ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CIVIL AND CRIMINAL PROCEEDINGS. [1]

BY

HON. JUSTICE ALABA OMOLAYE-AJILEYE [2]

In the beginning God created the heaven and the earth. The earth was without form, and was void; and darkness was upon the face of the deep. And the Spirit of God moved upon the face of the waters. And God said, let there be light and there was light. Genesis 1: 1-3

Introduction

It is expedient at the beginning of this paper to attempt to explain what constitutes electronic evidence. There is no direct or specific definition of what electronic evidence is under the Evidence Act, 2011. The word 'electronic' is a generic term which does not have any distinctive quality or application. Without any wish to run into any definitional problem, I will simply adopt the definition of Mason (2007)[3], that is, "data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicated by any device, computer or computer system or transmitted over a communication system that is relevant to the process of adjudication"[4] It includes but not limited to e-mails, text documents, spread sheets, images and graphics, database files, deleted files, and data back-ups. Electronic evidence may be located on floppy disks, zip disks, hard drives, tape drives, CD-ROMs or DVDs, as well as portable electronic devices such as PDAs, cellular phones microfilms, pen recorders, faxes etc.

The scope of this paper covers both civil and criminal proceedings. As a threshold point, it is important to clarify that electronic evidence in civil proceedings presents many of the same issues that arise in criminal proceedings. Understandably, the Evidence Act applies to both criminal and civil trials. The opening statement of section 84 of the Evidence Act, 2011 elucidates this point as it declares in an unambiguous term: "[*i*]n *any proceeding a statement contained in a document produced by computer shall be admissible as evidence …"* The words, "in any proceedings" indicate clearly that the provisions of the section apply to both civil and criminal proceedings with equal force.

We live in an age that is dominated by computers. Indeed, it has been christened "computer age" or the age of Information and Communication Technology (ICT). It is characterized by invention of hardware, software and media for collection, storage, processing, transmission, retrieval and presentation of information. They also include communication and computing equipment and programmes such as satellites, transmission lines, computers, modems, routers, the Internet, intranet, email, wireless networks, cell phones, iPods, digital cameras and other operating systems and applications. The unalterable truth is that the advancement in technology witnessed in the last few decades has revolutionalised the world and launched the world on an information super high way. It has

defined how we live, work and think such that the world has not remained the same again. It has brought the world, not only into a global village or global sitting room but a global palm.

In any event, we must as well not lose sight of the criminal use of computers. It is regrettable that the same technology which provides useful devices to humans has also been perverted for criminal and terrorist purposes. The advancing technology provides criminals and terrorists with a variety of tools and opportunities to conduct their heinous activities. The sad thing is that criminals are not relenting. At every stage of technological advancement, there is one form of perversion or another. Sometimes, it looks as if criminals are even advancing beyond the pace of technological development.

The court, today, therefore, faces a serious challenge on how to cope with technological development, especially as regards its treatment of electronically generated evidence. The issue of admissibility of evidence is crucial to any trial, whether civil or criminal, as it has the capacity to determine the outcome of a case one way or the other. And, how a particular court treats such evidence is of utmost significance. A case may be lost or won on the strength of a particular piece of evidence that has been admitted or rejected, as the case may be. The foregoing also underscores the need for judicial officers to have clear understanding and appreciation of the intricacies of electronic evidence.

As adjudicators, we should be familiar with basic computer terms and operations. Rudimentary knowledge of ICT is also essential to ensure proper and correct interpretation and application of the rules guiding a admissibility of electronic evidence, to avoid miscarriage of justice. And, with the enactment of the Cybercrime Act, 2015, more challenges now open to our courts as they will inevitably be called upon to try offences such as computer forgery, computer fraud, identity theft, child pornography, cyber stalking, cybersquatting, phishing, cyber terrorism and xenophobic offences, amongst other offences created in the Act. Courts will no longer be dealing with just common offences such as theft, criminal intimidation or criminal breach of trust but more technical ones that may arise from application of ICT. Inevitably, therefore, there is no way courts can run away from electronic evidence.

