT

Information Technology is an outcome of the nexus between the Computer Technology and the Communication Technology which has grown as silver fiber in Nigeria. Information Technology represents the fourth generation of human communication after sight, oral and written communications.

This paper seeks to appraise the challenges facing the legal profession in Nigeria because of want of Cyber Laws. The enormous benefits derivable from the use of information technology in administration of justice in Nigeria are highlighted. The paper also elaborated on the relationship between the law of evidence and information technology with clear case studies. The paper highlights the loopholes in the existing Nigeria laws and recommends the way forward

Keywords: Cyber crime, cyber laws, information technology, Law of Evidence, Nigeria

INTRODUCTION

With appearance of Information Technology (IT) many advanced countries have switched over from paper based commerce to e-commerce and from governance to e-governance[2] In today's scenario, Information Technology is all pervasive in every phase of our day to day life. Prominently in the service sector involving communications, railways, airways, scientific establishments, banks, universities, business establishments, in our homes and in industrial growth, the inescapable influence is apparent. The internet, as with all path-breaking technological developments gives us all the opportunity to act as a global community; advertise and operate across all frontiers; over boarders and beyond the control of any national government.

In Nigeria, the Information Technology revolution is spawning new businesses and forcing old ones to either change or die. Thus, creating and harnessing some opportunities and challenges at the same time. Therefore, it is of immense credit to the Nigerian government and also, in particular, the National Information Technology Development Agency (NITDA) that in the past few years much efforts has already gone into addressing some of the challenges and harnessing some of the opportunities presented by advancements in Information Communications Technology generally and, especially, as a result of the development and now widespread use of the internet and the World Wide Web. The introduction of the National Information Technology Policy and establishment of NITDA are much welcome developments evidencing the government's commitments in this area and the work that NITDA has already done, for example, in sponsoring the draft Electronic Transaction Bill, currently going through the Legislative Processes, in encouraging capacity building and introducing the Mobile Internet Units among other things are encouraging[3].

Some of the advantages of attending the global information communication technology revolution include productivity savings on time and costs, speeding up and facilitation of transactions, access to superior and more up- to- date information, easier and cheaper communication both domestically and internationally and, in the particular context of e-commerce, access to a wider, indeed, a global economic market at relatively little cost.

---

[1] **Odoh Ben. Uruchi, LL.M; BL; CDRS; ACIArb(UK); pnm**, Coordinator, Legal Clinic / Lecturer, Department of Public Law, Faculty of Law, Nigeria Police Academy, Wudil, Kano State, Nigeria. E-mail: benodoh@yahoo.ca.

[2] BB Nanda and RK Tewari, *'Cyber Crime - A Challenge to Forensic Science'*, The Indian Police Journal, (2000) 102

[3] G Bamodu, *'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigeria Legal System and Judiciary'* (E-Judiciary Conference, Abuja, March 22 - 23, 2004).

Benefits of Information Technology to the Legal Profession

With regards to Information Technology, particularly from the perspective of developing countries such as Nigeria, the benefits are enormous. The United Nations even recognized that Information Technology could be a contributing factor to achieving its Millennium Development Goal of reduction of poverty and economic development generally.[4]

In the Legal Profession, however, the essential benefits of Information Technology are hereunder:-

- It facilitates the storage, retrieval and dissemination of vital legal information for the successful pursuit of legal research and study;
- Facilitates the performance of routine processes like the amendment of law, indexing and abstracting services;
- Serves as a link among the various legal education institutions; as well as foster necessary cooperation and working relationship among them. This would also facilitate intellectual resource garnering and sharing;
- Assist in the formulation of legal studies syllabus that would have universal acceptability and applicability;
- Internet access to judicial decision: With basic Information Technology facilities like a personal computer, a dial-up or wireless connectivity, a lawyer can now access judicial decisions of the Supreme Court of Nigeria, and all other courts of superior records' judgment. Online legal databases like Lexis/Nexis and Westlaw are already a practical experience of legal professionals in developed countries;
- Documentation is a cordial aspect of the legal institution responsibilities. The legal process is undoubtedly documentation - intensive. Whether in drafting agreement for clients, or legislative drafting or litigations, preparing writs or even judges writing their judgments;
- Litigation Support Service: Information Technology is relevant to the lawyers' management and control of the diverse documents which they have to master in order to advance and prepare their clients' case. It relates to efficient use of Information Technology systems for the efficient storage and speedy retrieval of such documentation;
- Information Technology system allows lawyers to work on many documents simultaneously while at the same time downloading materials from the internet. He can copy and paste one document to another or from one section document to another;
- ICT is also relevant in the area of basic text retrieval, use of CD-ROM systems and quicker and more qualitative service to clients and cooperation between counsel, clients, courts and law investigation and enforcement institutions;
- Electronic Communication: Digital technology provides the platform for lawyers to:-
    - ✓ Transmit and receive messages from clients, colleagues and the court system,
    - ✓ Gain access to the internal know-how of the institutional memory of a law firm and provide access to information on specific matters[5]

Information Technology in the Administration of Justice in Nigeria

Almost all the courts have not fully appreciated the advantages of information technology. Record of proceedings are taken in long hand. Even the attempt at judicial performance evaluation by the National Judicial Council is not automated. A spread sheet is used and the data is manually generated. This has constituted a very serious setback to the efficiency of the Judiciary in Nigeria.

In realization of these problems, the National Judicial Council has recently set up a Judicial Information Technology Policy Commission, headed by Hon. Justice Kashim Zanna, the Chief Judge of Borno State. The task of the Commission is to explore ways on how the judiciary will be automated in respect of all court processes. The plan is even to link up prison inmates in video conference for purposes of

---

[4] Economic Commerce and Development Reports (UNCTAD 2002).

