



Journal of Information, Law and Technology

Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and Judiciary

Dr. Gbenga Bamodu

Lecturer, Faculty of Law, University of Essex, Colchester and Barrister & Solicitor of the Supreme Court of Nigeria.

oobamodu@essex.ac.uk

This is an adapted version of a paper presented at the 'e-judiciary' conference organised by the National Information Technology Development Agency (NITDA) of Nigeria on the theme 'Information Technology in the Nigerian Judicial System' at Abuja between March 22 and 24 2004. The author would like to express his gratitude to the anonymous reviewers for their helpful comments on the draft of this article. He also acknowledges that he alone is responsible for any errors that appear in this article.

This is a **refereed** article published on: 30 November 2004.

Citation: Bamodu, 'Information Communications Technology and E-Commerce: Challenges and Opportunities for the Nigerian Legal System and the Judiciary', [2004 \(2\)](#) The Journal of Information, Law and Technology (JILT).
<http://www2.warwick.ac.uk/fac/soc/law2/elj/jilt/2004_2/bamodu/>.

Abstract

Nigeria, like many other countries, is aspiring to develop legislation to facilitate electronic commerce specifically and the use of information communications technology generally. This article addresses some of the challenges that the legal system and the judiciary will have to tackle in this process and highlights some of the opportunities arising from properly addressing the issues arising from the advent of the information communications technology revolution.

Keywords: E-commerce, Top Level Domains (TLDs), Second Level Domains (SLDs), country code TLDs, Electronic contracts.

1. Introduction: The Nature of the Debate

It is of credit to the Nigerian government and also, in particular, the National Information Technology Development Agency (NITDA) that in the past few years much effort 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 IT policy and the 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 Transactions Bill [\[1\]](#) currently going through the legislative process, in encouraging capacity building and in introducing the Mobile Internet Units among other things are encouraging. [\[2\]](#)

The advantages attending the global information communications technology revolution are well documented and need not be restated at great length presently beyond stating that they 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. With regard to the benefits of information communications technology, particularly from the perspective of developing countries such as Nigeria, even the United Nations recognises that information communications technology could be a contributing factor to achieving its Millennium Development goal of the reduction of poverty and of economic development generally. [\[3\]](#) Nevertheless, it remains important to address the challenges that the information communications technology revolution throws up for the legal system and to consider the ways to maximise the opportunities that it opens up at the same time.

It is a factor, not exclusive to Nigeria, that hitherto the rules of law in existing legal systems 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 the 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 with 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 maximising their benefits.

As mentioned earlier, an electronic transactions bill is presently going through the legislative processes in Nigeria. This bill addresses 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 the future. [4] 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 regulatory regime should be put in place concerning the issuing and distribution of electronic money in smart cards and other media [5] ; and, to what extent should the contents of websites be regulated particularly in terms of offensive material or material contrary to public policy. In relation to the last example, there seems to have been some advance since, according to news reports, [6] the Working Group on cyber-crimes set up by the government has produced a draft Cyber-Crimes Act to address various types of criminal activity that are computer related.

The matters mentioned in the preceding paragraph are flagged up as examples of some of the wider matters on which policy and legislative decisions will become inevitably necessary. The rest of this paper considers some other specific areas where the law will need to strive to keep up with developments in information communications technology and how those developments impact the activities of economic actors, contracting practices and general inter-personal exchanges and transactions. It is also sought to point out some issues and 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. In this light, four specific areas are selected for further exploration. Two of the areas (the administration of the .ng domain name and the law of evidence relating to electronic documents) are surrounded by controversy and debate in Nigeria and in the other two areas the law could do with further development and greater clarity. There are other areas of the law concerning information communications technology and electronic commerce that are in need of further legal development and clarity, i.e., electronic payments, regarding which some products are already beginning to emerge, but the discussion here is confined to the four selected areas for reasons of conciseness and because they are considered of more immediate importance to the foundational growth of electronic commercial transactions in Nigeria.

2. The Administration of the .ng Top Level Domain

As this has been a matter of some amount of controversy lately, it is worth flagging up some of the issues arising from the administration of a country code Top Level Domain (TLD), in this case, the .ng TLD. Every computer connected to the Internet has a unique address, known as its Internet Protocol (IP) address, which other computers use to identify it and to route data intended for that computer. Technically, this IP address consists of a string of four numbers separated by dots such as 24. 48. 36.72. As such numbers are much more difficult to remember than words, especially, recognised words and names, the system of Universal Resource Locators (URL) was introduced to provide a word based referencing system that makes it easier to find

resources on the Internet. Thus, instead of using the numbers that constitute the IP address of NITDA, for example, it is easier to use the URL <http://www.nitda.gov.ng/> which is the website address of NITDA. A crucial part of the URL is the domain name of the person or organisation that operates the website associated with the particular URL. The domain name system allows for the use of easily remembered words and names as part of the URL of a website operator. It is not only a useful mnemonic device but also one that allows website operators to incorporate their preferred, well known or even trade mark names as part of the URL for their website.

Domain names operate in a hierarchical format of Top Level Domains (TLDs), Second Level Domains (SLDs) and so on. The Top Level Domains fall into two categories which are *generic* TLDs including, for example, domains ending with .com, .net, .org among others and *country code* TLDs (ccTLDs) which are those ending with two letters associating the domain with a particular country such as .UK for the United Kingdom, .za for South Africa and .ng for Nigeria. Beneath the TLDs, especially country code TLDs, are second and third level domains denoting further particulars of the host and operators of a particular website. Globally, a number of registrars have now been licensed to register domain names falling in the generic TLD categories and they all subscribe to the Dispute Resolution Policy and Rules of the Internet Corporation for Assigned Names and Numbers (ICANN), which is the body with overall responsibility for the administration of the domain name system. The focus here will be on the administration of country code TLDs and, in particular, the .ng domain.

