40

UNIZIK LAW JOURNAL

Vol. 11, 2015.

Stay of proceedings – A progressive Impetus to an Organic Growth of the Dynamics of Customary Arbitration in Nigeria **C.A Obiozor**

Right to Freedom from Discrimination and the Indigeneship Factor in Public Sector Employment in Nigeria **O.N Ogbu**

Interdisciplinary Approach to Legal Scholarship, Lawyering and Adjudication: Prospects and Challenges **E. Amaoji/ J.O Ezeanokwasi**

Appraisal of the Development of a Legal Framework for the Elimination of Gas Flaring in Nigeria **T.C Eze**

The Travails and Challenges of Democracy in Nigeria: A Study of Impunity and Ignominy **K.C Uwadineke / I.K.E.Oraegbunam**

Mediation as a Virile Alternative Dispute Resolution Mechanism in Nigeria **S. A Bello and Abifarin Olufemi**

An Indepth Analysis of JC E and Superior Responsibility as Basis for Individual Responsibility under International Law **B.O Abegunde**

Admissibility of Electronic Evidence under Section 84 of Evidence Act 2011: Examining the Unresolved Authentication Problem **I.K.E. Oraegbunam**

Presumption of Customary Law and Islamic Marriages Based on Cohabitation: Need for Guidelines in Interpreting Section 166 of the Evidence Act 2011 **M. Attah**

Examination of the Claw-Back Clauses in the African Charter on Human and Peoples' Rights **N. Oluchukwu Odiaka**

Section 12 of the Legal Practitioners Act Examined **O. B. Akinola**

Nigeria's Response to Quist Close as a Security Interest: The Need for Public Acceptance **E. E Ekanem and E.E Ntekim**

Fourth Tier of Government: District Council in Selected Jurisdictions a *Sine quo non* for a Sustainable Federalism in Nigeria **D.U: Ibe and Edeko Maria Omozele**

The Impact of Counter – Terrorism Laws on the Protection of Human Rights and Fundamental Freedoms **O.A. Arebamen & P.E. Oamen**

NNAMDI AZIKIWE UNIVERSITY, AWKA, NIGERIA

UNIZIK LAW JOURNAL

VOL. 11, 2015

Published By
FACULTY OF LAW
NNAMDI AZIKIWE UNIVERSITY AWKA,
ANAMBRA STATE, NIGERIA

Admissibility of Electronic Evidence under Section 84 of Evidence Act 2011: Examining the unresolved Authentication Problem*

Abstract

Electronic evidence is now admissible in Nigeria *vide* the Evidence Act 2011. Yet unresolved is the problem of authenticity of the electronic documentary evidence. Section 84 sets out the requirements for admissibility of certain types of computer-produced evidence. As part of the conditions of admissibility, the Act lays down minimum authentication requirements. However, the Act arguably only applies to evidence that would otherwise be excluded as hearsay and not to direct or real evidence. In such a case, the law contains no clear statements as to how that evidence should be authenticated. On hermeneutic and comparative approaches to English and Nigerian positions, the paper finds and argues that admissibility and authentication are separate issues, and that the failure to treat them independently gives rise to needless confusion. This failure also directs attention away from the urgent need for clear rules governing the authentication of computer evidence. It is therefore observed that the relevant provisions of the Act are due for review just on arrival. Without this review, a substantial obstacle to digital communication, data storage, e-commerce, diligent prosecution at the event of cyber criminality, for instance, shall have been inaugurated.

Introduction

June 2011 witnessed the enactment and promulgation of a new Evidence Act by the National Assembly[1]. With the enactment of the Act[2], a sigh of relief is heaved

* **Ikenga K.E.Oraegbunam, PhD (Law), PhD (Phil.), PhD (Rel. & Soc.), MEd, BL**, Senior Lecturer, Department of International Law & Jurisprudence, Faculty of Law, Nnamdi Azikiwe University, P.M.B. 5025, Awka, Anambra State, Nigeria. Email: ikengaken@gmail.com; ik.oraegbunam@unizik.edu.ng. Phone Number: +2348034711211.

[1]Evidence is item 23 of the Exclusive Legislative List (See part 1 of 2nd Schedule of 1999 constitution as amended). The main source of the law of evidence in Nigeria is the Evidence Act. The Act has passed through history. It was first passed in 1943 as Evidence Ordinance but came into operation in 1945. The provisions of the Act were taken mainly from the Digest of the Law of Evidence by Sir James Fitzgerald Stephen which in itself was an attempt to codify English Common Law Rules of Evidence. Before the Evidence Act came into operation in 1945, the English Common Law of Evidence was the applicable law in our Magistrates' Courts and High Courts, then known as the Supreme Court. Until 1945 there was no significant local legislation in Nigeria bothering on the law of Evidence. Therefore Nigeria, because of her colonial link with England relied on the English Common Law of Evidence. The authorities for the application of this law were contained in some of the legislation enacted in the colonial days. Even under the repealed Evidence Act, by virtue of section 5(a) which provides that "nothing in this Act shall prejudice the admissibility of any evidence which would apart from the provisions of this Act be admissible", the English common Law acted as a supplementary law of Evidence which could always be resorted to. With the exception of some minor amendments of the Evidence Act effected between 1948 and 1958 and another minor amendment in 1999, the provisions of the Act have largely been in force until it was recently repealed by the National Assembly. Prior to its abolition, the old Evidence Act had been criticized for being anachronistic by various lawyers, judges, legal

as the law to a great extent provides for the admissibility of electronic and computer generated evidence. The Act widens the scope of the definition of documents to include computer print-outs, compact disks, electronic messages, video tapes, and so on. Hence document now includes –

> (a) books, maps, plans, graphs, 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 that matter;
>
> (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it, and
>
> (c) Any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it;
>
> (d) Any device by means of which information is recorded, stored or retrievable including computer output.[3]

Similarly, for the first time in a Nigerian evidence statute, the word 'computer' is defined as "any device for storing and processing information, and any reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process"[4].

Evidence Act 2011 (EA) repeals the Evidence Act[5] that was enacted in 1943 and which came into force in 1945. The enactment of Evidence Act 2011 came after series of calls from the legal, judicial, and human rights communities as a result of

writers and concerned persons. An unsuccessful attempt to revise the law was made in 1998, when an Evidence Bill was prepared but was never enacted by the government and its successors. The Evidence Act which was in operation for about 64 years before its repeal had become too obsolete as a lot of developments in areas such as information technology etc had gone way beyond what the statute could envisage at its enactment. For example, under the operation of this Act, when information recorded or stored in the memory of a computer is printed out in paper, it is not easy to say whether the version in the memory is a document nor is it easy to assert that the printout is an original or a copy. However these issues and many more have been put to rest by the enactment of the Evidence Act, 2011 by the National Assembly on 3rd June, 2011. This Evidence Act 2011 has now repealed the Evidence Act 1945 which was contained in Cap E14, Laws of the Federation of Nigeria, 2004. By virtue of section 259, the new Evidence Act shall be cited as Evidence Act, 2011.

[2] Evidence Act 2011.

[3]Evidence Act, 2011, section 258.

[4]*Ibid.*

[5] Cap E 14, L.F.N. 2004.

the inadequacy of its predecessor in determining issues that bordered on the new trends of Information and Communication Technology. Issues of admissibility of computer print-outs of banks' statement of accounts, video tapes, compact disks, and the like materials inaugurated long debates in courts, thereby advancing a negative toll on precious judicial time needed, as it were, for much desired dispensation of legal justice. A result was that courts and judicial panels differed among themselves as to the admissibility of electronically generated evidence. Besides, the definition of 'documents' did not seem to cover computer programmes and products. It required only an activist judge to exploit the idea of judicial notice which recognizes progress in science and technology, *inter alia*, to admit in evidence computer generated materials. But even at that, the atmosphere of the old evidential regime could not allow the activist judges to attach much weight to the evidence as it was often classified as merely secondary. This state of affairs held sway for almost seven decades even when human activities and transactions were fast growing soft and paperless. The result became for a long time an ugly legal monster and constituted a clog in the wheel of judicial progress and justice dispensation.