[5] JE Owoeye, *'Information Communication Technology (ICT) Use as a Predictor of Lawyers' Productivity* (1998) <http://digitalcommons.unl.edu> accessed 10 March 2015.

administration of justice. Such that, in certain circumstances, the accused might not be required to be physically present in the court room for trial.

The Commission will draw up training programmes for Judges and other court officials. We hope that this Commission will take into account the statutory powers of the National Judicial Institute. At the completion of the assignment of the Commission, it is hoped that Judges will have legal assistants who are IT-compliant. Case management system will be computerized. The library and reference materials will be scanned and digitalized.

Information Technology and Administration of Justice

The security concerns, computer abuse and the side effects of information technology, have moved to the forefront of the consciousness of law enforcement agencies in Nigeria. It is pertinent to note that the rules of law in every existing legal system are predicated upon and tailored to traditional means of communication though they have been sufficiently adaptable to accommodate developments and advancements as they occur, for example from oral communications to exchanges via paper medium, telephone and facsimile. This adaptability of law means that fortunately, the challenges arising from new forms of communications especially through information technology are not insurmountable, though they have to be met carefully crafted policies and rules that reflect the unique characteristics of these new forms, that do not stifle their growth and that creates a positively enhancing environment for maximizing their benefit.[6]

As mentioned earlier, it is unfortunate that Nigeria is one of the countries in the world that is yet to legislate cyber laws, although severally unsuccessful attempts have been made in recent times at providing the legal framework for regulating the activities in Nigerian cyberspace[7]. We are not unmindful of the fact that we have the Advance Fee Fraud Act, 2006; Criminal Code; Penal Code, Economic and Financial Crimes Commission (Establishment) Act, 2004; Evidence Act, 2011 etc. These laws were not designed to handle the kind of cyber threats we are currently facing in Nigeria.

Nevertheless, there is an Electronic Transactions Bill that is presently going through the legislative processes in Nigeria[8]. The aforementioned bill addressees issues such as the formation and validity of electronic contracts as well as the issue of electronic signatures. Beyond rules related to electronic contracting, however, there are many other matters that will have to be addressed by the legislature at some point in future[9]. These include, among others, whether a regulatory or licensing scheme should be introduced for the providers of some types of internet service such as, for example, certification service providers, or whether they could be left to a system of self regulation, say under a code of conduct; whether or what type of regulation should be put in place concerning the issuing and distribution of electronic money in smart cards and other media; and to what extent should the contents of websites be regulated particularly in terms of offensive material or material contrary to public policy[10].This paper also considers some other specific areas where the law will need to strive to keep up with developments in information communications technology and how these developments will impact the activities of economic actors, contracting practices and general inter-personal exchanges and transactions. It also sought to point out challenges facing the legal profession as a result of the birth of information Technology, and the areas of law that the courts should be alert to in the administration of the law and adjudication of disputes that have connections to information communications technology usage, so as to improve the foundation growth of electronic commercial transaction in Nigeria.

---

[6] G Bamodu, op. cit.

[7] These include: The Cyber Security and Data Protection Agency Bill (2008); Electronic Fraud Prohibition Bill (2008); Economic and Financial Crimes Commissions Act (Amendments) Bill (2010).

[8] We pray that this Bill should not be slaughtered on the altar of legislative arguments and debates.

[9] See also O Soyele, *'The Internet & emergent Regulatory Legal Framework : A Selective Appraisal'*, (2000) 4 Modern Practice of Finance& Investment Law 166; AO Salu, *'Cyberlaws -Its (sic) Application and Enforcement in Nigeria'* (1998) 2 Modern Practice of Finance & Investment Law 10

[10] There is currently a Cybercrime Bill before the House of Representatives. It has undergone first and second reading. This Bill when passed to law will address types of criminal activities that are computer related.

The Law of Evidence Relating to Electronic Documents

Information communications technology also poses some challenges for the courts in terms of the use of electronic documents as evidence. In ordinary circumstances, that is, without the use of certification for example, electronic documents have a particular vulnerability in that deliberate or in-deliberate modifications may be difficult to detect if not altogether undetectable. In addition, most electronic documents tendered are likely to be copies of the original data contents of the document in terms of the way information systems, especially network systems, work. These factors pose challenges for courts in terms of some key concepts underlying the admissibility of evidence such as reliability, the best evidence rule, the rule on hearsay and generally in terms of the authenticity and integrity of the document[11]. Even if an electronic record satisfies the tests that may be laid down for its admissibility, there is the further question of what weight is to be attached to such evidence.

The best evidence rule requires the person tendering evidence to tender the best evidence possible which, in relation to documents, means the original document or that which is closest to it. Electronic documents do not really have an 'original' in a meaningful sense being invariably, in the visually represented form, copies or even copies of the initial data input. The hearsay rule, subject to permitted exceptions, prevents the use of second-hand information as opposed to information by an eyewitness who can be cross-examined on the information. Thus, a document purporting to represent the statement of a person who is not called as a witness to tender the document and be cross-examined on it is likely to be caught by the hearsay rule. Finally, courts would also need to be satisfied of the reliability of the document in the sense that it is what it purports to be and of its integrity in the sense that it has not been tampered with or modified from its original state unless of course it is being tendered as a modified version.[12]

In Nigeria, the inestimable benefits of the various advancements in information and communication technologies have until the enactment of the new Evidence Act in 2011 remained a matter of much debate and judicial uncertainty[13]. Tendering of electronic mails ("emails") for example are usually as contentious and acrimonious as the litigation itself, with the opposite party usually relying on the hearsay rule, among other forms of objections under the old Evidence Act 2004, to prevent the admission of such electronically generated evidence. The enactment of the Evidence Act, 2011 has attempted to correct some of the difficulties that the admissibility of electronically generated evidence do encounter in Nigerian Courts.