The case, *Federal Republic of Nigeria v Abdul*[5] underscores this point. The accused was arraigned on a two-count charge of being in possession of documents containing false pretences contrary to Section 6 (8) (b) and 1(3) of the Advance Fee Fraud and Other Related Offences Act. The accused was arrested in a Cybercafé in Benin City by a group of Economic and Financial Crimes Commission (EFCC) operatives, following a petition to the Commission by a citizen alleging the incidence of Internet crime activities at the Cybercafé. The accused and other customers of the Cybercafé were subjected to a search, at the end of which a handwritten letter and a diary containing several email addresses were recovered from the accused. Subsequently, the EFCC investigators, using the addresses found in the diary also discovered a number of scam emails in the email box of the accused. The emails were printed out by an official of the EFCC. At the trial, the handwritten letter, diary and printouts were tendered as exhibits by the prosecution. One of the questions that arose for determination before the trial court was whether or not the printouts which were tendered and admitted in evidence as Exhibits D, D1 and D2, could be said to be in the possession of the

accused, when they were not found physically with him but were printed out of his email box after his arrest. The trial Judge held:

> *The documents said to be in the possession of the accused do not exist in the physical form until they are printed.... I have read and construed Exhibits D – D2 clearly. Exhibits D and D1 are letters written with false pretences with intent to defraud. As for Exhibit D2, on its own has no meaning. Read along with Exhibits D and D1, it could be regarded as part of a fraudulent scheme. The point about Exhibits D – D1, however is that they have been sent to the addresses on them. The accused admitted... that he sent the letters. Where letters have been written and posted (in the regular and common method of sending mails), could the writer or the person who posted the letter be said to be in possession of the letter? While the writer may be guilty of sending scam letter, certainly he cannot be guilty of being in possession of a letter he has written and posted. Similarly, in this case, with the letters sent to the address as admitted, the accused is no longer in possession of the letters*."[6]

At the end of it all, the accused was discharged and acquitted.

It should be noted here that the document involved in the case that was allegedly found in possession of the accused was not in tangible or physical form. It was in the form of a "soft copy." The court in such a case ought to have appreciated the nature of technology by which the offending document was electronically stored and therefore "possessed" by the accused. Most respectfully, His Lordship did not appreciate the fact that when an email is sent from a shared mailbox, the sent email message remains in the Sent Box of the sender and can be said to remain in his "possession".

One may wish to contrast the decision in *FRN v. Abdul*[7] with *United States v. Romm*.[8] where it was held that the defendant "knowingly possessed" illegal pornography by the mere fact that he connected to the Internet, visited and viewed websites containing images of child pornography which were automatically saved in his computer's Internet cache. The defendant admitted to only having viewed the images for a few minutes and consciously sought to delete them. Nonetheless, the court held that the defendant "knowingly possessed" illegal pornography, as he could view the images in his computer's Internet cache on the screen, and print them, enlarge them, or copy them to more accessible areas of his hard drive and send them by emails to others. Thus, the computer's automatic, normal operation led to his conviction of knowingly possessing illegal pornography despite his conscious attempt to avoid possession by deleting the images.

The outcome of the decision in Romm's case teaches that the emphasis in *FRN v.* Abdul[9] should not have been placed solely on the physical possession of the printouts but the contents of the email box of the accused evidenced by the printouts.

Issues of Admissibility and Conflicting Judicial Decisions Prior to Evidence Act 2011

Before the enactment of the Evidence Act 2011, the issues concerning admissibility of evidence generated from electronic devices became highly contentious, as opinions were

divided, even amongst the superior courts. The contentions then revolved around the following questions:

1. Whether or not the old Evidendce Act, could accommodate the admissibility of electronic evidence in the absence of a clear provision for its admissibility.
2. Whether or not the definition of 'document' in the old Act was wide enough to accommodate computer storage devices or stored representation records such as 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, etc.