An instance of the ugly effect of this lacuna in the law is in relation to combating cybercrimes. Thus, it may happen that while much time, resource and effort may have been expended in the course of investigation, yet the product of such forensic activity may not be allowed to be adduced as evidence in relevant criminal proceedings. This is a matter of admissibility. It goes without saying that the issue of admissibility is quite cardinal in the dispensation of legal justice[6]. According to Walden, "admissibility is concerned with the ability to submit evidence into court for consideration by the judge and/or jury"[7].

In civil law inquisitorial systems, the investigating judge generally determines the issue. In common law adversarial systems of which Nigeria is a part, complex admissibility rules have historically existed to govern the issue, based in relevant evidence statute and case law. In this paper, the interest is to critically examine the extent to which the forensic product derived from computers and networks may be admitted to or excluded from evidence tendered before the Nigerian courts. The study is founded on the fact that challenges to the admissibility of such evidence are a key defence strategy in relevant

[6] Admissibility is a major concept in Evidence law. Unfortunately, it was not defined anywhere in the Evidence Act 2011. However, admissibility involves the court's acceptance of relevant evidence adduced by a party to a suit. Once evidence is relevant to a fact in issue it is admissible except, it is too remote to be material, or is excluded by the provisions of a statute. Admissibility is a matter of law.

[7] I.Walden, *Computer Crimes and Digital Investigation*, (New York: Oxford University Press, 2007), p. 367.

prosecutions[8]. The more vulnerable computer and network-derived evidence is to exclusion[9], the more problematic will prosecutions based on computer generated evidence be.

Limits of Admissibility of Electronic Evidence under the Repealed Evidence Act[10]

The repealed Evidence Act did not recognize electronically generated evidence. This worked a lot of hardship on litigants, and sometimes occasioned injustice in cases where parties relied heavily on electronic evidence; as the hands of judges were tied to convict on only admissible evidence. This situation was illustrated in a plethora of cases[11]. In *UBA Plc v Sani Abacha Foundation for Peace and Unity (SAFPU)* the court while applying the dictum of the Supreme Court in *Yesufu v African Continental Bank (ACB)*[12] stated thus:

[8] R. Smith, P. Grabosky, and G. Urbas, *Cyber Criminal on Trial*, (New York: Cambridge University Press, 2004), p 62.

[9] Evidential exclusions can be broadly distinguished into two categories: the first focuses on the material itself, the second on the circumstances surrounding the obtaining of the material for use as evidence. In the first, the unreliability of the material is the primary policy concern, either because the person was not witness to the facts, as in hearsay, or because the reliability of the source from which it is derived is considered vulnerable, as computers were treated in the early years. In the second, the policy concerns are the activities of the investigators in obtaining the material. This can be further subdivided into 'protective exclusion', where the objective is to protect the investigative process, which is the case with the current inadmissibility of intercept product, data obtained 'in transmission', and 'fairness exclusions', where the rights of the defendant have been, or could be, infringed were the material to be admitted. These exclusions may occur through statutory prohibition, through judicial determination or a combination of both. A court has the right to exercise discretion not to admit evidence based on a concern to ensure the fairness of any criminal proceedings and, to a lesser extent, to regulate the conduct of law enforcement agencies. In the latter scenario, evidence may be excluded because it involved the commission of an offence by the investigator, or a breach of a procedural obligation designed to protect the rights of the suspect. Evidential exclusion may operate as an alternative to a judicial stay for abuse of process. Law enforcement agencies must therefore give mind to such exclusionary rules in the course of a digital investigation, since their application may be triggered by the choice and manner in which the investigation is carried out. The following briefly reviews four historical grounds for excluding digital evidence, the first two of which have largely or wholly disappeared (See O. Kerr, "Lifting the "fog" of Internet surveillance: How a suppression remedy would change computer crime law", 54 *Hastings Law Journal* 805 (2003). See generally I. Walden, *op. cit*, p.368)

[10] Evidence Act, Cap E 14, L.F.N. 2004.

[11] *UBA Plc v. SaniAbacha Foundation for Peace and Unity (SAFPU)*[2003] FWLR (pt 178) 978, CA; *The Federal Republic of Nigeria v. Femi Fani-kayode* Case No. FHC/L/523C/08 of 26/3/2009 (Unreported) decided on 25/2/2010.

[12] *Yesufu v. ACB*[1976] 1 ANLR (pt 1) 328; (1976) 4 SC 1 at 16.

> Though the appellant's counsel made reference to the modern day practice of using computer in the day-to-day business of the bank, it is my opinion that the law still remains as it is. It has not been amended by the National Assembly, although it is high time they did that and I am bound to apply the law as it is.

In the light of *UBA Plc v SaniAbacha Foundation for Peace and Unity (SAFPU)* and *Nuba Commercial Farms Ltd &Anor. v NAL Merchant Bank ltd &Anor*[13], legal writers, judges and lawyers clamoured for the amendment of the Evidence Act. The repealed Evidence Act did not make provisions for electronic evidence and its admissibility. Due to this fact some Nigerian scholars and jurists were of the view that electronic evidence could not be rightly adduced in evidence and thus inadmissible[14].On the other hand, some legal writers and jurists advocated a liberal approach and posited that electronic evidence could be rightly adduced by litigant under the provisions of the Evidence Act relating to relevancy[15].

The result is that the appropriate position was therefore neither here nor there. There was still a controversy as to whether electronic evidence was admissible in trials or not. If it were, were it to be primary or secondary evidence, or were it to be tendered as one of the hearsay exceptions? In addition, there was a problem of whether electronic evidence was documentary evidence. These problems characterized the evidential status of electronic evidence under the old Evidence Act's regime. Admissibility of electronic evidence suffered from the same uncertainty which plagued its evidential status. The issue as to whether or not evidence generated from electronic devices were admissible within the framework of the repealed Evidence Act was highly contentious in legal circles, as opinions were divided, even amongst the courts. Some of the issues bothering on electronically generated evidence that had come before the court for determination include the following:

(i) Whether or not computer printouts are admissible in evidence at all?

(ii) Whether or not computer printout should be treated as primary or secondary evidence or are they to be treated as one of the numerous hearsay exceptions?

[13] *Nuba Commercial Farms Ltd &Anor.v. NAL Merchant Bank ltd & Anor* [2001] 16 NWLR (pt 740) 510.
[14] *UBA v. SaniAbacha Foundation for Peace and Unity (SAFPU)*[2003] FWLR, (pt 178), 978; *Yesufu v. ACB Ltd*(1976) 4 SC 1 at 16.
[15] *Alero Jadesimi v. Egbe*[2003] 10 NWLR, (pt 827), 1 at 25.

(iii) Whether or not a computer printout not found physically with an accused but printed out of his e-mail box after his arrest can be said to be in his possession?

(iv) Whether or not computer storage devices are themselves documentary evidence?

(v) Whether a video compact disc (VCD) recorded from a television broadcast is admissible as original or secondary evidence?

(vi) Whether or not a VCD copied from a miniature tape is the primary or secondary evidence.

(vii) When a pen-recorder is downloaded into a laptop and copied into a VCD, which one is the primary or secondary evidence?[16]

The courts sometimes held electronic evidence admissible on the grounds that it was secondary evidence[17] or by giving a liberal interpretation to the admissibility of electronically generated evidence[18]. In *Esso West Africa Inc v T. Oyegbola,* the Supreme Court made its first notable pronouncement on admissibility of computer printouts, when it stated thus:

> The law cannot be and is not ignorant of the modern business methods and must not shut its eyes to the mysteries of computer. Modern times' reproduction and inscriptions on ledgers or other documents by mechanical process are common place and section 37 cannot therefore only apply to books of accounts.