It is pertinent to note that relevant to the admissibility of electronic evidence are the common rules governing the admissibility of evidence generally. Under Nigerian Law, facts which are in issue, with the facts which are relevant to the facts in issue, are generally admissible in evidence[14].

In the Evidence Act, Cap. E14, Laws of the Federation of Nigeria 2004, which is now repealed, technologically generated evidence was argued to offend some of the following general rules of evidence:

- The issue of the custody and the reliability of the evidence tendered if it is not the original document;
- The best evidence rule which requires that a party must produce the original document during a trial or where the original document is not available, secondary evidence of it in the form of a copy, with other corroborating notes, etc, must be produced;
- The rule against the admission of hear-say evidence which forbids witnesses giving evidence on facts that they do not directly or personally witness or know about.

Fortunately, the general basis for the admissibility of documentary evidence has not radically changed under the Evidence Act 2011 as documentary evidence is still mostly admissible where the original hard

---

[11] G Bamodu, op. cit

[12] ibid

[13] Oserogho & Associates, *'Legal Alert: Admissibility of Electronic Evidence'*, (2012) <http://oseroghoassociate.com> accessed 9 March 2015.

[14] *Evidence Act 2011, section 4 (Herein referred as the Act)*

copy of such a document is produced in a Court of Law[15]. Section 83(1) of the Evidence Act 2011, provides:

> *(1) In a proceeding where direct oral evidence of fact would be admissible, any statement made by a person in a document which seem to establish that fact shall on production of the original document, be admissible as evidence of the fact if the following conditions are satisfied -*
> *(a) If the maker of the statement either -*
> *(i) had personal knowledge of the matters dealt with by the statement; or*
> *(ii) where the document in question is or forms part of a record purporting to be a continuous record made the statement (in so far as the matters dealt with by it are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had, or might reasonably be supposed to have personal knowledge of those matters; and*
> *(b) if the maker of the statement is called as a witness in the proceeding:*
> *Provided that the condition that the maker of the statement shall be called as a witness need not be satisfied if he is dead, or unfit by reason of his bodily or mentally condition to attend as a witness, or if he is outside Nigeria and it is not reasonably practicable to secure his attendance, or if all reasonable efforts to find him have been made without success.*

The Evidence Act 2011 has however expanded this basic general rule to enable the admission of electronically generated documents under certain conditions which are enumerated hereunder:

Explanatory Memorandum of the Evidence Act, 2011

In its explanatory Memorandum, the Evidence Act, 2011 repealed the 2004 Evidence Act, Cap. E14, Laws of Federation of Nigeria, and enacted a new Evidence Act 2011 which applies to all judicial proceedings in or before any Court of Law in Nigeria.

Conceptual Clarifications of Information Technology related terms in the Evidence Act 2011

The word "*Document"* is defined in the Evidence Act 2011. Section 258 (1)(d) describes a document, to include *"any device by means of which information is recorded, stored or retrievable including computer output".*

A" *Computer*" is in turn described to be *"any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process."*

Hearsay and Electronic Evidence

Under the Evidence Act 2011, one of the exceptions to the hearsay rule of evidence, which hearsay evidence will otherwise be inadmissible under the old repealed Evidence Act, 2004 is the provision that where even though the maker of the evidence cannot be called to give primary evidence on the *"hearsay evidence"*, such evidence is established to have been made and kept contemporaneously in an electronic device, in the ordinary cause of business or in the discharge of a professional duty or in acknowledgement, written or signed, of the receipt of money, goods, securities or of property of any kind[16]. Where the statement and the recording of the transaction are not instantly contemporaneous, they must occur such that a Court of Law will consider it most likely that the transaction was at the time of the record, still fresh in the memory of the maker of the recorded statement[17].

Admissibility of Statement in Documents Produced by Computers

Section 84 of the Evidence Act 2011 provides that a statement contained in a document produced via a computer, which statement is relevant to the facts in issue, is admissible as evidence on the fulfilment of the following condition precedents:-

---

[15] ibid, section 83 (1).
[16] *The Act, section 41*
[17] Ibid

(a) The computer from which the document was produced, was used regularly during the material period to store electronic information or to process information of the kind stated in the document;

(b) The computer from which the document was produced also had stored in it other information of the kind contained in the document or of the kind from which the information contained in the document was derived;

(c) That throughout the material period, the computer was operating properly; and where it was not, evidence must be provided to establish that during the period when the computer was not operating properly, the production of the document or the accuracy of its contents were not compromised or affected;

(d) That the information in the statement is reproduced or derived from the information supplied to the computer in the ordinary course of the activities in question[18].

Certificate Authenticating Computer Generated Documents

Where it is desirable to give a statement in evidence by virtue of Section 84 of the Evidence Act 2011, a Certificate identifying the document containing the statement and describing the manner in which the document was produced, with the particulars of any device involved in the production of the document, signed by a person occupying a responsible position in relation to the operation of the electronic device, shall be primary and sufficient evidence of the matters stated in the Certificate[19].