'*Document'* was then defined as including:

> *" 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 for the purpose of recording that matter.*

The tendency of courts in Nigeria then was to restrict the definition of 'document' to paper-based materials, typically expressed in words and figures.

The Basis of the Conflicting Decisions

The first notable pronouncement on admissibility of computer printouts in Nigeria was made by the Supreme Court in *Esso West Africa Inc. V. T. Oyegbola*.[10] The apex court in a pronouncement, tinged with foresight, pronounced as follows:

> *"The law cannot be and is not ignorant of the modern business methods and must not shut its eyes to the mysteries of computer. In 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*.[11]

In 1976, that is, thirteen years later, the Supreme Court in *Yesufu v ACB*[11 a] in another *obiter* dictum, sounded a note of warning, emphasizing the need for legislative 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 account" 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.*[12]

It is well known, under the principles of *stare decisis,* an *obiter* is not a binding authority. It is a judge's passing remark which is not the real live issue for determination in the matter. It is the statement of the judge by the way.[13] It is, however, doubtful if any lower court can afford to treat an *obiter* of the highest court in the land with levity without reprehension, as it is good law, that an *obiter* of the Supreme Court, could as well, in certain circumstances, assume the status of a ratio *decidendi.*[14]

Consequently, these two *obiter dicta* of the Supreme Court in *Oyegbola* and *Yesufu's* cases bestrode the lower courts with prodigious effects. The two pronouncements then formed the yardsticks to which references were often made by lower courts to determine whether or not a computer printout was admissible. A court that was determined to admit a computer printout readily found solace in *Esso v. Oyegbola*[15] while on the other hand, a court that was determined to reject same took succour in *Yesufu v ACB*[16] This scenario created a chaotic situation within the judicial landscape of Nigeria.

Decisions in Favour of Admissibility of Electronic Evidence

For instance, in *Trade Bank v. Chami*[17] the provisions of Section 38 of the 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 did not provide for entries in computers, or computer printouts 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 cover computer printouts. The court said;

> *"The section of the Evidence Act (supra) does not require the production of "books of account" but make entries into such books 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 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 S. 38 covers, in my respectful opinion, also electronic process such as computer and computer prints out comprised in Exhibit 4 are admissible..."*[18] (Underlining mine for emphasis)

The spirit of progressivism behind the court's obiter dictum in Oyegbola's case was fortified in 1987 by another decision of the Supreme Court in *Anyaebosi & Ors v. R. T. Briscoe Nig. Ltd*,[19] where the apex court clearly endorsed the admissibility of computer printouts as secondary evidence. The court held that computerized statements of accounts, after all, are not in the class of evidence which is completely excluded by the Evidence Act. The court, therefore, further held that the computerized statements in issue in that case were rightly admitted as secondary evidence. There was also the proactive statement of Rhodes Vivour, J.C.A. (as he then was) in the Court of Appeal decision of *Oghoyone v. Oghoyone*[20] decided in January 2010, before the enactment of Evidence Act, 2011 wherein His Lordship categorically declared that "[a]s the law stands today, computer printout of Bank Statement of Account can be admitted in evidence"[21] It is instructive to note that *Trade Bank v Chami*[22] was cited in that case.

The Court of Appeal, in *Federal Republic of Nigeria v Femi Fani-Kayode*[23] set aside the interlocutory decision of the Federal High Court, Lagos, in which the said court rejected, as inadmissible, the computer printouts of the accused statement of account, tendered by the prosecutor in the trial involving a former Minister of Aviation, Femi Fani-Kayode, on an allegation of laundering N4billion. The court stated that the certified true copy of the computer generated bank statement of account of the respondent, domiciled with the First Inland Bank at Wharf Road, met all requirements of being admitted as an exhibit at the trial. Applying the decision of the Supreme Court in *Anyaebosi's* case the court held further that the document did not fall within the category of evidence made completely inadmissible by law.