It must be noted that this pronouncement was an *obiter dictum*. Ajileye J[19]is of the opinion that this pronouncement has an element of foresight because it was made in 1969 (about 43 years ago), when technological advancement was not this overwhelming. On other occasions, the court held electronic evidence inadmissible either because it did not fall within the definition of documents according to section 2 of the Evidence Act[20]or because it was not provided for by the Evidence Act[21]. In *Yesufu v. ACB*, the Supreme Court, in another *obiter dictum* and with an attitude different from that portrayed in its earlier pronouncement; sounded a note of warning, emphasizing the need for legislative

[16] A .O. Ajileye, *Admissibility of Electronic Evidence in Criminal Trials* .Paper delivered at Refresher Course for Judges and Kadis including All Judges Handling Economic Crimes in Nigeria, Abuja, 10 October 2010, p. 4.
[17] *Anyaebosi v. R.T. Briscoe Nig Ltd*(1987). 2 NSCC, 805.
[18] *Esso West Africa Inc v. T. Oyegbola*(1969) 1 NMLR, 194.
[19] Judge of the High Court of Kogi State, Nigeria.
[20] *Nuaba Commercial Ltd v. NAL Merchant Bank* [2001] 16 NWLR, (pt. 740), 510.
[21] *Yesufu v. ACB* (*supra*); *UBA v. SAPFU* (*supra*).

clarification before admitting documents generated from computers. The court said:

> ..... while we agree that for the purpose of sections 96(1) (h) and 37 of the Act, "bankers books" and "books of accounts" could include "ledgers cards", it would have been much better, particularly with respect to a statement of account contained in document produced by a computer, if the position is clarified beyond doubt by legislation as had been done in England in the Civil Evidence Act....

It is common knowledge that under the principle of *stare decisis*, an *obiter dictum*, a 'statement by the way', is not binding. It is a judge's passing remark which has little or nothing to do with the real issues for determination in the matter. It is the statement of the judge "by the way". It is, however, doubtful if any lower court can afford to treat an *obiter* of the apex court of the land with levity without reproof, as it is good law that an *obiter* of the Supreme Court, could as well, in certain circumstance, assume the status of a *ratio decidendi*. Consequently, these two conflicting *obiter dicta* of the Supreme Court in *Oyegbola's* case and *Yesufu's*case burdened the lower courts with the liberty of choosing which of the precedents to follow. The two pronouncements formed the benchmark to which reference was made by lower courts to determine whether or not electronically generated evidence was admissible. A court that was determined to admit electronic evidence readily found solace in *Esso v. Oyegbola*, while on the other hand, a court that was determined to reject same took succour in *Yesufu v. ACB*. For instance, in *Trade Bank v. Chami*[22], the provisions of section 38 of the repealed Evidence Act came up for consideration. By virtue of the provisions of the said section, entries into books of accounts regularly kept in the course of business are relevant whenever they refer to a matter into which the court has to inquire, but such statements shall not alone be sufficient evidence to charge any person for liability. Although the said section does not provide for entries in computers, or computer print-outs containing entries of account, the Court of Appeal, applying the Supreme Court dictum in *Oyegbola's* case held that section 38 of the Evidence Act should be interpreted to admit computer print-outs.

The court said:

> The section of the Evidence Act (supra) does not require the production of "book of account" but make entries into such book relevant for admissibility. Exhibit 4 is a mere entry in the computer or book of account. Although the law does not talk of "computer" or "computer print-out" it is not oblivious to or ignorant of modern business world and

[22] *Trade Bank v. Chami* [2003] 13 NWLR, (pt 836), 158.

> technological advancement of modern jet age. As far back as 1969, the Supreme Court in the case of *Esso West Africa v. T. Oyegbola*(1969) NMLR 194, 198 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....

On this authority the provisions of section 38 covers, in the respectful opinion of this paper, also electronic process such as computer and computer prints out comprised in Exhibit 4 are admissible ..."[23] In direct contrast to the above decision, is *UBA v. SAFPU*[24] where the Court of Appeal held that a statement of account contained in a document produced by a computer could not be admitted in evidence under the Evidence Act until certain sections of the Act were amended. The Court, while applying the dictum of the Supreme Court in *Yesufu v. ACB* stated thus:

> Though the appellant's counsel made reference to the modern day practice of using computer in the day-to-day business of the bank, it is my opinion that the law still remains as it is. It has not been amended by the National Assembly, although it is high time they did that and I am bound to apply the law as it is.

The court then added:

> It is quite unfortunate that in Nigeria no clarification has been done by way of amendment or promulgation of an Act to exempt the statement of account contained in a document produced by a computer from the conditions stated in section 97 of the Evidence Act 1990. Hence, I will not deviate from my primary function in interpreting the law as made by the legislature to that of law making. I therefore hold that the lower court was in error when it admitted Exhibit D2 in evidence in this case.

Numba v Commercial Forms Ltd &Anor v NAL Merchant Bank Ltd & Anor[25] was also decided along the same line. The most recent of the cases in this category is *The Federal Republic of Nigeria v Femi Fani-Kayode*[26]. It was an interlocutory ruling in which a Federal High Court in Lagos, rejected, as inadmissible, the computer print-outs tendered by the Prosecution in the trial involving a former Minister of Aviation on an allegation of laundering a sum of ₦4billion. The

[23] Per Salami, JCA, (as he then was).
[24] *Supra.*
[25] *Supra.*
[26] Case No.FHC/L/523C/08 of 26/3/2009 (Unreported).

computer printouts of the accused person's statement of accounts which the prosecution tendered as evidence were rejected by the trial court as inadmissible. Applying the Court of Appeal decision in *UBA v. SAPFU*, the court held that the provisions of section 97(1) (b) and (2) (c) of the Evidence Act do not cover the admissibility of computer printout even if they are duly certified and relevant. The Court then concluded thus:

> I must also express the view that there is the urgent need for an amendment of the Evidence Law to cover admissibility of document made by means of computer printout since it is clear that that technological method of producing document now forms part of day to day business transaction circle.

What these decisions demonstrate is that courts in Nigeria grappled and contended with how best to treat electronic evidence. There is, however, a consensus of opinion for an urgent need for legislative intervention. Nevertheless, it seems the decisions which held electronic evidence as admissible were preferred and more favoured by legal writers and jurists because of the imperative need of the judicial system to take cognizance of electronic evidence. In a bid to address this imperative need, the courts took the initiative and applied proactive interpretations to certain sections of the repealed Evidence Act for the purpose of admitting electronic evidence. There is no doubt that in all cases in which electronically generated evidence were rejected, a common premise on which such rejections were based was the fact that the Evidence Act did not recognize electronically generated documents. To remedy this situation, the court in a plethora of cases called on the National Assembly to amend the Evidence Act. However, the calls seemed to fall on deaf ears as the Evidence Act remained in operation for 63 years. In fact, in *UBA v. Tejumola & Sons Ltd*[27], the Court in accordance with the principle of separation of powers reiterated the duty of the National Assembly to make and amend laws when it stated thus:

> ..... the court is not the legislature, its duty is to interpret the law and apply it to facts in the administration of justice. It does not overstep its bound and trespass upon the sacred provision of the legislature. It is the province of the legislature to enact laws and amend or repeal laws. The court can only draw attention to areas of the law where amendment is required or desirable[28].

All the same, the pertinent question was, whether the courts should wait endlessly in utter helplessness, under the prevalent circumstances? And, whether the courts should continue to reject computerized documents and other forms of electronic

[27] *UBA v. Tejumola & Sons Ltd*(1988), 5 SC 264.
[28] Per Obaseki JSC.

evidence until the National Assembly amends the Act? In answering the questions, the court adverted its mind to certain matters such as the fact that continued rejection of electronic evidence portended serious dangers for the economy of the nation and the entire administration of justice. For instance, if all statements of account are to be excluded from proceedings in court on the ground that the Evidence Act does not recognize computerized documents, then, a serious clog has been introduced, surreptitiously, into the wheel of legitimate transactions and the administration of justice. This is because, most bank customers will simply take loans from banks and refuse to pay their debts because the computerized statements of account narrating the accumulated debt and interests cannot be tendered in evidence during debt recovery exercises or court proceedings by their banks[29]. Again, those involved in e-crimes would definitely have a field day because various e-mails, taxes and e-documents and other e-messages forwarded to their victims will be inadmissible. Above all, such negative impact may even touch on the integrity of the court, as the court is capable of being perceived, albeit wrongly, by the ordinary man on the street, as shielding criminals. The list of the negative impact of exclusion of computer generated evidence is endless.