Primary and Secondary Electronic Evidence

Primary documentary evidence is the original document itself produced for the inspection of the Court. Secondary evidence is the direct opposite of primary evidence. Section 86 (3)of the Evidence Act 2011 provides:- *"Where a number of documents have all been produced by one uniform process as in the case of printing, lithography, photography, computer or other electronic or mechanical process, each of such documents shall be the primary evidence of the contents of all the documents so produced by this one uniform process".*

Proof of Electronic Signatures

An electronic signature will satisfy the legal requirement that a document must be signed where the electronic signature shows that a procedure was followed whereby the person that executed a symbol or followed some other security procedure for the purpose of verifying that an electronic signature was made to an electronic record, actually followed such an established procedure. Section 93 provides thus:

(1) If a document is alleged to be signed or to have been written wholly or in part by any person the signature or the handwriting of so much of the document as is alleged to be in that person's handwriting must be proved to be in his handwriting.

(2) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed; an electronic signature satisfies that rule of law or voids those consequences.

(3) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

Admissibility of Other Forms of Evidence

Other forms of evidence admissible under the Evidence Act, 2011 are hereunder:-

- Books of Accounts: Entries in books of accounts or electronic regularly kept in the ordinary course of business are admissible whenever they refer to a matter into which the court has to

---

[18] Oserogho & Associate, op cit.

[19] Evidence Act, 2011, section 84 (4) (a)(b)(i)&(2)

Inquire[20]. However, there is a caveat that such statements alone shall not be sufficient evidence to discharge any person of liability[21].

- Public Books: Any entry in any public or other official books, register or record including electronic records made by a public servant in the discharge of his official duties, stating a fact in issue or a fact relevant to a fact in issue, are now admissible evidence under the provision the Evidence Act 2011[22].

The Challenges of Electronic Evidence and the Burden of Proof in Civil Cases

The burden of proof in civil cases lies on the person who would fail if no evidence at all were given or provided on either side to establish a claim or claims[23]. Also remember that the burden of proof in civil cases is discharged on the balance of probabilities and not beyond reasonable doubt which is the burden of proof required in criminal proceedings.[24]However, on presumption and estoppels, one of the presumptions under the Nigerian law of Evidence is that an electronic message forwarded by the originator of the message through an electronic mail server corresponds with the message as fed into his computer for transmission; but the court shall not make any presumption as to the person to whom such message was sent without corroborating evidence[25].

In Lagos State, for example, there are however no direct provisions in the High Court of Lagos State (Civil Procedure) Rules 2012[26] regulating the electronic filing and service of court processes. All originating processes are to be printed in A4 paper of good quality[27]. The Rules also requires personal service of all court processes and where personal service is not possible, physical hard copies with the leave of court or judge can be served by pasting at the last known address of the party with the Process Server required to swear to an Affidavit of Service exhibiting the acknowledgement of the court process that was served[28]. Real evidence are tendered during trial.[29] Where depositions are required, they must be written with the witness available for examination and cross-examination in open Court. The Rules however allows the admission of official copies of court processes filed at the High Court as original copies of the filed court processes[30].

A Selective Assessment of Case Laws on Electronic Evidence in Nigeria

Firstly, the earliest and most commonly referred to case on the admissibility of electronic evidence in Nigeria is the Nigerian Supreme Court decision in *Esso West Africa Inc. v. T. Oyegbola*[31] where the Supreme Court said obiter that *"The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer"*. The document that called for the decision of the Court in the Esso West Africa Inc[32] matter was one that was signed in quadruplicate with carbon copies through one single process with the original copy. The Supreme Court ruled on this matter, relying on the old Section 93 of the 1945 Evidence Act to hold that where a number of documents have been made by one single act of the use of carbon paper, each of such document so reproduced is primary evidence of the other quadruplicate copies.

---

[20] The Act, section 51.
[21] ibid, section 53
[22] The Act, section 52.
[23] Ibid, section 132.
[24] Ibid, section 134.
[25] Ibid, section 153 (2).
[26] Herein referred to as Lagos Civil Procedure Rules
[27] Ibid, order 6
[28] Ibid, order 7
[29] Ibid, order 32 (rule 1 and 4)
[30] Ibid, order 32 (rule 6)
[31] (1969) 1 NMLR 194
[32] Supra

The *Esso West Africa Inc. v. T. Oyegbola*[33] case was referred to in the case of Yesufu v. A.C.B.[34] where the document that was tendered with objection by opposing Legal Counsel, was a bank statement prepared by a Machinist from the Ledger Card of the Respondent Bank; the Machinist obtained the entries from the Respondent's Bank day-to-day Vouchers. The bank officer that tendered the statements did not personally prepare the statements or verify that the statements were correct. Objection was raised to the admissibility of the bank statements on the grounds that the existence of a banker's book from which the entries were extracted was not established neither was the custody and control, with the examination of the original entries established, before the lower Court admitted the bank statements. The Supreme Court held in the *Yesufu v. A.C.B*[35]case that the admission of the bank statements which entries were derived from the day-to-day vouchers of the Respondent bank did not qualify, without other supporting oral evidence, as a bankers book and therefore offended the provisions of the Evidence Act[36].
The Supreme Court did however refer to the obiter in *Esso West Africa Inc.* (supra) and said as follows *".... it would have been much better, particularly with respect to a statement of account contained in a book produced by a computer, if the position is clarified beyond doubt by legislation as has been done in the English Civil Evidence Act, 1968."*

