Journal of Public Law and Constitutional Practice

Vol. 6, 2014

A Publication of
Department of Public Law
Faculty of Law, University of Jos
Jos, Nigeria

TOWARDS AN EFFICACIOUS SYSTEM OF ELECTRONIC COMMERCE IN NIGERIA: AN EXAMINATION OF CONTEMPORARY LEGAL ISSUES

ARIYOOSU, DAUDA ADEYEMI*

ABSTRACT

The most significant change in the use of Information Technology has been the rapid growth and development in Electronic Commerce. E-commerce is a relatively new technology which is growing rapidly with the ability to create a truly global digital economy. The regulation of e-commerce in any given economy therefore cannot be over-emphasised. Commercial transactions are conducted through the internet between parties from different parts of the world who may never see themselves in their lifetimes. However, the emergence of e-commerce has also resulted in a number of contemporary legal issues, and these issues pose significant challenges to the legal regime of e-commerce. This paper, therefore, examines a number of legal issues such as formation of contracts, evidential value of electronic commerce, digital signatures, encryption and cryptography regulations, tax issues and payment system in electronic commerce, cyber crimes, choice of law and jurisdictional issue and data protection.

Keywords: Electronic commerce, digital signatures, cyber crimes, data protection, taxation of e-commerce

INTRODUCTION

The emergence of electronic commerce (e-commerce) has revolutionalised the traditional business transactions. With the aid of the World Wide Web (WWW) and telecommunications, the world has become a global village with business transactions being made in billions of dollars within a twinkle of an eye. The budding phenomenon of e-commerce has left the domain of the developed economies; it has extended its strength to developing economies, Nigerian economy inclusive. Consequent upon the emergence of e-commerce in developing economies, the introduction of e-commerce has brought about a number of legal issues that need urgent legislative attention.

Because of the pivotal roles of electronic commerce in a given economy, electronic commerce has generated a lot of contemporary legal issues. The focus is no more on face-to-face or physical business transactions which hitherto have been the order of the day. People are now conscious of challenges brought about by electronic transactions which are concluded without necessarily the parties seeing or knowing one another, more so in Nigeria where there is no direct law on electronic commerce.

FORMATION OF CONTRACT IN ELECTRONIC COMMERCE

E-commerce has become part of our daily commercial activities. The internet which was primarily used as a means of communications now provides a vast avenue for agreements. The internet gives business access to a vast number of consumers and gives businesses access to each other. It is the first ever large scale consumer and business use that was made of the World Wide Web (WWW), the erection of websites of marketing and advertising purposes. Initially, these sites were used to promote companies and products; they did not offer the possibility of selling products and services. Sales and services took place parallel through traditional means of face to face communications.[1]

* **LL.B (Ilorin), LLM (Ife), BL, PGDE, ACTI, ACIArb, Notary Public** Lecturer, Department of Business Law, Faculty of Law, University of Ilorin, Ilorin, Nigeria ariyoosu.da@unilorin.edu.ng

[1] Gringras C, *The Laws of the Internet* (2nd ed, Butterworths Lexis Nexis, London, 2002) 14.

In Nigeria, there is generally no guidance for the formation of electronic contracts.[2] Most existing laws and regulations certainly do not provide for the electronic element in e-transactions and that by itself necessitates the modifications of the laws and regulations to accommodate this element.[3] Under the English Common Law, agreements become legally binding when four elements of formation of contract: offer, acceptance, consideration and intention to create legal relations are in place.[4]

Offer and Acceptance

Websites are generally designed in such a way as to constitute an invitation to make an offer. However, before such as invitation is made, pre-offer information is first made by the website owner. The Electronic Commerce (EC Directive) Regulations oblige almost every owner of a website to provide certain information to its visitors.[5] Unless parties who are not consumers have agreed otherwise before an order is being placed by the recipient of a service in electronic commerce contracts, the service provider has the onerous duty of providing a clear, comprehensive and unambiguous manner of information regarding:

- the different technical steps to follow to conclude the contract;
- whether or not the concluded contract will be filed by the service provider and whether it will be accessible;
- the technical means for identifying and correcting input errors prior to the placing of the order; and
- the languages offered for the conclusion of the contract.[6]

Also, unless parties who are not consumers have agreed otherwise, a service provider shall indicate which relevant codes of conducts he subscribes to and give information on how information on how those codes can be consulted electronically.[7] So also where the service provider provides terms and conditions applicable to the contract to the recipient, the service provider shall make them available to him in a way that allows him to store and reproduce them.[8]Having provided recipient with the requisite preliminary information,[9] offer in electronic commerce are made electronically, and the first question to consumer is when is an offer made? This question is necessary because electronic communications, especially e-mails[10] are often delayed in transmission and a court of law will have to decide whether a revocation of the communications is effective before the conclusion of the contract.[11]

In electronic commerce contracts, websites are designed in such a way as to constitute an invitation to make an offer and not a real offer. The recipient of the services usually makes an offer while the service provider accepts.[12] The order and the acknowledgement of receipt will be deemed to be received when the parties to whom they are addressed are able to access them and the acknowledgement of receipt may take

[2] Prof. Bolaji Owasanoye, 'Findings from Review of Laws for Social and Economic Development in Nigeria' (Paper presented at the Working Session of SPIDEL at the Nigerian Bar Association Annual General Conference on Tuesday August 18 2009 at Oceanview Expo Centre, Eko Hotels & Suites, Victoria Island, Lagos, Nigeria 2009).
[3] Paul Uyoro, 'E-Commerce in Nigeria: How to Move Forward Legal Framework for the Introduction of E-Commerce'< http://paulusoro/publications/Ecommerce.com> accessed 24 January 2010.
[4] Gringras C, *The Laws of The Internet*, 15.
[5] See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services.
[6] Electronic Commerce (EC Directive) Regulations 2002, Regulation 9 (1).
[7] Ibid, Regulation 9 (2).
[8] Ibid, Regulation 9 (3).
[9] Preliminary information is of great importance in electronic commerce contracts while same is not a requirement for consideration in traditional usual contracts.
[10] Faxes and Telephone Calls are more instantaneous than e-mails since e-mails messages are first sent to a service provider who in turn delivers it to the box of the receiver.
[11] In Electronic Commerce contracts, an offer can be retracted or revoked at any moment up to acceptance.
[12] Electronic Commerce (EC Directive) Regulations 2002, Regulation 11 (1) (a) & (b).

the form of the provisions of the service paid for.[13] The acceptance must unequivocally express assents to all the terms of the offer.[14] With an e-mail offer, the expiration will be implied sooner than an offer made by post.[15] An acceptance generally need not be in writing.[16]