The courts, therefore, took upon themselves the responsibility of interpreting the insufficient existing law progressively. The law remains a basic factor for making nations to advance or degenerate, as the case may be. Societies become dynamic through the application of the law. The advancement witnessed in technology demanded a proactive approach to the interpretation of the law. Some of these proactive approaches by the courts are delineated.

Under the regime of the repealed Evidence Act, the admissibility of computerized documents was put to rest by the Supreme Court in *Anyaebosi & Ors v. R.T. Briscoe Nig Ltd*[30]. In that case, the apex court endorsed the admissibility of computer printout as secondary evidence. The court held that computerized statements of account, after all, are not in the class of evidence which is completely excluded by the Evidence Act. Therefore, the computerized statement in issue in that case was rightly admitted as secondary evidence under Section 97(1) of the repealed Evidence Act. This judgment was seen as progressive. The Supreme Court in this case must have taken into consideration, electronic evidence and its present place in Nigeria within the globalised world and hence did not wait for the National Assembly to amend the law.

Furthermore, there is no gainsaying that by the virtue of section 5, the Act admits its inadequacies and accommodates the admissibility of other forms of

[29] A.O. Ajileye, *op.cit*, p.9.
[30] *Supra.*

evidence not covered by the Act. Oshipitan puts it more succinctly:

> The Evidence Act does not pretend to be an exhaustive legislation. It evidently does not cover the whole field of the law of evidence. The Act frankly admits its limitation and in-exhaustiveness in Section 5(a).[31]

Also, in *Alero Jadesimi v Egbe*[32], the Court of Appeal remarked as follows "under Section 5(a) of the Act, no piece of evidence can be excluded under the common law if the Evidence Act or any statute in force in Nigeria does not expressly render it inadmissible."

By far, the greatest challenge to admissibility of electronic evidence under the repealed Evidence Act related to the definition of the word 'document'under the Act[33]. The issue was whether or not the definition was wide enough to accommodate computer storage devices or stored representation records such as Portable Document Format (PDF) copies, e-mails, e-mail logs, word processing files on a computer or those records created by computer automatically, such as temporary internet files, cell phone records, computer log-in records, and so on. The tendency here was to restrict the definition of 'document' to paper-based materials, typically expressed in words and figures. However, it was submitted that the phrase "*and it includes any matter expressed or described upon any substance by means of letters, figures or marks or more than any one of these*" which was often overlooked could be interpreted to enlarge the scope of the meaning of the word beyond paper-based materials.

Furthermore, it was argued that the definition of the word 'document' under section 3 (1) of the Singapore Evidence Act is *in parimateria* with the definition of the word under section 2 of the Evidence Act. Therefore, since courts in Singapore have accepted that the definition of 'document' under their Evidence Act was wide enough to accommodate electronically generated documents; there was no reason why the same interpretation could not be applied in Nigeria. In the Singaporean case of *Megastar Entertainment Ltd v Odex Ltd*[34]the argument that the definition is broad enough to encompass information recorded in an electronic medium or recording device, such as a hard disk drive installed in a desktop computer or server computer was accepted.

Section 38 was certainly one of the obsolete provisions of the repealed Evidence Act. The section provides for "entries in books of account." It is a well-known fact, however, that commercial practices have gone beyond making entries in "books of account." Computer records now constitute the main source of

[31] *Supra.*
[32] T. Oshipitan as cited in A.O. Ajileye, *op.cit.* p.10.
[33] Evidence Act, Cap E 14, LFN 2004 , S.2(1).
[34] *Megastar Entertainment Ltd v Odex Ltd* (2005) 3 SLR 91.

business information today. Therefore, in *Trade Bank Plc v Chami*[35] the Court of Appeal per Salami JCA (as he then was) held that electronic processes such as computer and computer printouts are admissible.

Throughout the regime of the old Evidence Act there had been clarion calls for the Evidence Act to be amended to be at par with the realities of technological advancement and societal changes. The Act was described as "anachronistic and not in line with global reality[36]. In the same vein, in *Egbue v. Araka*[37], Pats Acholonu JCA (as he then was) had earlier observed thus:

> It must be clearly understood that our Evidence Act is now more than 50 years old and is completely out of touch and out of tune with the present scientific and technological achievements. Most of its sections are archaic and anachronistic and need thorough overhaul to meet the need of our times. But alas it is with us now like an albatross on our neck.[38]

Some of the reasons for the enactment of the new Evidence Act to provide for electronic evidence in particular are quite salient. The admissibility of electronic evidence under the repealed Evidence Act was uncertain. This uncertainty had grave consequences which included occasional occurrence of injustice because the issue of admissibility of evidence is crucial to any trial. Furthermore, certainty in law which is one of the basic features of the concept of law[39] was being questioned by the subsistence of this uncertainty. This uncertainty with its attendant problems was one of the reasons why the old Evidence Act was repealed and a new Evidence Act enacted to provide for electronic evidence and settle the dust that had hitherto surrounded its admissibility.

Moreover, in recent years, information and communication technology has advanced in leaps and bounds. Consequently, individuals and corporate bodies alike rely heavily on the usage of ICT as the world transforms into a global village at the speed of light. Today, a lot of transactions are done via cyberspace. There is also a great rise in e-crimes in Nigeria as evidenced by the rampant cases of account hacking, ATM frauds and internet fraudsters popularly known as "yahoo boys"[40]. These new developments are another reason why the new evidence Act had to be enacted to cover electronic evidence. Without such enactment perpetrators of e-crimes would have a field day, as they would be able to escape

[35] *Supra.*
[36] A.O. Ajileye, *op.cit*, p.3.
[37] *Egbue v. Araka*1996] 2 NWLR, (pt 433), p. 688.
[38] *Ibid.*
[39] F. Adaramola, *Jurisprudence*, 4th Ed. (Durban :Lexis Nexis Butterworths,2008), p. 232.
[40] A local term or slang to refer to people who dupe others especially foreigners through the internet.

the long arm of the law by taking advantage of the loopholes and silence on the issue of electronic evidence in the old Evidence Act.[41]

Generally, the legal system does not always keep up with the pace of technological development. There is always the need for legislative intervention either through amendments of existing laws or enactment of new laws. However, while other legal systems, such as, India[42], South Africa[43], United States of America etc, had in line with the tenet of sociological jurisprudence amended their Evidence Rules or Acts to accommodate these societal changes and technological advancement, Nigeria still depended on an Evidence Act handed down by the British colonial masters for over 60 years. This move by foreign legal systems to adapt to the changing times further emphasized the cogency for the amendment or repeal of the old Evidence Act to accommodate electronic evidence.

Admissibility and Authentication of Documents under Evidence Act 2011 (EA)

Before delving into the analysis of the rules governing admissibility and authentication of electronic evidence under EA, it is apt to show the nature of such evidence.Computer-related evidence falls into two clear categories. Each consists of information output by a computer, either as a result of some operation it has performed or as a hard copy of data stored in some permanent form (eg on magnetic disk). The first category is where the computer is used as a compact filing cabinet, in which are stored records of information provided to it by human beings. These records might be almost anything —academic records of students, observations of the weather, the serial numbers of cheques, minutes of a meeting --- but their essential characteristic for the purposes of admissibility is that they originate in an observation by a human. The second category consists of records generated directly by a computer, whether that which stores the record or another machine. Examples might be a system log for a mainframe installation, data received from a monitoring device such as a thermostat, or a record of an EDI (Electronic Data Interchange) message such as a purchase order produced automatically by a stock control system and transmitted to the supplier. Here the record is of an observation made directly by the machine without human intervention.