It is the provision of Section 5 of the English Civil Evidence Act, 1968 regarding the condition precedents for the admissibility of documentary evidence produced by a computer that was finally adopted in the 2011 Evidence Act as counselled by the Supreme Court in the 1976 case of *Yesufu v. A.C.B* (supra).
Secondly, in another Supreme Court decision of *Elizabeth Anyaebosi v. R. T. Briscoe*[37], the statement of account upon which the claims in this suit was reproduced and upheld were stored in and reproduced from a computer. This statement of account was admitted in evidence without objection at the High Court and in the Court of Appeal. The Supreme Court on further appeal upheld the judgements of the lower Court to the effect that the computerised statements of account were admissible under Section 96 (1) and (2) of the Evidence Act, 1945 which section allows the admission of secondary evidence upon the fulfilment of certain condition precedents. This is in contrast with some kind of evidence which are absolutely inadmissible under Nigerian law.
Thirdly, in the case of *Oguma Associated Companies (Nig.) Ltd v. I.B.W.A Limited*[38] the Nigerian Supreme Court said obiter that Nigerian Courts need to become circumspect in interpreting Section 96 of the 1945 Evidence Act in the light of modern day banking procedures and gadgets such as computers which are now increasingly used by businesses. The Supreme Court also said obiter that there are certain types of evidence such as hearsay evidence, unstamped and unregistered documents which are inadmissible in Law and which cannot be admitted by consent of the parties. It was held in this case that while the correctness of whether the statement of account was rightly or wrongly rejected by the lower Court as there was no cross-appeal on this point, other admissible and uncontradicted evidence were provided to entitle the Respondent Bank to judgment. This appeal was accordingly dismissed.
Fourthly, there are notorious typographical errors in the Evidence Act 2011. These typographical errors will have to be corrected at the first opportunity of any amendment to this legislation[39].
The subject of evidence and the admissibility of documents have remained a very technical subject for many years. The Evidence Act 2011 continued with this tradition by failing to simplify the evidence rules for both legal practitioners and non-legal practitioners, to easily read and understand the provisions of this Law.

---

[33] Ibid
[34] (1976) 4 SC 1 (Reprint) 1 @ 9 - 14.
[35] Ibid
[36] Evidence Act 1945, section 96 (1)(h).
[37] (1987) 3 NWLR (part 59) 84 @ 96-97.
[38] (1988) 1 NSCC 395 @ 413.
[39] See examples of these errors in Sections 71 and 206.

Draconic Provisions in the Cybercrime Bill 2013: A Selective Appraisal

The bid by the Federal Government to make a law for the regulation and interception of electronic communications is raising alarm in many quarters across the country[40]. The bill for the law, sent by President Goodluck Jonathan to the National Assembly, is known as Cybercrime Bill. Although it is designed as a comprehensive legislation for the protection of critical national information infrastructure, computer systems and electronic communications against attacks by hackers, the bill nevertheless empowers security agents to intercept, record and seize electronic communications between individuals, especially during criminal investigations. Security officials can also intercept and record personal emails, text messages, instant messages, voice mails and multi-media messages.

The bill also provides for the ultimate punishment, the death penalty, for those who hack into critical national information infrastructure if such hacking results in a death or a minimum of 15 years imprisonment if no death results. The punishment for cyber terrorism is life imprisonment. The production and distribution of child pornography would lead to at least 10 years imprisonment or a N20 million fine. Paedophiles will get years in jail, N15 million fine or both. The bill is being touted as "an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cyber crimes in Nigeria".

The reason it has been difficult passing this legislation is the nature of the subject-matter. Although the law is badly needed to regulate electronic funds transfers, check internet scammers and intercept communication by terrorists, the fact that it can be used by the government and security agencies to violate the privacy of citizens by spying on and recording their personal communications such as emails, text messages and phone calls, makes it controversial. This is more so as the internet is now a major tool for political communication, propaganda and mobilization.

The anxiety over Cybercrime Bill 2013 has, however, been heightened by some of its draconian provisions. For example, section 13 stipulates a 3year jail *for "anyone who intentionally propagates false information that could threaten the security of the country and that is capable of inciting the general public against the government through electronic message."* This appears to be a replication of Decree No. 4 of 1984.

The bill also states that its operations can be invoked without recourse to issuing of court warrants, where the need for 'verifiable urgency' is established. This for example, indicates that Section 22 of the Bill which provides for interception of electronic communication and issuance of orders to service providers to record and assist 'competent authorities' with the collection of content data of specified communications, could be enforced without court orders or warrants, if 'verifiable urgency' can be established. This is, indeed, worrisome. Nevertheless, there are so many reasons why Nigeria and all other countries need to regulate cyberspace. The severity of harm which can come through the internet is incalculable.

The Legal Validity of Electronic Contracts and its Challenges in Nigeria

There two common ways of entering into contracts on the World Wide Web (www) are by exchange of e-mail or by Web-click, whereby a shopper visits the website of an e-merchant and selects the item(s) or orders the service that he is after.[41] There are certain preliminary considerations that apply to both types of contract. Such considerations include whether a valid contract can be concluded wholly electronically at all and, if it can, how can such a contract be authenticated and attested by a legally valid signature if necessary and also what is the legally acceptable proof of the contract?[42]

It seems taken for granted that a contract can be concluded validly over the World Wide Web. In general, this is true. In the common law tradition to which the Nigerian legal system belongs, apart from a few specific exceptions, a contract may be concluded by any means including writing, orally or by conduct.

---

[40] Editorial, *'Before the Cybercrime Bill becomes Law'*, Daily Sun (Nigeria, 13 March, 2015) 19.