Just as in the general common law rules of contracts, an acceptance must be communicated to the person making the offer,[17] but the offeree must acknowledge the receipt of an order without undue delay and by electronic means. An acknowledgement of receipt may well also be the acceptance of the offer.[18] In exceptional circumstances, acceptance may be inferred from silence.[19]

Consideration

Consideration has been described as something of value in the eye of the law.[20]It is the price for which the promise is brought.[21]Mutual promises may be adequate consideration under the general common law of contracts. Similarly, promises to pay over the internet may be enough consideration to create a contract.[22]

Intention to Create Legal Relations

Whenever a person makes an agreement with a website, the site either accepts or rejects the communication according to the computer program being run at the time. Neither party to the contract sits on the server side and this poses a serious issue of how the contract can be formed without direct intention. This issue was settled by Lord Denning in *Thornton v Shoe Lane Parking*.[23] In that case, Mr. Thornton accepted a contract by driving a car into a car park. It was held that the automatic reaction of the car park turning a light from red to green and thrusting a ticket was enough to create a contract. The burden is on the offeror to prove that there was no intention to have a legal consequence.[24]

EVIDENTIAL VALUE OF ELECTRONIC COMMERCE

In electronic commerce and transactions, courts are much less familiar with the form of evidence to be adduced and so additional questions may need to be considered to enable them to assess the admissibility or otherwise of electronic transactions or the weight to be attached to it. At the extreme, there are two possible approaches to this; the court either assumes that an electronic document is reliable unless evidence is adduced to show otherwise or electronic evidence is treated as wholly unreliable and potentially inadmissible unless sufficient evidence can be adduced to convince the court that it is in fact useful.[25]In some jurisdiction,[26]there are electronic courts which are online forum of a virtual court that assists in management of pre-trial matters by allowing directions and interlocutory orders to be made online via the court's website.[27]

[13] Ibid, Regulation 11 (2).
[14] See Gringras G, *The Laws of The Internet*, 27; Akomolede TI, 'Contemporary Legal Issues in Electronic Commerce in Nigeria', 7.
[15] Ibid. See also *Quenerduaine v. Cole* (1883) 32 WR 185.
[16] Thus, acceptance can be by words, in writing or by conduct. See Sagay I. E., *Nigerian Law of Contract* (Reprinted, Spectrum Law Publishing, Ibadan, Nigeria, 1993) 13.
[17] See *Felthouse v Bindley* (1862) 7 L. T. 835.
[18] Gringras C, *The Laws of the Internet*, 27-28.
[19] See *Allied Marine Transport Ltd v Vale do Rio Doce Navegacao SA* (1985) 1 WLR 925 at 927.
[20] *Thomas v. Thomas* (1842) 2 Q.B. 851 at 859.
[21] *Dunlop Pneumatic Tyre Co. Ltd v. Selfridge Ltd* (1915) AC 847 at 855.
[22] Gringras, *The Laws of the Internet*, 40.
[23] (1971) 2 QB 163 at 169.
[24] *Edwards v. Skyways Ltd* (1964) 1 WLR 349 at 355.
[25] Lorna Brazell, *Electronic Signature and Identities, Law and Regulation* (2nd ed, Sweet & Maxwell, London, 2008) 294.
[26] Such as Australia.
[27] Philip N. Argy, 'Law of Evidence' in Stephen Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (LexisNexis Butterworths, UK 2007) 145.

In Nigeria, the absence of direct laws on e-commerce throws up a major challenge with regards to the evidential value of electronic commerce. The major identified challenges include:

- whether a record of digital commerce interaction can replace traditional paper agreement and all the associated safeguards like signature, witnessing, authentication e.t.c.
- whether national laws recognise electronic agreements.
- whether the courts and third parties can accept the digital copies as evidence of the electronic transactions.
- which of the copies will be the original since the parties may be in different geographical jurisdictions and the transactions were concluded electronically.
- since commerce over the internet is done with the support of a third party, namely the Internet Service Providers (ISP), will these be regarded as agents to all the electronic transactions that go through them or common law rule applicable to acceptance by post apply?
- there is also evidence and proof and possibly conflict of law issues with regard to all the jurisdictions in which parties are located.
- differences in jurisdictional laws on website establishment, regulations and operation.[28]

As far as admissibility of electronic documents is concerned, courts have traditionally placed reliance on the questions of whether a document presented to them is an original. If the document is original, there may be no problem admitting it, if other conditions for its admissibility are met.[29] Thus, in *Sharafadeen Aderemmy Kolawole v The Federal Polytechnic, Offa & Anor,*[30] the Federal High Court, Ilorin Judicial Division, having found as a fact that a computer-generated document was original unhesitatingly admitted same despite objection to its admissibility.

It has been observed that the issue of admissibility of computer-generated evidence is a practical legal conundrum in the Nigerian legal system.[31]This shows that the position of admissibility of computer-generated evidence appears dicey. This is even manifest in the various conflicting decisions of our courts as exemplified in a number of cases cutting across three tiers of the Federal Judicial System[32] with a bearing on the admissibility of Electronically Stored Information (ESI) evidence. Thus in *Esso West Africa Inc v Oyegbola*[33] the Supreme Court held 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. In modern times reproduction or inscriptions on ledgers or other documents by mechanical process are common place and section 37 of the Evidence Act cannot therefore apply only to "books of account…so bound and the pages… not easily replaced. It further held that the ledger cards in this case had been wrongly rejected and they should have been admitted in evidence. In *Yesufu v ACB,*[34] the Court of Appeal held that computer print-outs are not admissible while in *Elizabeth Anyaebosi v R T Briscoe Nigeria Ltd*[35] the Supreme Court opined that computer print-out is admissible as secondary evidence. Similarly, in *Unity Life and Insurance Co LTD v IBWA Ltd*[36] the Supreme Court held that computer print-out is admissible as secondary evidence. However

[28] Professor Bolaji Owosanoye, 'Findings from Review of Law for Social and Economic Development in Nigeria.
[29] Other conditions relate to whether the document is pleaded and whether it is relevant or not. See *Okonkwo Okonji v George Njokanma* (1999) 14 NWLR (Pt 638) 250 at 266; *Abubakar v Chuks* (2008) All FWLR (Pt 408) 207 at 221.
[30] (Unreported) Suit No. FHC/IL/CS/10/2008 delivered on 28th October, 2008 by B. B. Aliyu J.
[31] Sebastian Hon, SAN, 'Law of Evidence Can't Admit Posers of the Use of DDC Machines' The Guardian (Nigeria 25 January 2011) 70.
[32] That is the trial High Court, the Court of Appeal and the Supreme Court.
[33] (1969) NMLR 194; NSCC 354-355
[34] (1976) ANLP (Pt. 1) 328.
[35] (1987) 3 NWLR (Pt. 59) 84.
[36] (2001) 7 NWLR (Pt.713) 610.

in the Court of Appeal case of *Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd*[37] it was held that the admission in evidence by the trial court of computer print-out as secondary evidence of entries of a banker's book was wrong because, among other things, the relevant provision of Section 97 of the Evidence Act do not contemplate information stored 'other than in a book.' Another decision is the case of *Trade Bank v Chami*[38] where the Court of Appeal posits that Section 97 of the Evidence Act[39] does not require the production of 'books of account' but makes entries in such books relevant for admissibility. Although the law does not talk of 'computer' and 'computer print-outs', the law is not oblivious to or ignorant of modern business world and the technological advancement of the modern 'jet age'. As far back as 1969, the Supreme Court in the case of *Esso West Africa Inc. v. Oyegbola*[40] envisaged the need to extend the horizon of the section to include or cover computer which was virtually not in existence or at a very rudimentary stage at that time.