As has been pointed out elsewhere [7], the operation of ICANN's policy, as reflected in two important documents, RFC 1591 [8] and ICP-1 [9], involves the assignment of the administration of ccTLDs to a designated manager, who must be on the Internet, charged with operating and supervising the domain name system in the country concerned and that for each domain, there must be an administrative contact, who must reside in the country concerned, and a technical contact who, does not necessarily have to reside in the country. [10] The Nigerian ccTLD dispute centres around efforts to secure the re-delegation of the administration of the .ng ccTLD to a Nigerian non-profit organisation. Here, additional reasons are provided as to why securing such a re-designation is desirable and is in the best interests of the Nigerian and the global Internet communities.

From a technical perspective in the first place, administering the Nigerian country code TLD requires the maintenance and operation of a .ng name server. As the country code TLD is now recognised as a public resource, the best course is that such a server should be acquired, maintained and operated by a government designated or approved body (whether a public or private entity) in the interests of the Nigerian and global Internet communities. [11] Secondly, there are policy and legal matters arising from the operation of the country code domain that, even if not necessarily requiring direct governmental involvement in the operation of the country code TLD, at least requires government backing and some form of legitimacy for the body charged with its administration. For example, a decision would have to be made about the categorisation of second level domains in particular and how to make them reflect the kind of activities that the operators of a particular web site are involved in. For instance, would .gov.ng be reserved only for website operators that have a connection to government? Would .ac.ng be reserved only for institutions of higher education?

Would .sch.ng be reserved for schools and .co.ng for companies? Surely, the resolution of these matters should reflect national policy principles and objectives as well as applicable laws in each area.

Another crucial aspect of the management of the country code TLD relates to the introduction and operation of domain name dispute settlement machinery for tackling disputes that will inevitably occur over rights to use particular domain names. This does not seem to be a matter that is attracting much attention in Nigeria at the moment, [12] but as more and more people, businesses and organisations start to establish websites, disputes over domain names are likely to arise. Two domain name dispute proceedings that have connections to Nigeria, although decided by *fora* located outside Nigeria, demonstrate the potential for disputes over domain names when the .ng domain is fully functioning.

In the WIPO arbitration of *Shell International Petroleum Co. v Allen Jones* [13] a chap, who the tribunal ultimately regarded as a fraud, registered the domain name www.shell-nigeria.com (the hyphen is significant). When registering the domain name with the concerned registrar, he gave a supposed Yahoo e-mail address matching that of a 16 year old 'computer engineer' called 'Afez Adeyemi'! With this domain name he set up a website, which he claimed belonged to a supposed, but in the end fictitious, company called 'Shell Petroleum NG Unlimited' and from where he was offering consignments of oil at heavily discounted prices. The website copied information from the website of the well known Shell Oil Company and was sufficiently similar to the legitimate company's website that at least one person intending to enter into a contract to the tune of \$25,000 thought he was dealing with Shell. The legitimate Shell Oil Company's website address for its Nigerian business is www.shellnigeria.com i.e. different from that registered by the fraud by only the missing hyphen. The WIPO panel decided that the registered domain www.shell-nigeria.com infringed the unregistered/common law trademark 'Shell Nigeria' belonging to the genuine Shell Oil, which that company had used as part of its own registered domain name of www.shellnigeria.com.

The second case example is from the decision of the American-based National Arbitration Forum in the case *Gallup Inc. v Jerome Obinabo*, [14] in which the respondent had registered the domain names 'africagalluppoll.com', 'nigeriagalluppoll.com', 'igbogalluppoll.com' and 'yorubagalluppoll.com'. These registrations were challenged by Gallup Inc, a company that was accepted to be the largest and most well known provider of polling services in the US and in the world. Gallup argued that under ICANN's dispute settlement rules, the domain names registered by the respondent were confusingly similar to the trademarks in which they had rights, that the respondent had no rights or legitimate interest in respect of the registered names and that the domain names had been registered in bad faith. In the end, the arguments of the complainant were accepted and it was decided that the domain names must be transferred to Gallup Inc.

The examples above are disputes that have occurred under the generic .com TLD. It is suspected strongly that when the .ng domain is fully functional and domain names under it are readily available there is likely to be more cases of this nature. What this means is that whichever body ends up in charge of administering the .ng domain must have a sound dispute resolution policy in place. A mechanism designating *fora* and procedures for dispute resolution will also likely be necessary. Fortunately, there are a

number of jurisdictions whose experiences can be drawn upon in establishing the best approach for Nigeria on these matters. The underlying fundamental point that all these examples further demonstrate is that governmental authorisation or support (at the least) will be required for the body that will be responsible for administering the .ng TLD. [\[15\]](#)