[41] Apart from open network transactions as on the Internet/WWW, contracts may be entered into on closed electronic networks especially via electronic data interchange (EDI) although even EDI can be delivered on the Internet platform

[42] G. Bamodu, op cit @ 12

Other countries may require that contracts, especially involving above a set amount of money, should be in or evidenced in writing. In such a case the question that arises is whether an internet contract satisfies the requirement. Under pre-internet era traditional law, such a contract would not normally satisfy the requirement of writing because that would require visible representation in tangible form whereas computer data is strictly speaking intangible. This problem has been largely resolved in many countries through the passing of legislation that operate a 'functional equivalence' approach of giving the same legal effect to data messages as paper based documents. Incidentally, the legislation in different countries exhibit similarities in part because most can trace provenance in some way or other to an instrument of the United Nations Commission on International Trade Law (UNCITRAL).[43]

It is very germane to note that the current *Draft Electronic Transactions Bill* being sponsored by NITDA follows the same pattern by providing[44]that information shall not be denied legal effect solely on the grounds that it is in the form of an electronic document and that it is not contained in the electronic document purporting to give rise to such legal effect but is merely referred to in the document.

More so, legislation in different countries has also dealt with the question of effecting electronic signatures validly. In effect, it is now generally accepted that signature can be effected electronically which may be as simple as typing the signatory's name at the end of an e-mail with the intention to authenticate the document or scanning a regular signature onto an electronic document or using an electronic signature mechanism such as one that captures and encrypts biometric data from manual signatures. Other secure methods of effecting signatures electronically have been devised using encryption technology. These are called *'digital signatures'* and involve the use of a *'key'* (mathematical algorithm) assigned to the signatory uniquely to encode information emanating from that party. It mostly takes the form of asymmetrical encoding where one key (a private key) is used for the encoding and another key (a public key) is used for decoding. Generally speaking, legislative provisions on electronic signatures tend to give the more secure forms such as digital signatures ('advanced electronic signatures') greater recognition at law especially with regard to admissibility in evidence.

The *Draft Electronic Transactions Bill* paves the way for the legal recognition of electronic signatures in Nigeria by providing[45] that where an existing law or regulation requires the signature of a person, that requirement is met in relation to an electronic document by a signature as defined[46] in the prospective Act. The definition of 'signature'[47] is technology neutral and does not distinguish between ordinary electronic signatures, which may be as simple as a typed name in an e-mail or other electronic communication, and the more advanced and secure digital signature. This is understandable to some extent because the legal framework for the provision of certification services, often a necessary part in the use of digital signatures, has not yet been established and perhaps, more practically, also because there are arguably not many certification service providers within Nigeria as yet though by the nature of the Web, naturally, the services of providers abroad could be possibly obtained online.

In Nigeria in particular, the use of the certainly more secure digital signatures should be strongly encouraged because of the potential for fraud. It is sometimes said that on the World Wide Web 'no one knows you are a dog' because it is very easy for a person using the Web to disguise their identity and to hide behind aliases as in the case of *Shell International Petroleum Co. v Allen Jones*[48]. The use of digital signatures provided by a certification service provider will ensure that at least some steps would be taken

---

[43] known as the *Model Law on Electronic Commerce* of 1996

[44] Section 1 of the current draft

[45] Ibid, section 4

[46] 'Signature' is defined in the Draft section 15 as meaning 'data in, affixed to or logically associated with, a document which may be used to identify the signatory in relation the document and to indicate the approval of the signatory of the information contained in the document.'

[47] It is considered that in both the draft sections 4 and 15, it would be better off to refer specifically to *electronic* signatures rather than risk potential confusion by the use of the generic 'signature'.

[48] WIPO Case No. D2003-0821 of 18 December 2003, <http://arbiter.wipo.int/domains/decisions/html/2003/d2003-0821.html> accessed 5 March, 2015.

to verify the identity of the person putting forward the relevant electronic document and signature. It will also give some assurance as to the authenticity and integrity of the document and the signature.

With regards to the formation of electronic contracts, the basic rules concerning the formation of a contract apply equally to electronic contracts. Thus, among other things, there must be an 'offer' which is met with a matching and unconditional 'acceptance'. With regard to e-mail contracts it might be relatively clearer, possibly, to identify which party is making the offer ('offeror') and which party is making the acceptance by going through the exchange of e-mails to determine which party is finally agreeing to a set of terms proposed by the other party. Even at that, there are still a couple of not so straightforward questions that might have an important bearing on the parties' legal rights. After identifying the party who makes the acceptance, the questions following then are where and when did the acceptance become effective? This has a bearing on determining the precise moment that a contract was made as well as, in the case of a contract connected to more than one country especially, where the contract was made - the latter possibly having an effect on which country's law should govern the contract. For example Eze Ken in Kano sends an offer by e-mail to Janet Uburu in Canada. Janet sends an acceptance by e-mail from Canada to Kano. The e-mail is sent in Canada at 1100 GMT but does not reach Kano until 11.15GMT and is not seen by Eze Ken until 1300 GMT. Was the contract made in Kano or Canada? Was it made at 1100, 11.15 or 1300GMT? These are some challenges in electronic contracts.

However, with regards to web-click contracts, establishing which party is making an offer and which one is accepting may actually be more complicated and could have far more serious and potentially financially dangerous consequences. In the first instance, the online business (owner of a business website) advertises products for sale at its website usually with a price tag,[49] an online purchaser makes an order by selecting desired items through clicks and takes the items to the 'checkout' where the sale is confirmed and payment is made. The first question is whether the online seller is the one who makes an offer by advertising products online or whether it is the buyer who makes an offer by selecting items and presenting them at checkout. This may at first seem to be an inconsequential question but two examples below demonstrate the potential consequences attending how the question might be answered.