Also in *UBA v SAFDU,*[41] the Court of Appeal held that computer print-outs of statement of account are only admissible subject to the fulfilment of the condition listed in Section 97(2) (e) of the Evidence Act.[42] In the recent decision of the Lagos High Court of Justice in *Federal Republic of Nigeria v Femi Fani-Kayode*[43] the trial Federal High Court held that computer print-out of statement of account is inadmissible under Section 97(1)(h) and 97(2)(e) of the Evidence Act,[44] even if relevant to the proceedings, since the issue in contention is that the document, that is, the statement of account is a computer print-out, therefore, certification of the statement of account was inapplicable or irrelevant. However, on appeal, [45]interpreting the provision of Sections 97 (1) (h) and 97 (2) (e) of the Evidence Act, the Lagos Division of the Court of Appeal up-turned the ruling of the trial judge and accepted electronic evidence and ruled that the electronically-generated statement of account of the respondent (which was rejected by the trial High Court) be admitted in evidence.[46]

Despite the supposedly unsettled position regarding admissibility of computer-generated evidence, the point must clearly be made, however, that the inadmissibility of documentary evidence is regulated by the Evidence Act itself. The Evidence Act[47] provides that:, 'Nothing in this Act shall prejudice the admissibility of any evidence which would apart from the provisions of this Act be admissible'.[48]

The effect of this provision is that a computer-generated document is not thereby inadmissible on the mere fact that it is a computer-generated document. This position is buttressed by the West African Court of Appeal case of *R v Agwuna,*[49] where it was held that there is no provision in the Evidence Act which allows any evidence to be rejected as inadmissible save as provided in the Act itself.

It is submitted that even though the introduction of computers has persistently challenged evidentiary rules, the court has been liberal in interpreting the provisions of the law when it comes to admissibility of

[37] (2003) FWLR (Pt. 145) 661.
[38] (2003) 13 NWLR (Pt.836) 158.
[39] *Cap E14 LFN 2004* (which is *in pari materia* to Section 90 of the Evidence Act 2011).
[40] Supra.
[41] (2004) 3 NWLR (Pt.861) 516
[42] *Cap E14 LFN 2004*(which is *in pari materia* to Section 90 (e) of the Evidence Act 2011).
[43] See <www.thisdayonline.com/nview.php?id=174356> accessed on 26 July 2010. See also Dayo Atofolaki, 'Nigeria: Fani Kayode v EFCC- Did the Appeal Court Err in Law?' <http://allafrica.com/stories/201007160120.html> accessed on 27 July 2010.
[44] (which is *in pari materia* with Sections 89 (h) and 90 (e) of the Evidence Act 2011).
[45] *Federal Republic of Nigeria v Femi Fani-Kayode* (2010) All FWLR (Pt 534) 181.
[46] See also <www.thisdayonline.com/nview.php?id=174356> accessed on 26 July 2010.
[47] *Cap E14, Laws of the Federation of Nigeria 2004.*
[48] Evidence Act, *Cap E14, Laws of the Federation of Nigeria 2004,* Section 5 (a).
[49] (1949) 12 WACA 456 at 458.

computer or electronically-generated evidence.[50]It has also been concluded that foundation evidence by way of authentication of print-outs, reliability and safety devices of a computer system raise issues on the weight of evidence *vis-à-vis* a computer print-out and if one is able to clearly appreciate the distinction between admissibility and weight of evidence, the inevitable conclusion is that computer print-outs are admissible under our evidentiary rules.[51]

When a document does not require signature, the issue of admissibility may not pose any evidential problem. However, for most documents forming the basis of electronically signed transactions, it will not be at all clear what constitutes the original documents. This is because the image seen on the screen by the writer is only a representation of the electromagnetic signal passing through the computer at any one instant, and if saved, is stored in a different form that is represented to the viewer. It is therefore doubtful whether any electronic document can comply with the best evidence rule.[52]

In assessing the weight to be placed upon electronic documents, a court may require supporting evidence to be able to assess how reliable they are. The courts may not be familiar with the technology involved in signing and recording electronically and this unfamiliarity with the technology may also affect the weight to be attached to electronic documents.[53]

It appears the burden of proof in e-commerce transactions is the same as that in a paper-based transactions; each party must prove any fact he asserts.[54] Although there are certain provisions of the Evidence Act[55] that can be used to admit digital evidence in Nigerian courts such as Sections 33, 37, 38, 39, 90 and 91 of the Evidence Act, these sections however may not be adequate for the admissibility of computer-generated evidence. It is therefore arguable that there is no conclusive legal authority that can be relied upon for the admissibility of digital evidence in Nigeria under the Nigerian Evidence Act.[56] However, the enactment of the new Evidence Act 2011[57] has laid the argument on admissibility or otherwise of Computer Print-Outs to rest. Statements in documents produced by computers are now admissible if the conditions laid down in Section 84 (2) of the 2011 Evidence Act are satisfied. These conditions are:

(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purpose of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;

(c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and

(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

[50] Just like in *Federal Republic of Nigeria v Femi Fani- Kayode* (Supra) at 195 where the court held that 'once there is substantial compliance with the provisions of section 97 (2)(a) of the Evidence Act, banking documents, whether primary or secondary, are admissible in evidence'.

[51] Taiwo Osipitan, 'Admissibility of Computer Print Out under Nigerian Law of Evidence' (1995) 2 (2) Lawyer's Bi-Annual Journal of Nigerian and Comparative Law, 248.

[52] Lorna Brazell, *Electronic Signatures and Identities Law and Regulation*, 294-295.

[53] Ibid 296.

[54] Ibid 296-297. See Section 135 (1) of the Evidence Act, *Cap E14, LFN 2004*. See also *Famuroti v Agbeke* (1991) 5 NWLR (Pt 189) 1, *First Bank of Nigeria Plc v Chief Peter Oguebie & Anor* (2008) All FWLR (Pt 439) 493.

[55] *Cap E14, LFN Nigeria 2004*.

[56] *Cap E14 LFN 2004*.