There are three reasons why a record produced by a computer might be inadmissible as evidence:

[41] *UBA v SAPFU (supra)*; *FRN v Abdul* (2007) 5 EFCLR, 204 at 228.
[42] *Information Technology Act, 2000* which amended the Indian *Evidence Act, 1872.*
[43] *Electronic Communications and Transaction Act 25 of 2002.*

(a). A record may be inadmissible because it is not an original. This does not appear to present any real problem in relation to computer records, as the original will in almost every case be a magnetically-stored version of the record which cannot be examined directly. Where the original is not available, the courts are prepared to admit properly authenticated copies.[44]

(b). A record may be inadmissible because it is a hearsay. A document is hearsay if it is a record of a statement made by a human being of some fact which that human being has observed, or some action in which that human being has been involved. The reason for the hearsay rule is that the primary source of evidence in common law is oral evidence, given by a witness, of facts observed by that witness. In its original form the hearsay rule prevented a third party from giving evidence that the original witness claimed to have observed or taken part in some activity. This was because the second witness could not be cross-examined as to the truth of the first witness's observations. Documents falling within the first category outlined above will therefore be hearsay for exactly the same reason. However, a document that does not contain a record of such a statement is not in fact hearsay. If the computer document is a record of observations made directly by the computer, for example records of an ATM transaction, then it will not be hearsay but direct or real evidence. In general, direct evidence is admissible per se, though there is some debate whether this applies to computer records.

(c). A record may be inadmissible because some rule of law prevents the evidence from being adduced. It appears that all computer records fall within the definition of a statement in section 258 of EA.[45]This provides that a statement includes "any representation of fact, whether made in words or otherwise", which definition is a verbatim recopy of the relevant part of the provision of section 5 of the English Criminal Evidence Act (CEA) 1992. Computer records are clearly statements of fact and therefore subject to the requirements of section 84 of the Act, which prevent the statement from being admitted unless the conditions laid down in the section are fulfilled. However, it should be noted that the English courts have held that direct

[44] C Reed, "Authenticating Electronic Mail Messages - Some Evidential Problems" (1989) *MLR* 49, pp.652-3.
[45] This is similar to the provisions of section 10(1) of Criminal Evidence Act 1992 (UK) and section 72(1) Police and Criminal Evidence Act 1984 (UK).

evidence produced by a computer is not subject to the hearsay rule.[46]Yet the English Divisional Court has also held that section 69 of Police and Criminal Evidence Act (PACE) 1984 (*in pari materia* with section 5 of English Criminal Evidence Act 1992 and section 84 of EA) does not apply where the computer has been used to calculate results, and thus produced direct evidence.[47]Some English law scholars argue that this state of affair together with the fact that the context of section 5 of CEA suggests that "statement" means hearsay statement and that PACE uses the same definition, supports the view that the requirements of CEA and PACE apply only to hearsay statements.[48] Whatever the correct position, it is indisputable that the uncertainty is another factor militating against the effective use of computer communications. The matter would not be different in Nigeria wherein the relevant provisions of the above English enactments have been adopted *ipsissimaverba*.

Be that as it may, the rules governing the admissibility of computer-related evidence in Nigeria are delineated in section 84 of EA. Computer related evidence concerns statements in documents produced by computer. The provisions of section 84 are summarized thus: Subsection (1) makes a computer generated statement admissible in both civil and criminal proceedings. Subsection (2) provides for the conditions to be fulfilled, which are that the computer must be in regular use to store or process information of activities carried on over that period; that such supply was made regularly, in the ordinary course of business; that the computer was operating properly, or where it was not, that it was not such as to affect the accuracy of the statement; that the information derived was supplied in the ordinary course of those activities. Subsection (3) provides for the ways in which the computer(s) performed the function. This could be by a combination of computers; or different computers operating in succession; or different combinations of computers operating in succession; or in any other manner involving the successive operation, whatever order, and shall be treated as constituting a single computer. Subsection (4) provides for the proof of any statement produced by a computer to be given in evidence, to be made by a certificate to that effect. Subsection(5) provides that information supply to a computer may be made either directly or by means of any appropriate equipment;

[46]*R v Wood* (1983) 76 Cr App R 23, *Castle v Cross* (1985) 1 All ER 87; see also *The Statue of Liberty* (1968) 2 All ER 195.
[47]*Sophocleous v Ringer* (1988) RTR 52.
[48] N Reville, "The Admissibility of Computer Statements in Criminal Trials"(1989)6 *Computer Law & Practice* 19.
p.20; M Silverleaf & C Reed, "Evidence" in Reed (ed.) *Computer Law, Blackstone Press* (London 1990) Ch.9, pp.180, 196.

that information duly supplied to a computer though outside the ordinary course of activities shall be deemed to be appropriately done, though, depending on the circumstances of the case.As codified under section 84 particularly in subsection (1), electronic evidence is now admissible evidence in any trial, whether civil or criminal.

The implication of this provision is that the precedent set by the Supreme Court's *dicta* in *Yesufu v ACB*[49], will outright be bad law today. However, this study doubts if the courts will follow the precedent laid in *Anyaebosi v R.T.Briscoe*[50] because the *ratio decidendi* is neither ad remnor in consonance with the provisions of section 84 (1). It is, however, submitted that the decision which the court will reach today should likely be the same as reached in *Anyaebosi v R.T. Briscoe.*

Besides, EA has resolved the primary-secondary evidence controversy in respect of computer generated documents.Section 85 permits the content of a document to be proved either by primary or secondary evidence, while section 88 is categorical in providing that documents (as distinct from contents) shall be proved by primary evidence except in the cases mentioned in the Evidence Act as where, going by section 89, "the original of the document is in the possession or power of the person against whom the document is sought to be proved, or the original has been destroyed or lost, or the original is not easily movable, or the original is a public document within the meaning of section 102, or the original consists of numerous account or other documents which cannot conveniently be examined in court and the fact to be proved is the general result of the whole collection, or the document is an entry in a banker's book". Hence, In addition to other forms of primary evidence provided in section 86 (1) – (3), section 86 (4) goes to make specific provision regarding the subject matter of this paper by including computer generated evidence into the league of primary evidences:

Where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photography, *computer* or other electronic or mechanical process, each shall be primary evidence of the contents of the rest; but where they are all copies of a common original, they shall not be primary evidence of the contents of the original (italics mine).

Section 87(b) of the Act provides that copies made from the original by mechanical or electronic processes, which in themselves ensure the accuracy of the copy, and copies compared with such copies shall be secondary evidence. By the combined effect of sections 86 (4) and 87 (b), it would appear that the

[49]*Supra.*
[50]*Supra.*

Supreme Court decision in *Anyaebosi v R.T Briscoe*[12] to the effect that a computerized statement constitutes secondary evidence of the original is no longer tenable. Computerized statements are now clearly primary evidence.

On proof of execution of documents, section 93 of the Act provides as follows:

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

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

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

The Act is thus welcome development in Nigeria. The provisions on the admissibility of computer generated evidence and more as primary, provision on the acceptability of electronic signature, and the inclusion of computer files and programmes into the definition of documents are a milestone not only in combating, for instance, cyber criminality which veritable medium is the computer and computer-related devices, but also towards integrating Nigeria into the one-world order *vide* the globalization process.

The Act seems to clarify uncertainty and ambiguity associated with electronic evidence in Nigerian judicial system. By virtue of the enactment, the evidential status of electronic evidence appears definite. It seems no longer a subject of controversy or an avenue for academic debate or a matter of a juristic preference. Issues such as whether electronic evidence qualifies as a document[51], whether electronic evidence is admissible in trial or not and whether electronic evidence is primary or secondary evidence have all been settled by EA. By virtue of section 258 (1)[52] electronic evidence is a document[53] for purposes of adducing evidence in a trial.

[12] *Anyaebosi v. R.T Briscoe* (1987) 6 SC 15.

[51]Electronic documentary evidence is any statement relevant to a case which is contained in a document produced by any device used for storing and processing information. Electronic evidence includes but is not limited to computer print-out, e-mails, Automated Teller Machine (ATM) transaction logs, data base, contents of a computer memory, global positioning system tracks and logs from a hotel's electronic door locks. It is a form of documentary evidence.

[52]Interpretation section of Evidence Act 2011.

There are, however, some attendant problems associated with the admission of electronic evidence in respect of probative value and evidential weight. By their origin and nature of transmission, storage and usage, electronic generated evidence is most times viewed sceptically by opposing parties when adduced in evidence. This scepticism is due to the fact that it is easily accessible (hacked) either legitimately or illegitimately by third parties and this can affect its authenticity and integrity. These attendant problems affecting the admission of electronic evidence have been identified as authenticity, integrity and confidentiality of the piece of evidence[54]. Recourse to English law may be of help.