In one case in the UK, a company (Argos) advertised television sets on its website mistakenly for £2.99 instead of £299. It was reported that orders to the tune of £1 million were very quickly placed for television sets including several (1,700) by one lawyer - astutely or discreditably? It is not entirely clear how the case was ultimately resolved; it seems that no legal proceedings were brought especially with Argos arguing that those who made the orders must have realized that the quoted price was a mistake and also that they themselves had reserved the right to accept orders placed with them and, accordingly, no contract could be made until they accepted any such orders[50]. In another example, this time from the USA, a company (buy.com) advertised a Hitachi VDU monitor for sale at $165 on its website. The price should have been $588! 7000 orders were received but only 143 were in stock. The company initially insisted it would only honour the first 143 orders but it had to settle the subsequent class action for $575,000 with legal bills totaling up to $1m![51] Nigerians e-merchants beware or *caveat* e-merchant!

Consequently, e-merchants have taken heed and now use a number of protective legal mechanisms to prevent such fiascos. One of such is to make clear that an offer of products on their website does not in itself amount to an offer in which case it will be treated as an 'invitation to treat' as most advertisements are treated at law. This means that there can be no contract until an order (i.e. an offer) by the online purchaser is confirmed and accepted by the online business. In effect they keep control of determining the moment when a contract is concluded.

In Nigeria, The *Draft Electronic Transactions Bill* provides that an electronic document is dispatched when it enters an information system outside the control of the originator. More crucially, it also provides rules for determining when such a document is received as follows:

---

[49] Just like what is currently obtainable in Lumia online shopping in Nigeria

[50] <http://www.golds.co.uk/articles/articles_ec_conditions_online_business.htm > accessed on 5 March 2015

[51] Ibid

> *where the addressee has designated a particular information system for receiving documents, receipt occurs when the document enters that information system or if the document is sent to an information system other than that designated, receipt occurs when the document is retrieved by the addressee; if the addressee has not designated an information system, then receipt occurs when the document enters an information system of the addressee*.

It is then further provided that an electronic document is *deemed* to be dispatched from where the originator has his place of business and to be received where the addressee has his place of business. These provisions, based on the UNCITRAL Model Law on Electronic Commerce, will have to be worked out by the courts and might require even legislative amplification in the future[52]. For example, what is meant by 'an information system of the addressee' is that in an environment where many do not personally own computers and use internet cafes, the likelihood is that the phrase will be interpreted widely to include information systems to which the addressee has access or over which he has some control. The provision that an electronic document is *deemed to be received* at the addressee's place of business will mean that as a general rule a contract will be regarded in law as made at the offeror's place of business and this makes it crucial to identify who the offeror is in an electronic contract which will be most critical with regard to Web click or website contracts – less so with regard to e-mail contracts. Who the offeror is in such a contract is a matter yet to be decided by the courts but a lot will depend on the wording of the terms and conditions on the website and the practice of the proprietors with regards to orders placed on the website.

As the practice of concluding contracts electronically grows and evolves in Nigeria, another challenge that the courts are likely to encounter at some point in the future is that of whether a contract can be concluded between two computers operating at the time of the exchange without human input. In other words, can one computer make a contract with another computer and render that contract binding on the proprietors of the computers, that is, the computers being seen as electronic agents of the proprietors. A contract is of course regarded as requiring a meeting of the minds[53] of the parties concerned although of course the law has long recognized the ability to enter into contracts through agents[54] but that recognition was traditionally limited to agency capacity by human beings or recognized juridical persons such as companies and so on.

In the United States, for example, the possibility of contracting through electronic agents is now legally recognized. In the first place, s. 102 of their *Uniform Computer Information Transactions Act* (UCITA) 1999 defines an electronic agent as 'a computer program, or electronic or other automated means used independently to initiate an action or respond to electronic messages or performances without a review or action by an individual at the time of the action, response or performance.' The Act then goes on to provide rules for attributing the actions of an electronic agent. Thus, section 107 of UCITA provides that a person that uses an electronic agent that it has selected for making an authentication, performance, or agreement, including manifestation of assent, is bound by the operations of the electronic agent, even if no individual was aware of or reviewed the agent's operations or the results of the operations.[55] These are matters that will have to be addressed by future e-commerce legislation in Nigeria but it is believed that Nigerian general law is sufficiently flexible to be suitably adapted by the courts if an action on such a point arises in litigation before such legislation is enacted.

At the conclusion of the contract, the next question concerns the terms of the contract. In the case of e-mail contracts, the terms are most likely to be found within the contents of the exchange of e-mails between the parties but may also incorporate documents or material to be found elsewhere. With regard to web click contracts, the online merchant will most probably have a specific web page on its site outlining

---

[52] G Bamodu, op cit @ 13.

[53] This is called *consensus ad idem*

[54] *Qui facit per alium facit per se*

[55] RT Nimmer, '*Principles of Contract Law in Electronic Commerce'* in: I Fletcher *et al* (eds) *Foundations and Perspectives of International Trade Law* (Sweet & Maxwell, London, United Kingdom, 2001). 47

the terms and conditions under which it enters into the online transactions. Contract parties are of course essentially free to agree the terms of the contract. There are, nevertheless, a number of matters that should be of concern to legislators and that the judiciary might have to address with regard to the nature of contracting on the Web.

It is pertinent to note that In the first place, the way commercial websites are normally designed is to attract as much attention to the items on sale, which are displayed prominently. Information on the terms and conditions of contracts concluded at the site will usually be contained in a hyperlink which many shoppers might not be aware of, might not notice or might not bother to read. This raises the question whether such terms are actually incorporated into the contract in law and invokes the legal controls on the extent to which material from outside the contractual instrument per se could be incorporated into the contract.

Secondly, where one party has little choice but to enter into the contract upon terms prepared only by the other[56] there is a necessity for some legal controls to prevent or limit unfairness. Controls to prevent unfairness or abuse of position by a dominant party are necessary over and beyond the provisions in Nigerian Sale of Good Laws that automatically incorporate certain terms into sale of goods transactions such as the terms placing an obligation on the seller to have the right to sell the goods, to supply goods corresponding to contractual description, to supply goods of a merchantable quality and to supply goods fit for any purpose made known by the buyer.