3. Conflict of Laws Issues Arising from Internet/E-Commerce Transactions

In the information and electronic commerce age, more and more Nigerians will be involved in activities that have connections to countries other than Nigeria. Surfing the Web in itself is an activity that is connected to other countries in the sense that the computers, the servers and hosts, that are accessed, as well as the providers of the services offered through them, will be overseas in many cases. It is also important to bear in mind that a very large number of the Nigerians so using the World Wide Web will be ordinary consumers and not necessarily commercial people who may have more business savvy. At some point or other, disputes are likely to arise out of activities, the transnational activities, conducted on the Web. Possible examples include: dissatisfaction with goods bought or services procured over the Web and fraud on the consumer (e.g., by fraudulent website operators or by hackers who steal financial information). Even in the realm of tort, imagine the very possible scenario that an article is published on the Web and that the publisher is based abroad (US, Australia or indeed anywhere), but the article can be read on computers in Nigeria and it is alleged that the article is defamatory of a person resident in Nigeria. Does this amount to defamation (slander or libel?) in Nigeria and do the Nigerian courts have competence to adjudicate defamation proceedings over the article? These are all real possibilities and types of situations that might lead to judicial proceedings before the Nigerian courts or before alternative dispute resolution bodies.

In addition to issues of substantive law that these matters raise, there are some important matters of adjectival law that Nigerian courts will need to be alive to. For instance, in the example where a Nigerian consumer orders goods on the Web, pays by his credit card or smart card, and receives goods which he is dissatisfied with, it is easy to assume that one of the various Nigerian sale of goods laws applies and that the consumer should have rights under the provisions of such laws. That is to jump the gun, however, as there is a strong possibility that by the terms of the contract of purchase between the Nigerian consumer and the Web merchant the law of another country applies. Most Web merchants have a clause in the terms and conditions link on their Web site that the law of a particular country, usually their own home country, applies to the transaction. Thus, for example, the conditions of use on the retailer Amazon's website (www.amazon.com) provide that the law of the American state of Washington applies to transactions concluded at the website. Now, by the doctrine of party autonomy and freedom of contract, it is more or less universally accepted that parties to a contract having connections to more than one country, subject to some exceptions, are free to select whichever country's law they wish to govern the transaction. This principle is reflected in Nigerian law for example in s. 47 of the *Arbitration Act* - perhaps not the most elegantly drafted provision - which allows the arbitral tribunal to decide disputes 'in accordance with the rules in force in the country the parties have chosen as applicable to the substance of the dispute.'

Policymakers evaluating the myriad ways in which legislation regulates e-commerce transactions and activities will necessarily have to consider whether or not there are

areas of policy where Nigerian laws should apply to consumer transactions mandatorily, irrespective of the right of the parties to select which country's law is to govern the transaction. Even with regard to formalities, there might be a case to protect consumers against being caught unawares by such choice of law clauses.

Since low value transactions are not likely to come before the courts because of the costs (and length of time) involved in judicial proceedings, the likelihood is that disputes over such consumer transactions will be resolved by one of the online dispute resolution schemes now emerging. Nevertheless, it is still important for the Nigerian courts to be alive to the conflict of laws dimension of transactions that have connections to more than one country. Nigerian courts have certainly shown themselves to be competent at dealing with cases of all sorts including complex international commercial disputes. There have been cases, [16] however, where the courts have proceeded on an almost automatic assumption that Nigerian law applies and overlooked that preliminary matter. [17] It is desirable that the courts, when faced with disputes having connections to more than one country, clarify the matter of the governing law [18] and remove any possible speculation that the Nigerian courts adopt the oft criticised *lex fori* approach.

Related to the issue of governing law is that of jurisdiction, an issue of perhaps even greater importance to the courts and the judiciary, as jurisdictional issues figure prominently in both in e-commerce transactions and in examples of alleged defamation on the Internet, such as the ones outlined above. With regards to contractual transactions, a contract that contains a choice of applicable law is also likely to contain a clause setting out where disputes between the parties will be resolved, whether in a court or by arbitration, and the location of the tribunal. Thus in the example of www.amazon.com referred to earlier the conditions of use also provide that disputes arising from transactions concluded on the site are to be referred to arbitration, once again in the American state of Washington. Thus if a Nigerian e-purchaser who buys goods on those terms and is unhappy with them were to sue in the Nigerian courts, the Web merchant could apply for a stay of proceedings or even that the action be dismissed as being in violation of the agreement to go to arbitration in Washington. Would the Nigerian purchaser have the means and the 'facility' to go to Washington? Is he going to be deprived of a remedy because of the lack of means and facility to go to Washington?

In Europe, the European Union countries have introduced a regime that is intended to protect the consumer in such cases. The rules that apply for determining jurisdiction in civil and commercial cases [19] provide *inter alia* that a consumer can bring an action against the other party to a contract (who is not also a consumer) either in the consumer's own home state or in the courts of the home state of the other party. On the other hand, a consumer is to be sued only in the country of his domicile if he concludes a contract with another person who directs their commercial or professional activities to his home state 'by any means'. One of the means for directing commercial or professional activities nowadays is by the Web. The question then is whether a website operator directs his commercial or professional activities to *every* state in which the website is or can be accessed --- virtually every country in the world! Thus if a Nigerian merchant establishes a website and enters into a transaction through that website with a consumer from within the European Union, EU law stipulates that if the Nigerian merchant wishes to sue that consumer he must pursue

the consumer to his home state in the European Union. Naturally, in the interest of protecting Nigerian consumers, especially where most do not have easy opportunity to travel abroad, particularly to Western countries, it seems a reasonable course for Nigerian lawmakers to at least consider similar provisions in respect of actions against Nigerian consumers. It is recognised that there are some potential negatives, for example, whether fraudulent Nigerians will see that as some form of shield and whether foreign e-merchants will be reluctant to deal with Nigerian consumers. It is believed, however, that these difficulties are not so great as to prevent the consideration of similar provisions or a tailored version in the interest of consumers.