Specific Requirements for Computer-Related Evidence under English Law

It is necessary to advert to the provisions of English law of which those of EA, in relation to the subject,are a literal recopy. Hence, it has been provided to the effect that where the computer records in issue are hearsay, and possibly even where they are direct evidence, the Nigerian and English laws set out a number of preconditions for admissibility.Section 5 CEA provides that a statement in a document produced by a computer will be admissible to prove a fact so long as direct oral evidence of that fact would have been admissible. This is also provided for in section 84 (1) of EA.

For admissibility however, four conditions must be fulfilled. These conditions are set out in section 5(2)as follows:

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 purposes of any

[53]S.258 (1) of Evidence Act, 2011 defines documents to include (a) books, maps, plans, graphs, 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 that matter (b) any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to enable (with or without the aid of some other equipment) of being reproduced from it; and (c) any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being produced from it; and (d) any device by means of which information is recorded, stored or retrievable including computer output. It must be noted that subsections (b), (c), and (d) were absent in the statutory definition of document in the old Evidence Act. Its introduction is one of the many merits of the recent enactment. The implication is that under the new evidence act regime by virtue of subsection (b) recorded phone calls, tape recorded sounds will be admissible in evidence without contention; by virtue of (c) videos whether on Dissociated Vertical Deviation (DVD), Compact Disc Digital Video (VCD), mobile phones or digital cameras will be unquestionably admissible; while (d) covers the admission of every other form of electronic generated evidence as a document.

[54]I.M. Lawal, *op. cit*, p.68.

activity regularly carried on over that period, whether for profit or not, by any body, 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 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.

It is observed that with regard to the United Kingdom, these four conditions show the age of the enactments. They are aimed primarily at the batch processing of identical transactions, and the type of computer operation envisaged by the legislature is clearly a substantial mainframe operation which is processing hundreds or thousands of similar transactions daily. However, the widespread introduction of microcomputers in recent years means that the types of information stored are far more diverse, and the regularity with which information of that type is recorded is less frequent, than would have been the case with mainframe systems of the mid-1960s. There is thus some doubt whether free-form databases or information contained in wordprocessed documents will, at least in precise terms, comply with these four conditions. For criminal proceedings, section 24[55] Criminal Justice Act (CJA) 1988, replacing section 68[56] PACE,

[55](1)Subject—(a) to subsections (3) and (4) below;(b) to paragraph 1A of Schedule 2 to the [1968 c. 19.] Criminal Appeal Act 1968; and (c)to section 69 of the Police and Criminal Evidence Act 1984, a statement in a document shall be admissible in criminal proceedings as evidence of any fact of which direct oral evidence would be admissible, if the following conditions are satisfied— (i)the document was created or received by a person in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office; and (ii)the information contained in the document was supplied by a person (whether or not the maker of the statement) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with. (2)Subsection (1) above applies whether the information contained in the document was supplied directly or indirectly but, if it was supplied indirectly, only if each person through whom it was supplied received it— (a)in the course of a trade, business, profession or other occupation; or (b)as the holder of a paid or unpaid office. (3)Subsection (1) above does not render admissible a confession made by an accused person that would not be admissible under section 76 of the Police and Criminal Evidence Act 1984. (4)A statement prepared otherwise than in accordance with section 29 below or an order under paragraph 6 of Schedule 13 to this Act or under section 30 or 31 below for the purposes—(a)of pending or contemplated criminal proceedings; or (b)of a

provides that documents arising from trade, business, professional, occupational or official activities and which record information supplied by a person who has personal knowledge of the matters recorded are admissible in criminal proceedings provided the requirements of section 23(2) or section 24(4) (iii) are satisfied.

Under section 23(2), the document is admissible if the person who would otherwise give oral evidence is dead or unfit to testify, if he is abroad and it is not practicable for him to testify, or if he cannot be found although reasonable steps have been taken to find him. Perhaps more importantly, section 24(4) (iii) permits the document to be given in evidence if the maker of the statement cannot reasonably be expected to remember the matters contained in the record. This section deals with the hearsay problem. It is important to note that, where a document is sought to be admitted under section 24, oral evidence must be given that the requirements of the section have been complied with.[57]This is in contrast to the accuracy requirements of section 69 PACE, which can be proved by certificate. Even where a computer-stored statement fulfills the requirements of section 24 of the 1988 Act, it will not be admissible unless it also meets the provisions of section 69(1) PACE:

criminal investigation, shall not be admissible by virtue of subsection (1) above unless— (i)the requirements of one of the paragraphs of subsection (2) of section 23 above are satisfied; or (ii)the requirements of subsection (3) of that section are satisfied; or (iii)the person who made the statement cannot reasonably be expected (having regard to the time which has elapsed since he made the statement and to all the circumstances) to have any recollection of the matters dealt with in the statement.

[56](1)Subject to section 69 below, a statement in a document shall be admissible in any proceedings as evidence of any fact stated therein of which direct oral evidence would be admissible if—(a)the document is or forms part of a record compiled by a person acting under a duty from information supplied by a person (whether acting under a duty or not) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with in that information; and (b)any condition relating to the person who supplied the information which is specified in subsection (2) below is satisfied. (2)The conditions mentioned in subsection (1)(b) above are— (a)that the person who supplied the information—(i)is dead or by reason of his bodily or mental condition unfit to attend as a witness : (ii)is outside the United Kingdom and it is not reasonably practicable to secure his attendance; or (iii)cannot reasonably be expected (having regard to the time which has elapsed since he supplied or acquired the information and to all the circumstances) to have any recollection of the matters dealt with in that information; (b)that all reasonable steps have been taken to identify the person who supplied the information but that he cannot be identified; and (c)that, the identity of the person who supplied the information being known, all reasonable steps have been taken to find him, but that he cannot be found. (3)Nothing in this section shall prejudice the admissibility of any evidence that would be admissible apart from this section.

[57]*R v Minors* (1989) 2 All ER 208.

> In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown—
>
> (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer; ,
>
> (b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents ; and
>
> (c) that any relevant conditions specified in rules of court under subsection (2) below are satisfied.

It does seem that so far, no rules of court have been made under section 69(2). These provisions are designed to overcome any doubts as to the accuracy of the statement, either because it was not stored correctly in the first instance or has become corrupt over time. This is not likely to be a problem with, say, a record of serial numbers which are input once and then stored until needed. However, if the computer is programmed to collate a number of separately input records (e.g. the various serial numbers of the component parts of a car) to make the record sought to be admitted; the court will need to be convinced that no inaccuracy has crept in during the processing of the data. These matters may be evidenced by a certificate under para.8 of Schedule 3. The certificate must identify the document and describe the manner of its production, give particulars of the equipment used in its production, deal with the requirements of section 69(1) and purport to be signed by a person "occupying a responsible position in relation to the operation of the computer". It is sufficient for the certificate to be signed to the best of the knowledge and belief of that person. Para.9 gives the court power to require oral evidence of any of these matters, but it is unlikely to do so in practice unless the accuracy of the certificate is disputed. It was recently made clear by the Court of Appeal in R v Minors (1989) that computer records which are hearsay have to clear both these hurdles, and the mere fact that a record satisfies the accuracy requirements of s.69 PACE does not exempt it from the admissibility requirements of s.24 Criminal Justice Act 1988.

A critical examination of these admissibility requirements reveals that computer records, unlike other forms of evidence, are regarded as suspicious in two respects:

> a). The technology for storing and processing data is believed to be inherently inaccurate. Both s.69 of PACE and s.5(2)(c) of CEA require some minimum proof of accuracy before the record can be examined by the court. The assumption is that not only must the court be satisfied of the reliability of the statement as a true record of what the witness

> observed, but also of its authenticity as an accurate record of what was intended to be recorded. Parliament envisaged that there would be many cases where the document might have become corrupted by software errors or hardware malfunctions. For these reasons it was necessary to show that at all material time the computer had been functioning properly, or at least that any malfunction had not affected the accuracy of the information. This suspicion was probably unfounded even at the time of the legislation; it is certainly the case today that a computer record is likely to be at least as accurate as one maintained on paper. This seems to have been recognised in practice. as the accuracy requirements are normally proved by the production of a certificate emanating from a responsible person in relation to the computer system, and that person is only required to certify the matters in question to the best of his knowledge and belief.