In the course of time, Nigerian courts creatively took recourse to the application of the principle of judicial notice to admit electronic evidence. Electronic evidence was then treated as matters of science to which courts were entitled to take judicial notice under Section 74 of

the repealed Evidence Act. The Court of Appeal, for instance, relied on the concept of judicial notice in admitting a computerized document in *Ogolo v. IMB (Nig) Ltd*.[24] The court held that it had become a notorious fact that commercial and banking operations in Nigeria had changed in keeping with the computer age such that the court could take judicial notice of them under section 74 of the old Evidence Act.

Judicial Decisions against Admissibility of Electronic Evidence

In contrast to the above decisions in which courts strained and stressed the letters of the law to admit electronic evidence within the framework of the repealed Evidence Act, many courts entirely rejected electronic evidence on the sole ground that the repealed Evidence Act did not recognize it. In *UBA v. Sani Abacha Foundation for Peace and Unity (SAPFU),*[25] 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 old Evidence Act until certain sections of the Act were amended. The Court, while applying the dictum of the Supreme Court in *Yesufu v ACB*[26] 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.*[27]

The Court then lamented:

> *"It is quite unfortunate that in Nigeria no clarification has yet 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.*[28]

Numba Commercial Farms Ltd & Anor. v NAL Merchant Bank Ltd & Anor [28a] was also decided along the *Yesufu v ACB*[29] line of cases.

Another prominent case in that category was the interlocutory ruling of the Federal High Court in *The Federal Republic of Nigeria v Femi Fani-Kayode*[30] Applying the Court of Appeal decision in *UBA V SAPFU*[31] the court held that the provisions of Section 97 (1) (b) and (2) (c) of the Evidence Act did not cover the admissibility of computer printout even if they were duly certified and relevant.

Computerized documents were also rejected under the repealed Evidence Act because some courts were not comfortable with the fact that such documents are capable of being manipulated. It is recognized that records in computers can be tampered with ease or even changed completely. There was no safeguard against such manipulation under the repealed Act.[32]

So, for many years, courts in Nigeria contended with how best to treat electronic evidence.

Highlights of the Provisions of Evidence Act 2011 on Admissibility of Electronic Evidence

In 2011, the 6th National Assembly enacted Evidence Act, 2011 (Act No. 18). The enactment of the Act, in a way, represents the response of the Legislature to ceaseless clamour for amendment of the old Evidence Act. It took the Legislature a long time to act. When it eventually acted, it went beyond merely amending the Act. It repealed it. Significantly, the legislation attempts to bring the law in line with the reality of advancement in the area of electronic and computer technology as it clearly provides for admissibility of electronically generated documents. As a threshold point, it is necessary to highlight some of the relevant provisions of the Act relating to admissibility of electronically generated evidence.

By far, section 84 of the Act stands out noticeably as a towering provision. Briefly, it provides for admissibility of *"a statement contained in a document produced by a computer"*. Section 258 defines a 'statement' as "any representation of fact whether made in words or otherwise." Section 84 (2) enumerates four conditions that must be satisfied before such a statement becomes admissible. Section 84 (4) requires that a certificate be signed to authenticate the document by a person occupying a responsible position in relation to any matter mentioned in subsection (2). Indisputably, section 84 has been introduced to fill the wide gap that existed in the repealed Evidence Act which made no specific provision for admissibility of electronically generated evidence.

Another prominent provision of the Act is the re-definition of the word 'document'. It is recalled that the limited scope of the definition of 'document' under the repealed Act posed a serious challenge in the past and made admissibility of electronically generated evidence needlessly controversial. The Act now broadly re-defines 'document' thus:

> S. 258 (1) "*Document" 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; and*
>
> *(d) any device by means of which information is recorded, stored or retrievable including computer output.*

The use of the word 'includes' in the definition suggests that the category of 'document' under that section is not exhaustive. In *Ports and Cargo Handling Services Company Ltd & Ors v Migfo Nigeria Ltd & Anor*[33] the Supreme Court explains that when the word 'includes' is used in a statute or written enactment, it is capable of enlarging the scope of the subject matter it qualifies or tends to qualify. Flowing from this broad definition of the word

'document', therefore, the Court of Appeal in *Holdent International Ltd v. Petersville Nigeria Ltd* [34] has held that plastic bottles bearing trademark inscriptions are documents. This must be correct. The meaning of the word 'document' should no longer be construed in a narrow way. Tape recordings tendered in *Federal Polytechnic, Ede & Ors v Oyebanji*[35] were also accepted by the same court as documents. The same conclusion was reached in *Obatuga & Anor v Oyebokun & Ors*,[36] where a video tape was held to qualify as a document.