In the defamation [20] example referred to earlier, say the article is published in an American newspaper that is also published online. Would the Nigerian person who alleges that he has been defamed have to go to America to sue? Does the ability to read the article in Nigeria mean that the article is 'published' in Nigeria? [21] Such matters should be of interest to Nigerian media groups who publish electronic versions of their newspapers, which many Nigerians living abroad find extremely useful, because if the online edition of a Nigerian newspaper publishes allegedly defamatory material about someone living in Australia [22] or the UK [23] or in any number of other countries except the US [24], there is the strong likelihood that the newspaper will be sued in those countries, even though the allegedly defamatory material was written in Nigeria and originally appeared in a paper version of a publication that has circulation only or principally in Nigeria. These are actually issues of both substantive as well as conflict of laws.

On the matter of jurisdiction, in a case where the person alleging defamation is a Nigerian, even if it is decided that the article first published in an American newspaper is also published in Nigeria, do the Nigerian courts have jurisdiction over the American publisher or can they exercise long-arm jurisdiction to drag the foreigner before the forum? The rules of court do tend to permit jurisdiction to be obtained over a person outside the territorial limits of the court if the courts, in their discretion, grant leave that the foreign based person should be served with the court's writ outside the jurisdiction. The foreign defendant may choose, however, to ignore or challenge jurisdiction so obtained. Moreover, if the court's judgment needs to be enforced abroad [25], some countries tend not to enforce judgments granted where jurisdiction was obtained by long arm means and particularly where the defendant did not take part in the proceedings. [26]

The foregoing are just some of the matters of adjectival law that the Nigerian courts will probably have to address in this information communication technology age. One other related issue of adjectival law but considered deserving to be discussed separately, not being a matter of conflict of laws, is that concerning the use of electronic documents as evidence in dispute resolution and especially in judicial proceedings.

4. Internet/E-Commerce Transactions and the Law of Evidence

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. 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 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.

The Nigerian *Evidence Act* allows the *contents* of documents to be proved by primary or secondary evidence [27] though it also provides, curiously at first sight, that 'documents' (not mentioning the 'contents' in this particular respect) must be proved by primary evidence except as mentioned in the Act. [28] The apparent disparity is resolved, however, by section 97 of the Act which provides that 'secondary evidence may be given of the existence, condition or contents of a document' in circumstances listed within the provision. Primary evidence of a document includes the document itself or each counterpart or each part of a document produced in counterparts or in parts, or each product of one uniform process of production but excluding copies of a common original. [29] The secondary evidence that is admissible in the circumstances listed within section 97 of the Evidence Act includes a written admission of the existence, condition or contents of the original document, in some specific circumstances 'any secondary evidence' of the contents of the original – presumably including oral testimony, a certified copy of the original of a public document or of a document of which the Act or any law permits the use of a certified copy. In the specific case of a document which is an entry in a banker's book, copies could be permissible as secondary evidence provided that the book in which the entries copied were made was at the time of making one of the ordinary books of the bank, and the entry was made in the usual and ordinary course of business, and the book is in the custody and control of the bank. [30]

There has been some academic debate in Nigeria recently on the issue of whether computer print-outs, which have been held to be admissible in evidence by the Nigerian Supreme Court in *Anyaebose v R T Briscoe Nigeria Ltd* [31], should be admissible as primary evidence or should always only be secondary evidence. [32] In the *R T Briscoe* case, the Nigerian Supreme Court confirmed in a unanimous decision that computer print outs are admissible in evidence under what is now section 97 of the *Evidence Act* with the underlying assumption by all the members of the court that

such evidence amounts to secondary evidence. An interesting point that seems to have been overlooked in the judgment and in the academic debate is that of the status of the original data of which the print-out was admitted as secondary evidence.

The provisions, presently section 97 of the Evidence Act, on which the decision in the *R T Briscoe* case was based, contemplate the admissibility of secondary evidence of a 'document'. Thus the computer printout that was admitted as secondary evidence must have behind it an original 'document'. The question then is whether the original computer data satisfies the meaning of 'document'. Normally, original computer data being in intangible form would not satisfy the traditional meaning of a document, which contemplates reduction to some tangible form. However, section 2 of the Nigerian Evidence Act provides:

‘ “document” includes books, maps, plans, drawings, photographs and also includes any matter expressed or described upon *any substance* by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording the matter.’ (Present author’s emphasis)

It seems that, albeit unwittingly, the definition of 'document' will permit computer data to be treated as documents. Firstly, the definition is non-exhaustive of what amounts to documents because of the use of the word 'includes'. Secondly, the definition encompasses within the meaning of 'document' expression by letters, figures or marks on any substance, with 'substance' not being confined to *tangible* substances. Accordingly, despite oversight of the necessity for a document of which a printout could be admissible as secondary evidence, the Nigerian Supreme Court did not necessarily reach a wrong decision. On the point of whether computer print-outs are always only secondary evidence or whether they can be primary evidence, it is believed that the underlying assumption by the Nigerian Supreme Court that they are secondary evidence is also correct in that the print-out will always be copies of the original data input which, being in intangible form, cannot itself be produced as evidence.