Nonetheless, there is a substantial degree of uncertainty amongst computer users as to whether their computer records will be attacked on this ground by challenging the certificate [Castell (1987)]. If such an attack is made it will be necessary for the person issuing the certificate to give oral evidence as to the working of the computer. In many cases it is unlikely that the available information about the operation of the computer system will be sufficient to satisfy the court that the record has not been altered or corrupted. This uncertainty is delaying the introduction of computer systems to perform transactions which have potential legal significance (e.g. for contract formation under EDI).

b). The wording of s.5(2)(a), (b) and (d) CEA clearly assumes that the record to be adduced in evidence is a record of human observations, probably entered into the computer by a different person from the observer. It also assumes that information processed by a computer will normally be highly structured and consist of quantities of similar records, and that information which does not possess these characteristics will have been processed by ad hoc and ill-tested software and for this reason be potentially inaccurate. In 1968, given the cost of mainframe software and its comparative difficulty of production, this might have been a valid assumption. That is untrue today, both in respect of the type of information stored on computers and its processing. The case for restricting the admissibility of computer-related evidence to accurate records is at least arguable, but if these conditions were strictly applied they would exclude records whose accuracy is not in doubt. On any rational assessment of the problems in this area, authentication should go to the assessment of the weight to be attached to the record, rather than its admissibility. The confusion of authentication with admissibility can lead to erroneous decisions (the classic example is R v Pettigrew (1980)) and act as a

brake on the introduction of new technology. As Tapper points out, "There is no intrinsic reason why different regimes should apply to different forms of record-keeping, and every reason why they should not when the different forms are not readily distinguishable upon their face. There may be no obvious difference in appearance between a document produced by a computerised word-processing system and one produced by a manual typewriter, nor is there the slightest justification for subjecting them to different hearsay rules. To do so creates nothing but anomaly and confusion."

Authentication of Computer-Related Evidence: Problems

The above defects in the rules of evidence, confusing as they do admissibility and accuracy, detract attention from the real difficulties which arise in relation to the authentication of computer-related evidence. It is important to understand here the issues that are at stake.Authentication means satisfying the court (a) that the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or machine, and (c) that extraneous information such as the apparent date of the record is accurate. As with paper records, the necessary degree of authentication may be proved through oral and circumstantial evidence, if available, or *via* technological features of the system or the record.

Authenticity deals with whether or not the piece of information actually emanated from the person or source it purports to emanate from and is correct in what it conveys. Related problems are those of integrity and confidentiality[58]

[58]Integrity has to do with whether or not the information was distorted or tampered with even after it emanated from a correct source. In terms of integrity, the concern is to be able to show that the material is accurate and complete. This essentially reflects the 'operating properly' test. While the burden of proof has been shifted, the party adducing computer-derived evidence may still need to ensure that they have the necessary evidence, whether oral or documented, to be able to refute any serious challenge raised as to the integrity of evidence derived from a computer or network. For a complex system, this may require an array of witnesses with familiarity with the different components (I.Walden, *op. cit.*, p.382). Thus, a message can be sent from one source but is by some means tampered with such as to have at the receiver's end, a different message, substantially or otherwise from the one that was originally sent out. An audio or visual tape can be edited or tampared with through the imposition of images and devices, and so on. Through any such inteference. the latter form of the contents is fundamentally different from the first or original form. Telefaxes can be interpreted and possibly exhanged just as text messages (sms) can be intercepted, listened to and even edited by an unscrupulous operator working for a GSM network from or through the form which the message or conversation is sent, for example, through hacking of computer and crashing of passwords information stored in computer memories can be altered even without the knowledge of the maker, sender or receiver as the case may be. Confidentiality/accountability is another problem which confronts electronically generated evidence. Electronically generated evidence hardly enjoys confidentiality since it is legitimately or illegitimately accessible to third parties or undesirable/ unpermitted readers. Accountability is

discussion of which are beyond the scope of this paper. Normally, when information is entered on computer memory, or an e-mail is sent or an order is placed for goods and/or services through the internet, the sender is unable to authenticate the information he has sent by way of signature. It is the same if he speaks with another person on the telephone, leaves a message on that other person's voicemail or sends a text message. A voice on the phone can be imitated[59]. In a work place, any person can enter information into a computer memory, purporting it to be entered by another person. If such a false data or message is presented in the court there will hardly be a way of detecting the false nature. The court can thus be easily misled.[60]Authenticity is concerned with the origin of the material and can be further subdivided into two tests. The first is the need to establish a link between the material being adduced as evidence and the accused. Such evidence depends on investigators being able to adequately address the 'identity problem'. This may create a forensic challenge for a number of reasons, obviously more so in a network environment, whether open, such as the Internet, or closed, such as a corporate network.

The location of the source computer may mean that multiple users had potential access to the machine at the relevant time, which can make it difficult to show 'beyond reasonable doubt' that the accused was the person with 'his fingers on the keyboard'. In the English case of *Vatsal Patel*,[61] the accused was a contract programmer at Dun and Bradstreet who was alleged to have installed 'wrecking programs' on the organization's network to delete complete development work, in order to extend the period of his lucrative contract. He was acquitted, however, because the prosecution was unable to prove that it was Patel who had initiated the programs, partly due to the physical position of the relevant terminal behind a concrete pillar.

In a networked environment, where the illegal content or the act is only evidenced from remote sources, authenticity will mean establishing an adequate evidential

concerned with the circumstances under which evidence is obtained and subsequently handled. Computer-derived evidence is notoriously vulnerable to alternation, which extends from the manner of obtaining it. the acquisition process. to the handling of such evidence by investigators, prosecutors and expert witnesses at all stages until trial. the 'chain of custody test'(P. Sommer, 'Digital Footprints: Assessing Computer Evidence', *Criminal Law Review*, Special Edition, December 1998, p.5). This could be particularly relevant where a digital copy of an original item of evidence was being relied upon in court (*Kajal v Noble* (1982) 75 Cr App R 149).

[59]I.M. Lawal, *op. cit*, p.84.

[60]*Ibid.*

[61]Aylesbury Crown Court, 2 July 1993. Reported in *Computers and Law*, vol. 5, No 1, 1993, pp.43-45.

link between the material and the virtual identity used, and then between that and the defendant. As much as machines may have multiple users, online identities may be shared, compromised or 'spoofed', where someone deliberately inserts incorrect identification details into a message. Even when it is beyond dispute that source computer belongs to the suspect, as second course of challenge is for the accused to deny that he was aware that such illegal or incriminating material was present on his machine: the so-called "Trojan horse' defence and its variants. It is observed that widespread ignorance about the manner in which computers and the Internet work, coupled with the technical reality that data can be placed surreptitiously on a remote machine (eg 'spyware'), means that such claims can be a fruitful basis for disputing prosecution evidence.

In another English case, *Mould*,[62] for example, the accused maintained that the indecent images found on his machine had got there accidentally and unknowingly. To counter this claim, the prosecution was required to adduce evidence that showed that Mould had an interest in pedophile material and had previously accused newsgroups, chat lines and websites concerned with such material. In *Schofields*,[63] the prosecution was unable to offer evidence against the defence expert's report that a 'Trojan horse' virus found on the machine of the accused could have placed the indecent images on the hard drive without his knowledge.[64] In *Caffrey*,[65] the jury acquitted the defendant of the section 3(1) offence under the Computer Misuse Act 1990 even though the prosecution expert witness stated that no evidence of the presence of a 'Trojan horse' virus could be found. The defendant argued that it was impossible to test every file on the computer and that the virus could be designed to self-destruct leaving no trace, which seems to have sown sufficient doubt in the minds of the jurors.