[57] Which by its Section 257 repealed the Evidence Act, *Cap E14 LFN 2004*.

It is submitted that once the above conditions are established, computer print-out are admissible. Fortunately, the 2011 Evidence Act defines documents to include any device by means of which information is recorded, stored or retrievable, including computer output.[58]

DIGITAL SIGNATURES

Digital signatures provide information regarding the sender of an electronic document. The technology has assumed huge importance recently with the realisation that it may be the remedy to one of the major barriers to growth of electronic commerce: fear of lack of security. Digital signatures provide data integrity, thereby allowing the data to remain in the same state in which it was transmitted. The identity of the sender can also be authenticated by third parties.

In legal parlance, a signed document denotes legal authenticity and validity. Thus, the traditional function of a signature is evidentiary. It confers clearly defined legal rights and responsibilities on the parties who have signed documents and represents a solid foundation upon which a commercial relationship can be sustained.[59] The basic purpose of signing any document is to authenticate the document and to identify and bind the person who signs it. Once a signature is laid on document, the endorser cannot later falsely state that he had not signed the document and consequently cannot repudiate it.[60] Once a literate person appends his signature on a document, the contents of the document is binding on him and this is the position of the court. Thus in *Afribank (Nig) Plc v Alade*,[61] it was held that:

> A literate adult of sound mind and capacity is deemed to know the nature and contents of the document he voluntarily signed. He is therefore presumed at law to understand what he appended his signature upon. Whatever the contents of the document is, it will not avail him to deny it.

In India, an electronic record may be authenticated by affixing a digital signature by the use of asymmetric crypto system which develop and transform the initial electronic record into another electronic record.[62]In the United State of America, some states have adopted digital signature laws while some have considered giving effect to both electronic and digital signatures. The United State Federal Government has enacted an Act,[63] the purpose of which is to enable electronic commerce and e-sign generally to create an equivalency between electronic and non-electronic writings and signatures.

The United Nations Commissions on International Trade Law (UNICITRAL) has strenuously worked on a model digital signature law. Also the Organization for Economic Co-operation and Development (OECD) adopted guidelines concerning cryptography. This is for the purpose of digital signatures in order to evidence the development of electronic commerce.[64] The United Kingdom also introduced the key elements of the Electronic Signature Directive and it is that the mere fact that a signature is electronic does not prevent a court from relying upon its veracity in a dispute.[65]

[58] Evidence Act 2011, Section 258.

[59] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* (3rd Ed, Wadhwa and Company Law Publisher, India 2007) 918.

[60] Ibid 767.

[61] (2000) 13 NWLR (Pt 685) 591 at 602. See also *Moss v Kentrow (Nig) Ltd* (1992) 9 NWLR (Pt 264) 207 at 221.

[62] See Section 3 of the India Information Technology Act 2000.

[63] The US Federal E-Sign Act which took effect on October 1, 2000.

[64] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet*, 804. See also UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 <http://www.uncitral.org/pdf/English/texts/electcom/05-89450_Ebook.pdf>accessed on 24 August 2010.

[65] Section 7(1) of the UK's Electronic Communications Act 2000 and UK Electronic Signatures Regulations 2002. See also Clive Gringras, *The Laws of the Internet*, 38.

ENCRYPTION AND CRYPTOGRAPHY REGULATIONS

The role of encryption and digital signatures go hand in hand. Encryption provides authentication, authorisation, confidentiality and integrity to services, increasing the security of e-commerce transactions.[66]Cryptography provides the technology used in digital signatures as well as for encryption. Encryption renders an electronic document unreadable, thereby providing another level of security and increasing the attractiveness of the Internet as a means of transferring confidential data of the type often used in electronic commerce. Encryption is either a powerful tool or a dangerous weapon. As a tool it is an important aid to the security of legitimate data transactions, but as a weapon it could be used for criminal means. [67]

The most widely used type of cryptography is public key cryptography where the sender is assigned two keys – one public, one private. The original message is encrypted using the public key while the recipient of the message requires the private key to decrypt the message. The recipient can then determine whether the data has been altered. However, although this system guarantees the integrity of the message, it does not guarantee the identity of the sender (public key owner).[68]Here we have yet another example of the phobia surrounding electronic commerce and the invasion of privacy.[69]

Cryptography technology and process used to encode (encrypt) and subsequently, to decode (decrypt) information to prevent its being read by unauthorized party has been a major component of the complete data security system.[70]Clearly any encryption of message needs to be agreed and implemented by all parties to an Electronic Data Interchange (EDI) transaction.[71]

TAX ISSUES IN ELECTRONIC COMMERCE

Electronic Commerce represents a new business model, and as such it creates some challenges to tax systems that were designed with different model in mind. Tax administrations face the challenge of adopting tax sysfems to an economy that increasingly ignores physical borders.[72] Since electronic commerce can be conducted virtually instantaneously around the globe and around clock, the question where the profits should be taxed becomes of outmost importance.[73] Furthermore, the anonymity of the internet transactions means that internet activities are difficult to trace. A number of countries have passed legislations in the area of taxation for e-commerce activities.[74]

One of the challenges to e-commerce to the Nigerian tax system is that the laws governing direct taxes (income taxes) are currently premised on the concept of permanent establishment[75]as presently defined in

[66] Mensah A.O., Bahta A and Mhlanga S.,'E-Commerce Challenges in Africa: Issues, Constraints, Opportunities' <http://www.uneca.org/ais/docs/policy Briefs/E-commerce challenges in Africa.pdf> accessed on 28 July 2010
[67] Ibid.
[68] Swindells C and Henderson K., 'Legal Regulation of Electronic Commerce<http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/swindells/#a2>accessed on 28 July 2010.
[69] Ibid.
[70] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet*, 812.
[71] Peter K. and Clayton Utz, 'Contracts for Products and Services' in Susan Cotter (ed) International Information Technology Law (Cepter for International Legal Studies, John Wiley & Sons, Salzburg Australia) 17.
[72] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)*, 209.
[73] Ibid.
[74] Prof. Bolaji Owosanoye, 'Findings from Review of Laws for Social and Economic Development in Nigeria'. Such countries include the United States of America, the European Union, South Korea, Chile, South Africa and Peru.
[75] The expression 'permanent establishment' as far as taxation of e-commerce concept is concerned is defined in Article 5 (1) of the Organization of Economic Co-operation and Development (OECD) 1995 Model as a fixed place of business through which the affairs of an enterprise are wholly or partly carried on.

double tax treaties. With the advent of e-commerce, the need for physical presence is removed or at best diminished and this creates the problem of how to determine the right to tax profits that are derived from electronic commerce, and the question is whether a website or a server, owned or used by a foreign company can create a fixed place of business and hence a taxable transaction.[76]

Any debate on taxation of e-commerce would definitely include both technical and policy issues. The policy issues run the spectrum from whether on-line sale should be subject to sales tax to who should decide what should or should not be taxed. Technical issues include how to simplify tax systems, how to source sales[77] and how tax compliance and administration can be streamlined.[78]

In considering whether to tax internet sales and transactions, certain recognized principles are of paramount consideration such as: equity and fairness,[79] certainly,[80] convenience of payment,[81] economy in collection,[82] simplicity,[83] neutrality,[84] economic growth and efficiency,[85] transparency and visibility,[86] minimum tax gap[87] and appropriate government revenues.[88]Similarly, as retail methodologies and the relevant technologies develop in the area of internet transactions, it can be assumed that more new and innovative business unknown in the non-virtual world will be created.