Whilst the decision of the Nigerian Supreme Court in *Anyaebosi v R T Briscoe* is supportable, a more recent decision of the court immediately below it, the Nigerian Court of Appeal, is rather regrettable. In *Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor.* [33], the Court of Appeal held that the admission in evidence by the court of first instance of computer print-outs as secondary evidence of entries in a banker's book was wrong because, among other things according to the court, the relevant provisions of section 97 of the *Evidence Act* do not contemplate information stored 'other than in a book'. The relevant provisions are set out below:

97 (1) Secondary evidence may be given of the existence, condition or contents of a document in the following cases –

(a) when the original is shown or appears to be in the possession or power –

(i) of the person against whom the document is sought to be proved

(h) when the document is an entry in a banker's book.

(2) The secondary evidence admissible in respect of the original documents referred to in the several paragraphs of subsection (1) of this section is as follows –

(a) in paragraphs (a) {relating to when the original is shown or appears to be in possession or power of the person against whom the document is sought to be

proved}, (c) and (d) any secondary evidence of the contents of the document is admissible;

(e) in paragraph (h) {i.e. relating to banker's books} the copies cannot be received in evidence unless it be first proved that the book in which the entries copied were made was at the time of making one of the ordinary books of the bank, and that entry was made in the usual and ordinary course of business, and that book is in the custody and control of the bank

In interpreting these provisions *Omage JCA*, with whom Muhammad and Mohammed JJCA concurred, held that the bank's computer print-out of the record of transactions between it and its customer should not have been allowed in evidence by the court below because firstly, applying section 97(1)(a) above, the computer record *per se* had never been in the possession of the customer and, secondly, that the provisions above do not contemplate information stored other than in a 'book'. The part of the decision, in *Omage JCA*'s judgment dealing with this issue was rather very brief and, sadly, reflects a lack of deep consideration of the import of the concerned provisions. The other members of the court simply concurred with the lead judgment and thus, unfortunately, there was not the benefit of specific discussion of the issue by the other members of the court.

An examination of the decision in light of the provisions being considered leads to no other conclusion than that the Court of Appeal was, unfortunately, in error on this point. Firstly, the court appears to have conflated the provisions relating to when the original is in the possession of the person against whom the document is sought to be proved {section 97(1)(a) and (2)(a)} with the separate and alternative provisions dealing with entries in a banker's book {section 97(1)(h) and (2)(e)}! The court seemed to consider the two separate provisions as necessary requirements for admissibility of secondary evidence of entries in a banker's book when only the second set of provisions is relevant in this specific regard. Secondly, the court did not discuss what amounts to an entry in a banker's book and specifically whether a bank's computer records, not the printout, could amount to a banker's book for the purposes of the relevant provisions. It seemed to have assumed that a bank's computer records could not amount to a banker's book. The definition of 'banker's books' in the Evidence Act was not considered although even that might not necessarily have been conclusive one way or another.

Section 2 of the Evidence Act provides that 'the expressions relating to 'bankers' books' include ledgers, day books, cash books, account books and all other books used in the ordinary business of a bank.' Again, this is a non-exhaustive definition because of the use of the word 'include'. While it does not specifically say that bankers' books include computer entries relating to the kinds of things it mentions, it does not seem to exclude that possibility either. In an age of increasing computerisation of banking and general business processes with the advantages that that entails, a more liberal interpretation of bankers' books to take account of current prevailing realities might have been expected particularly because, as has been noted prior to this decision [\[34\]](#), Nigerian courts had previously adopted a liberal approach in relation to the admissibility of bankers' books in evidence. It is hoped that the higher Nigerian superior courts (the Court of Appeal or the Supreme Court) will reconsider this decision at the earliest opportunity.

A more welcome recent development is that the current *Draft Nigerian Electronic Transactions Bill* seeks to lay down rules for the admissibility of electronic evidence and on the weight to be attached to such evidence. In the first place, the bill provides that if information is required to be presented or retained in its original form, that requirement is met by a document if there exists a reliable assurance as to the integrity of an electronic document from the time that the information was first generated up to the point of its receipt by the addressee. [35] It then provides further that in legal proceedings, nothing in the law of evidence shall apply as to deny the admissibility of an electronic document in evidence on the sole ground that it is in the form of an electronic document or on the ground that it is not in its original form if it is the best evidence that the person adducing it could be reasonably expected to obtain. [36] After these provisions which do the basic, that is, allow for electronic documents to be admissible in evidence, it is further provided that 'due evidential weight' is to be given to information in an electronic document and that in assessing this evidential weight regard is to be had to: (a) the reliability of the manner in which the information was generated; (b) the reliability of the manner in which the integrity of the information was maintained; (c) the manner in which its originator was identified; and (d) any other relevant factors as may be identified from time to time. [37]

The guidelines on the evidential weight to be accorded to electronic evidence are quite general and the courts will still have to attend to issues of detail. Although the bill proposes that information in electronic form should not be denied admissibility in evidence solely on the ground that it is in electronic form or not original, the provisions do not prevent challenges to the integrity of the information, which can indeed go into the issue of admissibility particularly if it can be shown that the information had been compromised and that the attending electronic document is not what it claims to be. In working out the naturally related issue of reliability and what weight is to be attached to the electronic document if it is admitted in evidence, some of the factors that will be relevant include: in the first place whether the electronic document is tendered by or through the person who actually and directly created it; the security and control procedures over the information system of the person who tenders the electronic document or of the proprietor of the information system from which it emanates, if they are different persons; whether trusted third party authentication or certification was involved and so on. These matters can still be explored in further depth and there are other related matters that have not been mentioned, but attention must now be turned to matters of substantive law.