To assist the process of linking the material with the accused, Barrett describes a 'scene-of-habitation' analysis process, which involves examining 'innocent' as well as 'criminal' information contained in the sieved media.[66] By examining the suspect's normal usage of a range of applications, such as email, patterns may be discerned that can reinforce an assertion of authorship. In *Takenaka (UK) Ltd v Frankl*,[67] evidence linking the defendant's wife, using a different account but sent in proximity; communications that recognized the presence of the computer in the defendant's hotel room; and email extracts saved in a Word document.[68] Such an approach does raise potential legal concerns,

[62] *Mould*, [2001] 2 Cr App R (S) 8.
[63] Reported in *The Times Online*, 18 April 2003.
[64] *Schofields* This also arose in *Julian Green*. Exeter Crown Court in July 2003.
[65] *Caffrey*, Southwark Crown Court, 17 October 2003(Unreported).
[66] N. Barrett, *Traces of Guilt*, (London: Bantam Press. 2004). pp 214 *et seq.*
[67] *Takenaka (UK) Ltd v Frankl* [2001] EWCA Civ 348.
[68] *Ibid*, at para 22; although in this case the standard of proof is civil rather than criminal.

however, where material is deemed outside the scope of the original search warrant, or it involves collateral intrusion on an individual's privacy, whether the suspect's or a third party's[69].

A second authenticity test is to link the material to the relevant computer or system, the 'computer source' test. This is partly an extension of the person/material test, since people operate in a networked environment through computers, whether using a traditional PC or a mobile phone. However, it also arises from the manner in which some environments operated. For example, what is displayed on a computer screen when a 'webpage' is downloaded over the Internet may potentially comprise a mosaic of material drawn from different computers based in different jurisdictions, the image being assembled only at the moment it is requested.[70] Such mechanisms have apparently been used for the distribution of child abuse images. As well as raising problematic forensic issues in terms of identifying the source of such material, it may offer a potential defence against a charge for supply.

Electronically generated materials therefore do not easily lend themselves to effective test of authenticity, unlike with conventional documents where signatures or hand writings can be compared easily. In *R v Silverluck*[71], a solicitor who had given considerable attention for many years to the study of handwriting and had on several occasions compared handwritings for purposes of evidence was permitted to testify on the subject as an expert, thus helping the court to determine the authenticity of the document in issue.

A simple example of the vulnerability of digital evidence to alteration is a document created using Microsoft Word. As well as the document, the application generates meta-data about the document, for example detailing the time and date the document was created, modified and accessed.[72] However, an investigator, when accessing such a document, may inadvertently alter the document in some way and therefore alter such meta-data.[73] Alterations made to a file once it is in the possession of an investigator obviously create a strong basis upon which to raise a challenge to the probative value of evidence. Law enforcement agencies therefore need to follow procedures designed to minimize such accountability

[69] I. Walden, *Op.cit.*, p.381.
[70] E.g. in a web environment, image files are often stored separately from text files.
[71] *R v Silverluck*(1894) 2 QB 766. See also I.Walden, *Op. cit.*, p.381.
[72] To view these details, on the menu, go to File, Properties, Statistics.
[73] E.g. if you go to the menu, Tools, Word Count, recounting the words in a document constitutes a recorded modification.

threats and ensure the provenance of any adduced evidence, including disk 'imaging'[74] techniques and filming screen shots.[75]

Evidence Act 2011 and the Authenticity Problem

In light of these problems, section 84 (2) laid down certain conditions which must be shown to exist for electronic evidence to be admissible in any proceeding. These conditions were provided to militate against the problems affecting the authenticity and integrity of electronic evidence. These conditions are outlined in section 84 (2) & (4) of the Act. Before electronic evidence is admissible in any proceeding by virtue of section 84 (1) certain conditions specified in subsection (2) must be shown to exist.

The conditions are thus:

a. The document containing the statement must be produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities. Such activities must be regularly carried on over that same period;
b. The information supplied to the computer in the ordinary course of those activities must be of the kind contained in the statement or the kind from which the information contained in the statement was derived;
c. The computer was in proper working condition throughout the material part of the period. Where it was not, it must be shown that the fault was not such as to affect the production of the document or the accuracy of its contents; and
d. The information contained in the statement must be reproduced or derived from information supplied to the computer in the ordinary course of those activities.

An illustration may be helpful. If A and B are parties to a proceeding and A is relying on electronically generated evidence to prove that B a bank manager laundered money, before the evidence becomes admissible A must show that-

a. The document containing the statement (evidence) was produced by a computer used regularly to store or process information of the banking activities. the banking activities must have been carried on regularly over the period in question:

[74] Where a complete copy of the computer's permanent memory is preserve. Also referred to as 'bit stream imaging methodology', see E. Kenneally and C. Brown 'Risk Sensitive Digital Evidence Collection', *Digital Investigation* (2005) 2, pp. 101-119.
[75] E.g. using Lotus ScreenCam.

b. The information supplied to the computer over the period is the same kind of information sought to be proved by the statement in the document, that is, record of cash transactions;
c. The computer was working properly; if not, that the fact that it was faulty did not affect the authenticity of the document, that is, its production and accuracy of its contents; and
d. The information contained in the statement (evidence) was reproduced or derived from the information supplied to the computer.

The jurisprudence of the above conditions is founded on the fact that it is easy to create, alter or destroy electronic evidence as computers are manipulable devices. What these conditions have done is to prevent a situation where parties to a suit will take advantage of these frail features of electronically generated evidence by cooking up evidence favourable to their case before coming to court. This purpose is achieved by the implication of expressions such as "used regularly to store or process information" "ordinary course of activities' and "activities regularly carried on over that period". The implication of these expressions is that the information contained in the statement sought to be adduced in evidence would be of events or activities which occurred before the suit was instituted and at a time where neither of the parties had the possibility of such suit in mind, hence, the evidence will be unbiased and accurate.

Besides, due to the uniqueness of this type of evidence and its frail features portrayed above, section 84 (4) provides a special form through which it can be tendered in evidence. Thus, by virtue of section 84 (4) where electronic evidence is sought to be tendered in evidence, it should be accompanied with a certificate:

a. identifying the document containing the statement and describing manner in which it was produced
b. giving such particulars of the device used to produce the document, for the purpose of showing that the document was produced by a computer.

Furthermore in view of subsection (2) the certificate should be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities, as the case may be. It is sufficient if the matter stated in the certificate is made to the best of the knowledge and belief of the person stating it.

Yet, there is no doubt that authentication means satisfying the court (a) that the contents of the record have remained unchanged, (b) that the information in the record does in fact originate from its purported source, whether human or

machine, and (c) that extraneous information such as the apparent date of the record is accurate. It should be clear from the analysis above that section 84 EA, just as the English CEA and PACE, at best address only the first of the three requirements for authentication. Indeed, they only address part of that requirement, for a record can change without any system malfunction or improper use of the system, e.g. if it is amended over time to take account of new information, thus overwriting the original contents. Nothing in EA assists computer users in deciding how best to link the record with its maker, a role traditionally performed in relation to physical documents by an autograph signature. Nor, particularly if the record emanates from another computer, is there any provision which will assist in proving when it was sent, and from where. These matters are important in commercial transactions, to say the least.

Conclusion

It is time for section 84 of EA to be reviewed. Special rules for the admissibility of computer-related evidence can no longer be justified, particularly where those rules are based on false assumptions about the technology. It is also time to legislate for authentication. Important questions need to be answered. Can an electronic document be "signed", and if so what will constitute a signature? Can the parties to a communications network agree authentication procedures which will then be accepted by the courts? Is a system log adequate evidence of the changes made to a record, and if so what should it contain? It is beyond the scope of this paper (and indeed the competence of the author) to put forward a draft Bill at this stage, but the longer work on this topic is delayed the worse the position will become. Some might argue that a gradualist, case-based approach to reform will identify the real issues and produce better law. Such a "laissez faire" attitude is an inadequate response to these problems.

The tradition that the law lags 10 to 15 years behind technological development will not produce the guidance which industry and commerce require if they are to compete in an increasingly international market. Indeed, the pace of technological change is so fast that the law is likely to fall further and further behind commercial practice, for instance. In the meantime uncertainty and confusion rule. Systems are not adopted, or (perhaps worse) are introduced in parallel with what may turn out to be unnecessary duplicate records, a sort of "belt and braces" approach which imposes heavy financial burdens and inefficient and cumbersome procedures. It is necessary that the law should give a lead. Industry, commerce and criminology require clear guidance on how to make their records acceptable to the courts. Until this guidance arrives, the evidence law on computer generated records in Nigeria will indeed remain 'an ass'.