In this respect when the time comes to address these matters in the Nigerian Legal System, lessons can be learned from the experience of other legal systems. For example, in the European Union one very important aspect of legal control and regulation of contracts generally and electronic contracts specifically is the protection of the interests of consumers. This is especially so under the framework of European Union legislation. Other European Union instruments and national legislation implementing or based on them provide further protection for consumers either against the use of unfair terms in contracts generally or in relation to distance selling (ergo, Web click) contracts specifically.

Verily, a consumer will not be held bound by a term of a contract that has not been individually negotiated if that term, contrary to the requirements of good faith, causes a significant imbalance in the parties' rights and obligations.[57] In relation to distance selling contracts,[58] it is required that a consumer be provided in a clear and comprehensible manner with written information before the contract is made detailing, among other things, the identity and address of the supplier, a description of the main characteristics of the goods or services, the price, delivery costs, existence of a right of cancellation etc. The consumer must receive written confirmation of these matters in a durable medium available and accessible by him. In addition, the consumer is given a right to cancel the contract without giving any reason[59]. Further, the distance seller is required to execute a consumer's order within 30 days unless otherwise agreed and if the distance seller is unable to perform the contract he must inform the consumer and refund any sums received from him within 30 days[60]. Finally, some protection is given to the consumer in relation to payments against fraudulent use of his credit or debit card and to some extent in relation to such payments when there is a breach of contract. Useful lessons can be learned from the intention behind as well as the provisions.

---

[56] As in most web click contracts

[57] Council Directive 93/13 of 5 April 1993 as implemented for example in the United Kingdom by the *Unfair Terms in Consumer Contracts Regulations* SI 2083 of 1999 (as amended)<http://eur-lex.europa.eu/LexUriServ/LexUri> accessed 5 March 2015.

[58] Directive 97/7 of 20 May 1997 as implemented for example in the United Kingdom by the *Consumer Protection (Distance Selling) Regulations* SI 2334 of 2000<http://bu.edu/bucflp/laws/directive-97> accessed 5 March 2015.

[59] Ibid; extending up to at least 7 working days

[60] Ibid

RECOMMENDATIONS

Firstly, we the urge the National Assembly to exercise all due diligence on this bill as it has tried to, all these years. But, it is time to quickly review its draconian provisions, pass it and see how it works. It can always be amended if found to have inadequacies. Let there be an end to its endless odyssey in the National Assembly.

Secondly, subject to the inherent discretion of the National Assembly in passing the bill, we wish to remind them to be mindful of other laws of the land. Efforts must be made to ensure that the bill does not contradict Chapter 4 of the Constitution which deals with the Fundamental Human Rights.[61] It must not also infringe on the Freedom of Information Act and the right of Nigerians to privacy must not be violated for no good reason.

Thirdly, we strongly object to the provision of the bill which would allow security agencies to spy on Nigerians. The Cybercrime Law can easily be abused and used for a witch-hunt of political opponents. We need specificity in the drafting of this portion of the bill. Even in the process of criminal investigation, there must be rules about spying on Nigerians. The best practice all over the world is to seek a court warrant by presenting to the Judge evidence of the existence of a reasonable cause. It is not too much to ask that if a Nigeria citizen must lose his or her privacy, a Judge ought to be told why, and the Judge must concur.

Fourthly, the idea of the death penalty as part of this bill should be reconsidered. All over the world, there is a re-thinking of the death penalty. We also need to reconsider the use of this irreversible sanction in view of our own rich experience in the execution of convicted criminals.

Finally, we strongly recommend that the sponsors of the Electronic Transactions Bill take the opportunity of the yet inchoate state of the Bill to amend the provisions on signatures before the Bill is approved and signed into law by making a distinction between ordinary electronic signatures and digital signatures and also by giving an enhanced legal status to digital signatures, particularly with regard to its admissibility as evidence in Nigeria

CONCLUSION

The present Nigerian Government is committed to take this country into the "Computer Age". The outlook for Nigeria is sunny with clouded patches. The repealing of the Evidence Act demonstrates Nigeria's willingness to meet the challenge of the computer age. The new computer age require new skills from lawyers, who would have to develop new skills to meet the new challenges for instance, the skill of comprehension, rather than interpretation. The lawyer's ingenuity would be employed, not only in testing judiciously the limits of applicability of old concepts but of also developing what may be described as "New Law in New Bottles". Legal professionals in Nigeria, and the world over, will have to be competent in dealing with a variety of information sources, to bear new methods of interrogating them, and to be able to extrapolate from the information available to us in order to provide relevant and proactive advice for over clients. New challenges to the Legal Profession are presented by the need for security in electronic networks. Due to lack of security very precious information is hacked by terrorists which has given birth to cyber terrorism. We have need to develop computer forensics. We, as a legal community, also have to recognize, and resolve, the difficulties, which new technological development has brought with them; conflict of laws such as jurisdictional problems across world, protection of intellectual property, security, data protection, privacy and other forms of regulation. The message is simple: It is Time to be enlightened and face the inherent challenges thereto. Now we are living in global village- it is only because of information technologies. So there is need to strengthen computer forensics. Police investigation and forensic investigation are two entirely different aspects. Forensic help is the best help in cyber crime investigation. Thus in the information age, significant opportunities for gain despite these challenges exist for lawyers who are best able to utilize both technology and information.

[61] *Constitution of the Federal Republic of Nigeria 1999(as amended), sections 33 - 45.*