It is therefore important to bear in mind that tax policy can have an important impact upon the creation of on-line and e-commerce businesses and this can equally have a reciprocal effect on tax policy.[89]It is for commercial negotiators and general legal advisers to be aware of the basic tax issues effecting internet transactions for which they are responsible. This basic awareness would enable them to ask the right questions of specialist tax advisers and understand the advice when they receive it.[90]

PAYMENT SYSTEM IN ELECTRONIC COMMERCE

The world has become a global village as a result of technological developments in cyber space and this is manifest in the current trends where the movement of money through the Internet has paralleled the processes which were hitherto established for commercial activities. The Internet provides an alternative medium for exchange of money. Consequently, the actual exchange of value between parties over the internet has evoked few jurisdictional issues for various reasons. The sheer volumes of currencies and

[76] Prof. Bolaji Owasanoye, 'Findings from Review of Laws for Social and Economic Development in Nigeria'.
[77] Either to the seller's location or to the buyer's location.
[78] Annette Nellen, J.D, 'E-commerce: To Tax or not to Tax? That is the Question. Or is it? <http://www.cob.sjsu.edu/facstaff/nellen-a/> accessed on 24 January 2010.
[79] Thus, similarly situated tax payers should be taxed similarly.
[80] The tax rules should clearly specify when the tax is to be paid, how it is to be paid, and how the amount to be paid is to be determined.
[81] A tax should be due at a time or in a manner that is most likely to be convenient for the taxpayer. This principle is mostly met with today's sales tax rules, which tend to require periodic filing and payment at a time subsequent to the sale.
[82] The costs to collect a tax should be kept to a minimum for both the government and taxpayers.
[83] The tax law should be simple so that taxpayers can understand the rules and comply with them correctly and in a cost efficient manner.
[84] The sales tax could be made more neutral by requiring sales tax to be charged by remote vendors enforcing use tax rules exempting all digitised items from sales tax along with their tangible counterpart or taxing all products regardless of how they are transferred.
[85] The tax system should not impede or reduce the productive capacity of the economy.
[86] Tax payers should know that a tax exists and how and when it is imposed upon them and others.
[87] This means that a tax should be structured to minimise non-compliance.
[88]The tax should enable the government to determine how much tax revenue will likely be collected and when.

[89] Clive Gringras, *The Law of the Internet*, 399.
[90] Mark Anderson, *Technology Transfer, Law, Practice and Precedents* (2nd Ed, Butterwoths Lexis Nexis 2002) 689.

value involved in international payment system demands efficient processing.[91] International agreements on payment systems and regulatory oversight seem to be the most appropriate step towards facilitating the internet's promise. As electronic commerce grows, the number of financial institutions should, exponentially, grow as well.[92] The success of e-commerce, no doubt, depends largely upon effective electronic payment systems. Due to the explosive growth of the on-line and internet business, electronic commerce uses various electronic payment mechanisms that can cater for much diversity of applications.

The need for electronic payment technologies is to respond to fundamental changes in socio-economic trends. The efficient payment system reduces the cost of exchanging goods and services, and is indispensable to the functioning of the inter-bank money and capital markets. A weak payment system, however, has the tendency of hindering the stability and developmental capacity of an economy.[93] The electronic payment system consists of users, issuers and regulators.[94] Electronic payment system has been classified into cash-like payment system and cheque-like payment system.[95]

With particular reference to the banking industry, the Central Bank of Nigeria (CBN) issued Electronic Banking Guidelines for all banks seeking to use technology in delivering banking services. It is hoped that the guidelines are accorded a stronger regulatory teeth by providing sanctions for violations and penalty for non-compliance.

In the consciousness of embracing and enhancing electronic payment system in the economic landscape in Nigeria, the Central Bank of Nigeria recently came up with a reform policy aimed at checking the increasing dominance of cash in the banking sector.[96] It came up with a circular dated 20th April 2011 titled: 'Industry Policy on Retail Cash Collection and Lodgment.'[97] The circular constitutes guidelines in the quest to migrate from cash to cashless economy. The basis of the policy has been clearly stated in the circular itself as follows:

> In view of increasing dominance of cash in the economy with its implication for cost of cash management to the banking industry, security, money laundering, etc., the Central Bank of Nigeria, in collaboration with the Bankers Committee, is adopting policies to reduce the high usage of cash, moderate the cost of cash management and encourage the use of electronic payment channels.[98]

The policy directives are as follows:

- Commencing from June 1, 2012, a daily cumulative limit of ₦150,000 and ₦1,000,000 on free cash withdrawals and lodgments by individual and corporate customers respectively with Deposit Money Banks (DMBs) shall be imposed. To this end, individuals and corporate organizations that

[91] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 85.
[92] Ibid, 86.
[93] Raja J. *et al*, 'E-payment: Problems and Prospects' (2008) 13(1) Journal of Internet Banking and Commerce (JIBC) <http://www.arraydev.com/commerce/jibc/> accessed on 13 December, 2009.
[94] Ibid. The user can, in turn, be sub-divided into retailers and consumers depending on the transaction model adopted. Issuers are banks and other financial institutions that are providing actual mechanisms or the means to integrate the mechanism into other financial systems while the regulators are those who are concerned with issues ranging from assuring the integrity of the mechanism and its operators, to the potential impact on the wider economy.
[95] Ibid. Both cash-like payment system and cheque-like payment system are direct payment system, that is, payments that require interaction between buyer and seller. There are also indirect payment systems where other buyer or seller initiates the payment without having the other party involved online.
[96] See Odidison Omankhanlen, 'From Cash to Cashless Economy: How Practicable is CBN's Mop up Policy?'<http://tribune.com.ng/sun/index.php/crime-features/3801-from-cash-to-cashless-economy-how-practicable-is-cbns-mop-up> accessed on 20 October 2011. The policy is otherwise known as the CBN Guidelines on a Cashless Economy.
[97] CBN, 'Industry Policy on Retail Cash Collection and Lodgment' http://www.cenbank.org/out/2011/circulars/cod/retail lodgment>accessed on 21 October 2011.
[98] Ibid.

make cash transactions above the limits will be charged a penal fee of ₦100/thousand and ₦200/thousand respectively for amounts above the cumulative limits.