5. Formation of Electronic Contracts

The two most common ways of entering into contracts on the World Wide Web are by exchange of e-mail or by what is known as 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. [38] 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?

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. 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) known as the *Model Law on Electronic Commerce* of 1996. The current *Draft Electronic Transactions Bill* being sponsored by NITDA follows the same pattern by providing [39] 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.

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. Most take 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 [40] 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 [41] in the prospective Act. The definition of 'signature' [42] 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.

It is 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 admissibility as evidence. [43] 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* [44] discussed earlier. The use of digital signatures provided by a certification service provider will ensure that at least some steps would be taken 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.

Turning to more substantive matters concerning the formation of an electronic contract, 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 Dave in Lagos sends an offer by e-mail to Jan in Amsterdam. Jan sends an acceptance by e-mail from Amsterdam to Lagos. The e-mail is sent in Amsterdam at 1100 GMT but does not reach Lagos until 11.15GMT and is not seen by Dave until 1300 GMT. Was the contract made in Lagos or Amsterdam? Was it made at 1100, 11.15 or 1300GMT?

With regard 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. 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 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 discredibly? 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 realised 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. [45] 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! [46] So e-merchants beware or *caveat* e-merchant!

Indeed 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.

The *Draft Nigerian 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: 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. For example what is meant by 'an information system of the addressee'? 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, another interesting issue 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 (*consensus ad idem*) of the parties concerned although of course the law has long recognised the ability to enter into contracts through agents (*qui facit per alium facit per se*) but that recognition was traditionally limited to agency capacity by human beings or recognised juridical persons such as companies and so on.

In the United States, the possibility of contracting through electronic agents is now legally recognised. 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. [47] These are matters that will have to be addressed by future e-commerce legislation in Nigeria but it is believed that Nigerian common 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.

When the contract is validly concluded, 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 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.

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 (as in most web click contracts), 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. 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. An example was given earlier concerning the requirement that a consumer in the European Union should normally be sued in the EU country of his domicile. 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.

Broadly speaking, 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. [48] In relation to distance selling contracts [49], 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 (extending up to at least seven *working* days) to cancel the contract without giving any reason. 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. 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 content of these legislative provisions.

6. Conclusion

The advent of the information communications technology revolution poses new challenges for the legal system and the administration of justice. It requires a re-orientation of the traditional focus of laws on paper-based transactions to accommodate the new methods of communication. These challenges must be addressed through carefully considered policies, legislation and judicial decisions. The prize is the enormous economic and social benefits that attend the advent of information communications technology. In a developing economy where there is concern about marginalisation and a keen desire to take advantage of some of the benefits that attend globalisation, it is a prize worth the efforts necessary to address the challenges posed by the information communication technology revolution. It is to be hoped that the Nigerian legislature will expedite action on the enactment of the Electronic Transactions Bill and other legislation that will facilitate the growth of electronic commercial transactions. Similarly, it is to be hoped that the Nigerian judiciary will apply itself to tackling the legal issues that will arise out of electronic commercial disputes in an informed and accurate manner that enhances confidence in the sector.

Notes and References

[1] I am grateful to the staff of the Legal Department of the Nigerian National Information Technology Development Agency (NITDA) for providing me with a copy of the draft Nigerian Electronic Transactions Bill which, unfortunately, has not been otherwise circulated widely. It is also understood that a private member's bill on the same subject is also being (or at least was at one time) sponsored by a member of the House of Representatives. See Tony Anyanwu, 'Internet Commerce: Awaiting Legislative Intervention' available as of 19/03/04 at: <<http://www.tonyanyanwu.com/cservices/billsfolder/download/bills21.pdf>> (cached copy still available through google.com).

[2] See Gabriel O Ajayi, 'NITDA and ICT in Nigeria' paper presented at *Round Table on Developing Countries Access to Scientific Knowledge, The Abdus Salam ICTP Trieste, Italy* (2003), text available online as of 13/05/04 at:

<<http://www.ejds.org/meeting2003/ictp/papers/Ajayi.pdf>>.

[3] See e.g. *Economic Commerce and Development Report* (UNCTAD 2002).

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

[5] See generally, O Ajayi, 'Leap Frogging the African Economy into the 21st Century through Electronic Smart Cards: The Legal Perspective' (1998) 2 *Modern Practice of Finance & Investment Law* 113.

[6] See *The Daily Times* of 12 March 2004.

[7] 'Gbenga Bamodu, 'Towards a Resolution of the Controversy over the Administration of the Nigerian Country Code Domain (.ng ccTLD)' available online as of 29/04/04 at: <<http://www.nigeriavillagesquare1.com/Articles/bamodu.html>>.

[8] Request for Comments Memorandum of 1994 titled 'Domain Name System Structure and Delegation', text of which is available online as of 29/04/04 at: <<http://www.isi.edu/in-notes/rfc1591.txt>>. RFC 1591 is originally a document of the Internet Engineering Task Force (IETF) - which deals with the technical operation of the Internet – but is now administered by the ICANN which has taken over the function of the Internet Assigned Numbers Authority (IANA) concerning the allocation of Internet Protocol (IP) address space, 'protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management'; see <<http://icann.org/general/>>, especially paragraph 1.

[9] Internet Coordination Policy Document titled 'Internet Domain Name System Structure and Delegation (ccTLD Administration and Delegation)' text of which is available online as of 29/04/04 at: <<http://www.icann.org/icp/icp-1.htm>>.