'Copy of a document' is also defined. The definition of 'copy of a document' in section 258 of the Act relates to the electronic devices mentioned in the definition of document as it refers to transcript of sounds of any disc, tape, sound track; and a reproduction or still reproduction of the images embodied in them whether enlarged or not. It is defined thus:

S. 258 (1) *Copy of a document includes –*

(a) in the case of a document falling within paragraph (b) but not (c) of the definition of "document" in this subsection, a transcript of the sounds or other data embodied in it:

(b) in the case of a document falling within paragraph (b) but not (c) of that definition, a reproduction or still reproduction of the image or images embodied in it whether enlarged or not:

(c) in the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and

(d) in the case of a documents not falling within the said paragraph (c) of which a visual image is embodied in a document failing within that paragraph, a reproduction of that image, whether enlarged or not, and any reference to a copy of the material part of a document shall be construed accordingly.

Again, the use of the word "includes" in the definition of 'copy of a document' quoted above is significant, as it has been held to have been inserted to serve the purpose of widening the scope of the concepts covered by the term a "copy of a document"[37]

Other new definitions are introduced in the Act. One of such definitions is 'computer' which means "any device for storing and processing information"[38] The Act explains that 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. The definition of 'film' also includes microfilm.[39]

There is now a presumption as to electronic messages. The court *may* presume that an electronic message forwarded by the originator through an electronic mail server to addressee to whom the message purports to be addressed corresponds with the message as fed into the computer for transmission; but the court *shall not* make any presumption as to the person to whom such message was sent.[40] In simple terms, the court may presume the accuracy of the contents of an electronic message but shall not presume the recipient. Strangely, however, the Act omits to define who the 'originator', 'addressee' and 'recipient' of an electronic message are.

Upon acknowledgement of electronically generated documents as admissible evidence, the Act proceeds to give a guide to courts on how to assess such evidence. Section

34 thereof makes specific guidelines as to how courts are to attribute weight to statements admitted. It prescribes that regards shall be had to all circumstances, pointing to the accuracy or otherwise of the statement, including contemporaneity, and the existence of the motive to conceive or misrepresent facts.

Proof of Conditions for Admissibility of Computer Generated Evidence under Section 84

Section 84 provides:

> *84. (1) In any proceeding a statement contained in a document produced by a computer shall be admissible as evidence of any fact stated in it of which direct oral evidence would be admissible, if it is shown that the conditions in subsection (2) of this section are satisfied in relation to the statement and computer in question.*
> *(2) The conditions referred to in subsection (l) of this section are-*
> *(a) that the document containing the statement was produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period, whether for profit or not by anybody, whether corporate or not, or by any individual;*
> *(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the information so contained is derived;*
> *(c) that throughout the material part of that period the computer was operating properly or, if not, that in any respect in which it was not operating properly or was out of operation during that part of that period was not such as to affect the production of the document or the accuracy of its contents; and*
> *(d) that the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.*
> *(3) Where over a period the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in subsection (2) (a) of this section was regularly performed by computers, whether-*
> *(a) by a combination of computers operating over that period; or*
> *(b) by different computers operating in succession over that period: or*
> *(c) by different combinations of computers operating in succession over that period; or*
> *(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.*
> *All the computer used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.*
> *(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate -.*

(a) identifying the document containing the statement and describing the manner in which it was produced;

(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer:

(i) dealing with any of the matters to which the conditions mentioned in subsection (2) above relate, and purporting to 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, shall be evidence of the matter stated in the certificate: and for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section-

(a) information shall be taken to be supplied to a computer if it is supplied to it in any appropriate form and whether it is supplied directly or (with or without human intervention) by means of any appropriate equipment;

(b) where, in the course or activities carried on by any individual or body, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;

(c) a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

The provision of section 84 is novel. Principles of law emerging from its application and courts' interpretation are still at developmental stage in Nigeria. It is hoped that as more cases are brought before the courts, particularly, the appellate courts, the provision will be subjected to further judicial scrutiny. One obvious fact about section 84 is that, it has prescribed a special procedure to be applied in admitting electronically generated evidence.