Contravention of this policy attracts a fine of five (5) times the amount that the bank waives as a first offender. Subsequently, the bank shall pay ten (10) times the charges waived.

- 3rd party cheques above ₦150,000 shall not be eligible for encashment over the counter. Value for such cheques shall be received through the clearing house. If a bank allows 3rd party cheque encashment, it shall be liable to a sanction of 10% of the face value of the cheque or ₦100,000 whichever is higher.
- Banks will cease cash in transit lodgment services rendered to merchant-customers from June 1, 2012. In this regard, customers could engage the services of the CBN licensed cash-in-transit (CIT) companies to aid cash movement to and from their banks at mutually agreed terms and conditions. Contravention of this policy shall attract a fine of ₦1.0 million per specie movement.
- The arrangement shall be in force in Lagos State, Federal Capital Territory, Port Harcourt, Kano and Aba in the first instance. The arrangement shall be extended to other parts of the country at a date to be determined by the Bankers Committee.
- To achieve interoperability of local currency POS transactions, no card scheme, foreign or local, shall operate exclusive acquirer agreement or contract in Nigeria with effect from June 1, 2011. Any payments scheme, processor, switching company, service provider or bank that contravenes this policy may be suspended for a minimum of one (1) month by the CBN as a processor, switching company, service provider etc in the first instance. The license may be withdrawn by the CBN if the contravention is repeated.
- The policy shall apply to both private and public sector transactions. All financial institutions including Deposit Money Banks, Savings and Loans, Mortgage and Microfinance Banks shall comply accordingly.
- Compliance with the policy shall be monitored by the Banking Supervision Department and the Other Financial Institutions Supervision Department with appropriate sanction applied to erring institutions.[99]

Ahead of implementation of the scheme in Lagos, effective January 1, 2012, the CBN selected four manufacturers for the provision of Point-of-Sale terminals.[100] These manufacturers were selected after a through process by a committee comprising of key stakeholders in the payments system value chain.[101]

Expectedly, the new policy has generated mixed reactions from Nigerians. The policy is riddled with many implications which may be positive or negative to banks and customers during the course of business activities and financial transactions. It has been argued by those who support the policy that the policy will reduce cost of cash management in banks and encourage the use of electronic payment channels. This will bring the nation close to the Millennium Development Goals and join the league of developed countries with cashless economy. The policy and the eventual cashless economy will reduce snatching of money from customers at gun-point on the street and also reduce the incentive for robbery and employee theft. The nation's economy will witness less money in circulation as huge of quasi-money is expected to be in the vault and there will be reduction in the cost of printing and minting of money by the Central Bank of Nigeria. Use of electronic money, which may be the outcome of the policy, will eventually reduce cost associated with storage, transportation and security and it is expected that the policy may lead to the 'explosion' of mobile financial services companies in Nigeria. In fact, many members of the formal and

[99] Ibid.
[100] The manufacturers are: PAX Technology, Bitel, Ingenico and Verifone.
[101] Abdulwahab Isa, 'Cashless Economy: CBN Appoints 4 Manufacturers for POS' http://www.peoplesdaily-online.com/news/national-news/21924-cashless-economy-cbn-appoints-4-manufacturers-for-pos>accessed on 18 October 2011.

informal sectors may decide to open and use more bank accounts since there is limit to cash they can withdraw at once so as to make up for their cash need per day. There will also be decline in operating expenses per customer in the financial sector and in the long run, there will be less traffic in the banking hall when many would have adopted e-transaction.[102]Aside reduction in the risk associated with cash movements across the country, the policy will check further abuse of local currency.[103]

Others see the new policy as a bitter pill to swallow. They opined that the policy is completely diversionary even considering the issues it addresses. They believe the issues are the least in the hierarchy of problems of Nigeria's financial sector. Moreover, not only is the supporting infrastructure for its enforcement lacking, the policy does not take cognizance of the realities of Nigeria's informal market, which is very much cash-based. Therefore, they conclude that no matter how much effort is put into both public enlightenment and education before its expected take-off, the policy may, just like others before it, most likely end up as a wide goose chase.[104] They feel the policy would hurt traders more, given the fact that their business is on a 'cash-and-carry' basis. The businessman may have to withdraw more than the minimum amount that can be withdrawn for his business, and in such a situation he would be surcharged for withdrawing more than the stipulated amount. Some see the policy as unrealistic. They argued that the policy could be abused as in the case with beneficiaries of Western Union who end up being short-changed by operating banks. Some even posited that the high level of illiteracy in the country, low level of banking population porous e-banking system are factors that may militate against the success of the policy. They believe that if the idea is to promote e-banking by encouraging the use of e-payment channels like ATM, the wide-spread scale fraud associated with its use would make the policy counter-productive. The policy, they say, may further dampen the savings culture in the country. Some reacted that the transformation from a cash-centric to a plastic economy will need a longer period; they therefore prefer a gradual introduction of the scheme to enable the fundamental structures to be put in place.[105]

It is important to note that the nation is not very ripe for a stringent policy on cashless economy as Nigerian economy is dominated by informal sector where use of banking services is highly limited. There is need for a longer deadline as members of the informal sector may find the policy cumbersome at the beginning. By and large, human habits and cultural attachments to the traditional use of money may also militate against the policy. The Central Bank of Nigeria (CBN) therefore should encourage and intensify awareness among citizens, especially among the informal sector of the economy and put in place necessary measures to make the dream for cashless economy a success.

The most popular methods of effecting payment in electronic commerce are through credit cards, smart cards, digital or electronic cheques or cash, and debit cards.[106] Of all the above-mentioned methods of effecting payment in e-commerce, the only payment mechanisms currently which satisfy the mass market for internet use are credit and debit cards. They are familiar and internationally recognized and widely

[102] Pan African Capital, 'CBN Policy on Retail Cash Collection and Lodgment Analysis and Implications'<http://www.panafricancapitalplc.com/uploads/reports/CBN CASH COLLECTION AND LODGMENT POLICY_MAY 2011.pdf>accessed on 22 October 2011.
[103] 'CBN's Quest for a Cashless Economy' http://crisisboom.com/2011/05/17/cbn's-request-for-a-cashless-economy/>accessed on 18 October 2011.
[104] 'CBN's Policy on Retail Cash Collection and Lodgment'<http://allafrica.com/stories/201105100714.html>accessed on 21 October 2011.
[105] See Emmanuel Uffot, 'Towards a Cashless Economy' http://www.newswatchngr.com/index2.php?option=com_content&do_pdf=1&id=3073accessed on 18 October 2011.
[106] See Akomolede I. 'Taxation and Payment System in Electronic Commerce.' Akomolede I.T. 'Contemporary Legal Issues in Electronic Commerce in Nigeria.'

held. They meet many of the ideal-mechanism criteria. They also result in immediate settlement and work for distance purchase and transactions.[107]

Credit and debit cards are, however, not without their own deficiencies for internet purposes; their cost is high and they are not secret- they leave a clear audit trail.[108] Credit cards constitute the predominant form of on-line payment because they fulfil the requirements for a payment system. With a credit card, the customer by presenting a valid card or by issuing a valid set of numbers honour his obligations under the contract.