[10] These designated authorities are regarded as trustees of the domain and, in particular, the designated manager is trustee of the ccTLD for both the nation concerned and the global Internet community.

[11] It is understood that the Nigeria Internet Group, a non-profit organisation concerned with the promotion of Internet awareness in Nigeria and supposedly at one time licensed to operate the .ng TLD, did, some time ago, acquire technical equipment worth about N15 million to host the .ng TLD. See Welcome Address by Mr. Jim Ovia, President of the Nigeria Internet Group to the 2nd NIG Convention/AGM held in Lagos on November 7-8 2003. Text available as of 29/04/04 at: <<http://www.nig.org.ng/papers%20PRESENTED.htm>>.

[12] See, however, M. Ajakpovi, 'Domain Names and Trademarks in Nigeria' in (2001) 2 *Modern Practice of Finance & Investment Law* 202.

[13] WIPO Case No. D2003-0821 of 18 December 2003, text available online as of 29/04/04 at: <<http://arbitrator.wipo.int/domains/decisions/html/2003/d2003-0821.html>>.

[14] Claim No. FA0110000100756 of 2 January 2002, text available online as of 29/04/04 at:

<<http://www.arb-forum.com/domains/decisions/100756.htm>>.

[15] Since the presentation of the original conference paper the author has submitted proposals to the National Information Technology Development Agency, on invitation, about the rules, structure and dispute resolution mechanism concerning the administration of the .ng top level domain.

[16] See e.g. *Societe Generale de Surveillance SA v Rastico Nigeria Ltd.* [1992] 6 NWLR 93; *Nahman v Wolowicz* [1993] 3 NWLR 443 and *Adesanya v Palm Line Ltd* (1967) LLR 18; cf. *Ghassan Hallaoui v Grosvenor Casinos* [2002] 17 NWLR 28, 45 (part 795).

[17] See further on this issue: 'Gbenga Bamodu, 'Jurisdiction and Applicable Law in Transnational Dispute Resolution before the Nigerian Courts' (1995) 29 *The International Lawyer* 555.

[18] In the absence of statutory provision, the rules that the court will apply on the conflict of laws issue of applicable law will be derived from the common law as one of the sources generally of Nigerian law. For example, in *Benson v Ashiru* (1967) N.M.L.R. 363 at 365, Brett JSC said that '[t]he rules of the common law of England on questions of private international law apply in the High Court of Lagos.'

[19] Council Regulation 44/2001, 'The Brussels I Regulation', especially articles 15 and 16.

[20] Issues arising in defamation and the law of tort generally in connection with ICT are considered further in a second paper to be presented by the present author later on at this conference.

[21] There are other matters still: in particular who is the publisher or responsible for disseminating the article when many host/server computers will probably copy and

pass on the material at several stages before it is downloaded in Nigeria. Will the proprietors of such Web hosts/servers also be potentially liable?

[22] See *Dow Jones & Company Inc v Gutnick* [2002] HCA 56.

[23] See *Harrods v Dow Jones* [2002] EWHC 1162.

[24] In contrast to the Australian and UK approach American courts, following what is sometimes described as the 'single publication' rule, tend to regard online defamatory statements as only actionable where it was not uploaded outside the jurisdiction unless there was a manifest intent to aim the website or the posted material at an audience in the concerned jurisdiction. See e.g. *Young v New Haven Advocate & the Hartford Courant* 315 F 3d 256 US Court of Appeal, 4th Circuit (2002).

[25] Incidentally, the enforcement of foreign judgments is an important third aspect of adjectival law in international commercial dispute resolution but the topic is beyond the scope of the present paper.

[26] See for example *Ghassan Hallaoui v Grosvenor Casinos* [2002] 17 NWLR 28, 45 (part 795) and also section 9 of the UK's *Administration of Justice Act 1920*.

[27] See section 93 of the *Evidence Act* cap 112 Laws of the Federation of Nigeria 1990.

[28] Section 96 of the Nigerian *Evidence Act*.

[29] Section 94 of the Nigerian *Evidence Act*.

[30] On the admissibility of computer print-outs in relation to entries in bankers' books specifically, see text accompanying notes 33-34 below.

[31] [1987] 3 N.W.L.R. 84 (part 59).

[32] See Y. Osinbajo, 'Problems of Proof of Computer and other Electrically Generated Evidence in Legal and International Financial Transactions' (1991) *Gravitas Review of Business & Property Law* 89; Y. Osinbajo, 'Admissibility of Computer-Generated Evidence under Nigerian Law' (1990) 1 (1) *JUS* 11; T. Osipitan, 'Admissibility of Computer Print out under Nigerian Law' (1995) 2(2) *Lawyers' Bi-Annual* 236 and T. Osipitan, 'Legal Impact of Technology on Rules of Evidence in Banking and Commercial Litigation' (1998) 2 *Modern Practice of Finance & Investment Law* 71.

[33] [2001] 16 N.W.L.R. 510 (part 740).

[34] See O Oyewo, 'Admissibility of Banker's Books and Records under Nigerian Law' (1998) 2 *Modern Practice of Finance & Investment Law* 155.

[35] Section 5(1)(a) of the current draft.

[36] Section 6(1) of the current draft.

[37] Section 6(2) of the current draft.

[38] 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.

[39] Section 1 of current draft.

[40] Section 4 of current draft.

[41] '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.'

[42] 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'.

[43] This recommendation was acknowledged and reflected in the final Communiqué produced at the end of the aforementioned e-judiciary conference.