Section 84 (2) specifies the following four conditions which must be proved:

(i) that the statement sought to be tendered was produced by the computer during a period when it was in regular use, to store or process information for the purpose of any activity regularly carried on over that period;

(ii) during that period of regular use, information of the kind contained in the document or statement was supplied to the computer;

(iii) the computer was operating properly during that period of regular use or if not, the improper working of the computer at any time did not affect the production of the document or the accuracy of its contents; and

(iv) that the information contained in the statement was supplied to the computer in the ordinary course of its normal use.

Section 84 (3) provides that where over a period, the function of storage or processing is performed by a combination of computers or different computers operating in succession over that period all the computers used for that purpose during that period shall be treated as constituting a single computer.

A computerized document that is sought to be tendered in evidence must necessarily undergo a process of judicial scrutiny under section 84 (2). The conditions stipulated to be fulfilled therein appear elaborate. The explanation for this is not far-fetched. It is a well-known fact that electronic records are very easy to tamper with. They are generally vulnerable to manipulation. Tobi, J S. C., in *Araka v. Egbue*[41] alludes to this in respect of admissibility of secondary evidence under section 97 (2) of the old Evidence Act when he says:

> *In this age of sophisticated technology, photo-tricks are the order of the day and secondary evidence produced in the context of section 97(2) (c) could be tutored and therefore not authentic. Photo-tricks could be applied in the process of copying the original document with the result that the copy which is secondary evidence does not completely or totally reflect the original… court has not eagle eye to detect such tricks*.[42]

What Tobi, J.S.C., refers to as 'photo-tricks' can, in modern parlance, take the form of 'enhancement', super-imposition, transposition, modification, excision or alteration. In the same vein, Onyemenam, J.C.A., in *Ekiti State Independent Electoral Commission, & Ors v PDP & Anor*[43] states that, "with our modern information communication technology, anything is possible. Documents and signatures are easily manipulated to the extent that genuineness of documents can no longer be ascertained by mere observation with the eyes"[44] Indeed, a computer generated document can be altered without leaving any obvious trace of its alteration. Computer generated documents can also be copied, updated, intercepted or deleted. Johnson (1992)[45] asserts that although computer generated documents may carry the aura of accuracy and reliability, the truth remains that they are actually more inaccurate and unreliable than traditional forms of documents.[46] The nefarious activities of *hackers* have also become notorious. The relative success of such *hackers* in intruding into the operation of computers and the increasing activities of digital criminals pose serious dangers to the accuracy of computer generated evidence. Their activities include theft, fraud, destruction of data and unauthorized access to stored information, amongst others, which tend to compromise the integrity of the contents of computers.

The conditions stipulated in section 84 (2) and (4), therefore, simply seek to ensure that what is presented before the court is *prima facie* reliable and worthy to be accepted as evidence. In other words, that the statement claimed to have been produced from the computer reflects, in the words of Tobi, J.S.C., 'completely and totally', what was fed into and contained in the computer. It is to safeguard the source and authenticity of the electronically generated evidence sought to be used in evidence.[47]

The Supreme Court of Nigeria has pronounced on the conditions stipulated under section 84 (2), in *Kubor v Dickson*,[48] holding that fulfilment of the said conditions is mandatory if a party desires to tender e-documents. The Court of Appeal, in *Akeredolu &*