The digital or electronic cheques or cash are modeled on conventional cheques except that they are authorized using digital signatures rather than handwritten signature. This offers the facility to write digitally signed cheques using public or private key cryptographic techniques. Debit cards are issued with standard bank accounts and are issued for e-commerce purchase. They are preferred by sellers because payment is more guaranteed by the bank. Smart cards are physical cards that must be inserted into a smart card reader before purchases can be made. Since such card readers are not yet a feature of many home computers, the use of smart card for purchases on the internet is not popular.[109]

Without prejudice to the popularity or otherwise of any of the methods of payment in electronic commerce, an ideal Electronic Payment System (EPS) has the following characteristic features:

- It is available to all buyers.
- It is available to all sellers.
- It is internationally accepted.
- It is able to handle both large and small payments.
- It results in immediate, unconditional settlement of the payment obligation.
- It has very low or zero costs.
- It has in-built security.
- It is confidential between the parties.[110]

Payment system in electronic commerce is not without its disadvantages. The risk of interception of payment messages remains and there is no protection in respect of goods or services which are inadequate or not supplied. Also there is no time-to-pay feature.[111]

CYBER CRIMES AND ELECTRONIC COMMERCE

With the advent of the Internet, cyber crimes have been on the increase. Cyber Law and Regulations have therefore become emerging fields in various jurisdictions. Cyber Law apparently encompasses cyber crimes, electronic commerce, freedom of expression, intellectual property rights, jurisdiction and choice of law, and privacy rights.[112] Cyber criminals have, over the years, adopted services of innovative strategies

[107] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 115.
[108] Ibid.
[109] Akomolede I . 'Taxation and Payment System in Electronic Commerce' (2008) 1 (1) Lead City University Law Journal (LCULJ) 184.
[110] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 115.
[111] Ibid 118.
[112] See Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 1068.

to induce and trap the internet users into craftily designed schemes that are more stealthy and sophisticated than ever before.[113]

In Nigeria, one of the challenges to effective electronic commerce system is inadequacy of law. The efforts of the Economic and Financial Crimes Commission (EFCC) in combating crimes committed on the internet are highly commendable. However, inadequacy of laws has been a clog in the realisation of the dreams towards eradicating or combating cyber crimes. In fact, the probable way of proving the commission of internet crimes is by circumstantial evidence as the crime can even be committed right inside the culprit's room. In the Court of Appeal case of *Harrison Odiawa v Federal Republic of Nigeria*[114]Dongban-Mensem JCA held on the nature of internet crimes and the extent of circumstantial evidence as the plausible means of discovering exploiters of Information Technology in the Commission of crime as follows:

> It is like the crime of armed robbery. The only difference here is the words, the internet, letters and telephoned, are the "arms" rather than "guns" and other lethal weapons. The criminal can commit his crime in the comfort of his bedroom. The common feature of the two crimes are the planning and executions; like the armed robbers who sometimes use masks, with internet robbery, the perpetrators, employ all sorts of gimmicks to cover up their trails.
>
> The point one strains to make here is that circumstantial evidence is the only plausible if not probable means of discovering the true monsters and exploiters of the I. T. (Information Technology) in the commission of crime.[115]

Various types of cyber crimes have been identified in various jurisdictions where cyber laws and regulations have been enacted and these include fraud, forgery, computer sabotage, hacking, unauthorized copying of computer programs, cyber stalking, phishing, data and Information theft, criminal intimidation, outraging the modesty of women and violation of privacy.[116]

CHOICE OF LAW AND JURISDICTIONAL ISSUE

Of all the banes confronting e-commerce activities, not in the least is choice of law and jurisdiction. In the Nigerian context, this stems from inadequacies in laws, institutions and policy as well as infrastructural and manpower needs.

With regard to laws, the general trend has been to adapt laws fashioned for off-line transactions to e-commerce situations where no laws or no adequate laws are on ground to address any issue arising out of e-commerce transactions. Where there are laws or adequate laws, problems of choice of law hardly arise, especially where the transaction took place within the same territorial jurisdiction. The laws fashioned for off-line transactions to e-commerce where there is no law or inadequate law include the common law of contract generally, the Statute of Frauds, Bills of Exchange Act, Communications Act, Consumer Protection Council Act, Evidence Act, National Information Technology Development Agency Act and various[117] Criminal Legislations, among others.

[113] Vivek Sood, *Cyber Crimes, Electronic Evidence and Investigation Legal Issues* (Nabhi Publications, New Delhi, India, 2008) 63.
[114] (2008) All FWLR (Pt 439) 436.
[115] Ibid, 473-474.
[116] See generally, the United Nations Manual on the Prevention and Control of Computer-Related Crime.
[117] Prof. Bolaji Owasanoye, 'Findings from Review of Laws for Social and Economic Development in Nigeria'.

Most emerging economies have enacted laws and subscribed to international policies, conventions and regulations on e-commerce.[118] Jurisdiction over cyber crimes has been an area of debate. While it is argued by many authors and jurists that since the internet is a borderless world, a separate regulatory law is required, and that the internet is a separate jurisdiction, others argued that the internet is part of this physical world and not divorced from it, hence the law of jurisdiction applicable in the real world should apply to the virtual world as well.[119]

The issue has always been, especially in international transactions, which court assumes jurisdiction in resolving disputes arising out of the transactions between the parties in view of the singular fact that the parties may be residing in different jurisdictions with different legal systems?[120] Although an e-commerce transaction may contain an agreed choice of law, other laws may be applicable in addition.[121]

The question that usually comes to mind is: when an online purchase is made, either directly or through the intervention of an electronic robotic agent, has the buyer stepped into a new place or simply used a different means of communication, much like a telephone fax or satellite.[122]

In *U.S. v Thomas*[123] when Thomas argued that given the nature of digital technology, he did not 'push' pornographic picture into Tennessee. Rather they were 'pulled' into that jurisdiction by someone there whose computer could gather the O's and I's from his server and create a pornographic picture.