[44] Note 13 above.

[45] See: <

http://www.golds.co.uk/articles/articles_ec_conditions_online_business.htm>.

[46] *ibid.*

[47] See further, R.T. Nimmer, 'Principles of Contract Law in Electronic Commerce' in I. Fletcher *et al* (eds) *Foundations and Perspectives of International Trade Law* (Sweet & Maxwell, 2001).

[48] See generally 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).

[49] See generally 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.

Books

Nimmer, R T (2001) 'Principles of Contract Law in Electronic Commerce' in Fletcher I, Mistelis, L & Cremona, M (eds), *Foundations and Perspectives of International Trade Law* (London: Sweet & Maxwell).

Journal Articles

Ajakpovi, M (2001) 'Domain Names and Trademarks in Nigeria' 2 *Modern Practice of Finance & Investment Law* 202.

Ajayi, O (1998) 'Leap Frogging the African Economy into the 21st Century through Electronic Smart Cards: The Legal Perspective' 2 *Modern Practice of Finance & Investment Law* 113.

Bamodu, G (1995) 'Jurisdiction and Applicable Law in Transnational Dispute Resolution before the Nigerian Courts' 29 *The International Lawyer* 555.

Osinbajo, Y (1991) 'Problems of Proof of Computer and other Electrically Generated Evidence in Legal and International Financial Transactions' *Gravitas Review of Business & Property Law* 89.

Osinbajo, Y (1990) 'Admissibility of Computer-Generated Evidence under Nigerian Law' 1 (1) *JUS* 11.

Osipitan, T (1998) 'Legal Impact of Technology on Rules of Evidence in Banking and Commercial Litigation' 2 *Modern Practice of Finance & Investment Law* 71.

Osipitan, T (1995) 'Admissibility of Computer Print out under Nigerian Law' 2(2) *Lawyers' Bi-Annual* 236.

Oyewo, O (1998) 'Admissibility of Banker's Books and Records under Nigerian Law' 2 *Modern Practice of Finance & Investment Law* 155.

Salu, A O (1998) 'Cyberlaws – Its Application and Enforcement in Nigeria' 2 *Modern Practice of Finance & Investment Law* 10.

Soyele, O (2000) 'The Internet & Emergent Regulatory Legal Framework: A Selective Appraisal' 4 *Modern Practice of Finance & Investment Law* 166.

Conference Proceedings

Ajayi, G O (2003) 'NITDA and ICT in Nigeria', *Trieste Round Table on Developing Countries Access to Scientific Knowledge, The Abdus Salam ICTP*, 2003. Available online at:

<<http://www.ejds.org/meeting2003/ictp/papers/Ajayi.pdf>>.

Ovia, J (2003) 'Welcome Address', Nigeria Internet Group Convention/AGM, Lagos, November 2003. Available online at: <<http://www.nig.org.ng/papers%20PRESENTED.htm>>.

Cases and Page Numbers Within Cases

Adesanya v Palm Line Ltd (1967) LLR 18

Anyaebose v R T Briscoe [1987] 3 N.W.L.R. 84

Benson v Ashiru (1967) N.M.L.R. 363 at 365

Dow Jones & Company Inc v Gutnick [2002] HCA 56

Gallup Inc. v Jerome Obinabo National Arbitration Forum Claim No FA0110000100756 of 2 January 2002

Ghassan Hallaoui v Grosvenor Casinos [2002] 17 NWLR 28 at 45

Harrods v Dow Jones [2002] EWHC 1162

Nahman v Wolowicz [1993] 3 NWLR 443

Nuba Commercial Farms Ltd v NAL Merchant Bank Ltd & anor [2001] 16 N.W.L.R. 510

Shell International Petroleum Co. v Allen Jones WIPO Case No D2003-0821 of 18 December 2003

Societe Generale de Surveillance SA v Rastico Nigeria Ltd. [1992] 6 NWLR 93

Young v New Haven Advocate & the Hartford Courant 315 F 3d 256 US Court of Appeal, 4th Circ. (2002)

Statutes

Administration of Justice Act 1920 (UK), section 9

Electronic Transactions Act (Draft Bill) (Nigeria), sections 1, 4, 5, 6 & 15

Evidence Act cap 112 Laws of the Federation of Nigeria 1990, sections 93, 94, 96 & 97

Uniform Computer Information Transactions Act 1999 (USA) sections 102 & 107

Subsidiary Legislation

Consumer Protection (Distance Selling) Regulations SI 2334 of 2000

Unfair Terms in Consumer Contracts Regulations SI 2083 of 1999

Directives and Regulations

Council Regulation 44/2001, 'The Brussels I Regulation', articles 15 & 16

Directive 97/7 of 20 May 1997

Directive 93/13 of 5 April 1993

Links to Uniform Resource Locators (URLs)

<http://arbiter.wipo.int/domains/decisions/html/2003/d2003-0821.html>

<http://www.arb-forum.com/domains/decisions/100756.htm>

<http://www.ejds.org/meeting2003/ictp/papers/Ajayi.pdf>

[http://www.golds.co.uk/articles/articles ec conditions online business.htm](http://www.golds.co.uk/articles/articles_ec_conditions_online_business.htm)

<http://www.icann.org/icp/icp-1.htm>

<http://www.isi.edu/in-notes/rfc1591.txt>

<http://www.nigeriavillagesquare1.com/Articles/bamodu.html>

<http://www.tonyanyanwu.com/cservices/billsfolder/download/bills21.pdf>