Where the parties are domiciled in a contracting state under the Brussels Convention, the rules of the convention are applicable,[124] while the rules of common law are applicable where the parties are not domiciled within a contracting state. Where, however, parties to the internet contract are citizens of countries that have ratified the Rome Convention, then the provisions of the Rome Convention shall apply in determining which law to apply.[125]

DATA PROTECTION

The rise in Internet based transactions over the last few years has resulted in a vast increase in the amount of personal and financial information being transmitted.[126] In some economies, individual's right to privacy is considered as a human right to be protected by the state. In particular, in view of the increasing capacity for automated storage and processing of data of a personal nature, specific legal and technical provisions to protect fundamental rights and freedom become necessary.[127] The thrust of the problem associated with

[118] For instance Section 4 of the Indian Information Technology Act, 2000 provides that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is rendered or made available in an electronic form; and accessible so as to be usable for a subsequent reference.
[119] Vivek Sood, *Cyber Crimes, Electronic Evidence and Investigation, Legal Issues*, 108.
[120] Akomolede TI, 'Contemporary Legal Issue in Electronic Commerce in Nigeria' (2008) 11(3) PER/PELJ 2 <http:www.puk.ac.za/opencms/export/puk> accessed on 11 December 2009.
[121] Clive Grigras, *The law of the internet*, 62.
[122] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 643.
[123] 117 S. Ct 74 (1996) cited in Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000, E-commerce, Data Protection & the Internet)* 644.
[124] Brussels Convention on Jurisdiction and Enforcement of Judgments in civil and Commercial Matters 1958.
[125] The Rome Convention on the Law Applicable to Contractual Obligations 1980.
[126] Swindells C. and Henderson K., 'Legal Regulation of Electronic Commerce'.
[127] Rodney D. Ryder, *Guide to Cyber Laws (Information Technology Act, 2000 E-Commerce, Data protection & the Internet)* 422-423.

data protection in e-commerce was captured by Lord Hoffman in *R. v Brown* [128] where it was held as follows:

> Vast amounts of information about everyone are stored on computers, capable of instant transmission anywhere in the world and accessible at the touch of a keyboard. The right to keep oneself to oneself, to tell other people that certain things are none of their business is under technological threat.

Unlike in some developed countries[129] (or even developing countries), there is no specific legislation on data protection presently in Nigeria. While right to private life[130] as enshrined in the Nigerian constitution can be referred to as protecting personal data, there is a need for specific law on the subject. Privacy concerns are being raised in many countries around the world and some countries have enacted laws, implemented industry self-regulations, or instituted administrative solutions designed to safeguard their citizens' privacy.[131] The European Union (EU) is leading the way in this sphere and by its implicit linkage of standards of data protection in any country to trade relations with itself, the EU is pushing for change across the globe.[132]The right of privacy is also guaranteed by both the European Convention on Human Rights and the United Nations Universal Declaration of Human Right.[133]

The United Nations Commission on International Trade law (UNCITRAL) also provides for legal recognition of data messages. Information cannot be denied legal effectiveness, validity or enforceability solely on the ground that it is in the form of a data message.[134]

In Nigeria, some bills are already on the way for the protection of electronic transactions.[135] The principal body for the Nigerian information technology policy is the National Information Technology Development Agency (NITDA), which developed a Nigerian Information Technology (IT) Policy. The IT Policy identifies some of its objectives as promoting legislation for the protection of online business transactions, privacy and security and enhancing freedom and access to digital information at all levels while protecting personal privacy. The policy also ensures the protection of individual and collective privacy security and confidentiality of information.[136]

CONCLUSION

In this paper, attempt has been made to discuss the contemporary legal issues in electronic commerce. The fact is no more in dispute the electronic commerce is now part of our daily lives. Electronic Commerce gives business access to a vast number of consumers and gives business access to each other. E-commerce activity in Nigeria is steadily growing as a result of vast improvement in telecommunications services. The

[128] (1996) 1 ALLER 545, 556.

[129] For instance, there is Australian Federal Privacy Act 1988 as amended by the Privacy Amendment Act 1990; UK Data Protection Act 1984; German Federal Data Protection Act revised in 1990; Singapore Computer Misuse Act 1994; US Privacy Protection Act 2000.

[130] See Section 37 of the Constitution of the Federal Republic 1999.

[131] William J. Clinton and Albert Gore, Jr. 'A Framework for Global Electronic Commerce' <http://www.buscallegis-cij.utsc.br/revistas/index.php/buscalegis/article/viewFile/32002/271>accessed on 02 September 2010.

[132] Assafa Endeshaw, *Internet and E-commerce Law* (Prentice Hall Pearson Education Asia, Pte Ltd, 2001) 12. See also William J. Clinton and Albert Gore, Jr. 'A Framework for Global Electronic Commerce.'

[133] Swindells C. and Henderson K., 'Legal Regulation of Electronic Commerce'.

[134] See Article 5 of the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 <http://www.uncitral.org/pdf/english/texts/electcom/05-89450-Ebook. pdf>accessed 24 August 2010.

[135] For instance, the Nigerian government sponsored the Computer Security and Critical Information Infrastructure Protection Bill (otherwise known as the Cyber Crime Bill. See privacy International http://www.privacy.International.org/article.html?cmJ347]=x-347-559 511> accessed on 04 September 2010.

[136] Privacy International <http://www.PrivacyInternational.org/article.8html?cmJ347]=x-347-559511>accessed on 04 September 2010.

advances in the telecommunications market, and the explosion in the number of subscribers has demonstrated the potential market for information communication technology services generally in Nigeria.

The relative infancy in the introduction of electronic commerce in commercial activities in Nigeria has brought with it thorny and fundamental issues that requires legal and regulatory frameworks for effective and efficient implementation of electronic commerce in Nigeria. The benefits of the e-commerce system cannot be over-emphasised. This, notwithstanding, the rate at which fraudsters are manipulating access to internet to perpetrate crimes is of legal consideration. This is because both the buyer and seller on the Internet may be transacting business across the border. The party who has committed himself and performed his obligation in the transaction may find it extremely difficult to understand whether or not the other party will also be committed to the transaction. The position has been put succinctly by Lord Denning in *Thornton v Shoe Lane Parking*,[137] where he held thus:

> The customer pays his money and gets a ticket. He cannot refuse it. He cannot get his money back. He may protest to the machine, even swear at it. But it will remain unmoved. He is committed beyond recall. He was committed at the very moment when he put his money into the machine

The conclusion that can be drawn here is that people should get involved in internet transactions and be careful and prudent with a defined business strategy. It is hoped that when considering internet-related legislations being pass into law, the government will consider the adverse effect of created by cyber crimes and provide necessary safeguards to protect the citizens from being victims of internet fraudsters.

Government itself must be internet-friendly by setting the internet access and use as a priority to encourage foreign investments in domestic businesses. Similarly, researchers and software architects should endeavour to always create secure systems that would eliminate the need for anti-virus products in the computers meant for use in developing countries.

[137] (1971) 2 QB 163 at 169.