Anor v. Mimiko & Ors[49] reaches the same conclusion. In Akeredolu's case, one of the issues that came up before the Court of Appeal was whether or not the contents of voters' registers for 2011 and 2012 tendered in evidence as Exhibits P50A and P50B respectively, before the Governorship Election Petition Tribunal ought to have been allowed to be demonstrated through electronic gadgets before the Tribunal. The Court of Appeal, while affirming the decision of the trial tribunal in rejecting the application for such a demonstration, emphasizes the need for the laying of requisite foundation regarding the conditions stipulated for admissibility of electronic evidence under section 84. The court states thus:

> *"Going by the foregoing provision it is discernible that the appellants who were desirous of demonstrating electronically the content of Exhibit P50A and P50B failed to lay the necessary foundation regarding the condition of the electronic gadget or computer they were going to use. To the extent that those conditions as spelt out in section 84 supra were unfulfilled the demonstration ought not to be allowed".*[50]

The decision of the Supreme Court in *Kubor & Anor v Dickson & Ors*[51] is important. It came in the nick of time. It was decided barely one year after the enactment of the Evidence Act, 2011. The apex court, therefore, took advantage of the opportunity to make an authoritative pronouncement on the application of section 84 (2) early enough to chart a course for other courts in Nigeria to follow. It has thus attained the status of a *locus classicus* on issues relating to admissibility of electronic evidence in Nigeria. The relevant facts of the case are straight forward. The appellants challenged the election and return of the first respondent as the Governor of Bayelsa State in the February 11, 2012 governorship election. The documents tendered by the appellants included a computer printout of the online version of *The Punch* newspaper and another document from the website of the Independent National Electoral Commission (INEC), the third appellant in the appeal. The electronic version of *The Punch* was admitted and marked Exhibit 'D'. The document from INEC's website was equally admitted and marked Exhibit 'L'. There was no evidence on record that the appellants, in tendering Exhibits 'D' and 'L' satisfied any of the conditions stated in section 84 (2). The Supreme Court affirmed their rejection by the lower court. Apparently, the exhibits were tendered from the bar. The Supreme Court declares:

> *Granted for the purpose of augment, that Exhibits "D" and "L" being computer generated documents or e-documents down loaded from the Internet are not public documents whose secondary evidence are admissible only by way of certified true copies then it means that their admissibility is governed by the provisions of section 84 of the Evidence Act 2011… There is no evidence on record to show that the appellants in tendering Exhibits "D" and "L" satisfied any of the above conditions. In fact they did not as the documents were tendered and admitted from the bar. No witness testified before tendering the documents so there was no opportunity to lay the necessary foundations for their admission as e-documents under section 84 of the Evidence Act 2011. No wonder therefore that the lower court held at page 838 of the record thus:- "A party that seeks to tender in evidence a computer generated*

document need to do more than just tendering same from the bar. Evidence in relation to the use of computer must be called to establish the conditions set out under Section 84(2) of the Evidence Act 2011. I agree entirely with the above conclusion. Since appellants never fulfilled the pre-conditions laid down by law, Exhibits "D" and "L" were inadmissible as computer generated evidence/documents.[52]

Laying Foundation for Admissibility of Computer Generated Evidence under Section 84 (2).

In Kubor's case, the Supreme Court emphasizes the need to lay 'necessary foundation' for admissibility of e-documents. Clearly, the whole essence of the conditions stipulated under section 84 (2) is to enable witnesses lay proper foundation for admissibility of electronically generated evidence. The basic issue is, computer generated evidence must be found reliable and trustworthy to be admitted in evidence. This, essentially, is a function of the computer that generated the evidence and the contents of the documents vis-à-vis what is contained in the computer. According to Johnson (1992)[53]:

[C]omputer data acquires reliability as evidence from the system under which it is produced. If the original data fed in is not accurate or if the machine and its program are not well designed and operated or if the data produced is not properly evaluated, it has no probative force[54]

Therefore, a witness who desires to tender a piece of electronically generated evidence under section 84 (2) is required to lay proper foundation for its admissibility.

Laying foundation is the practice or requirement of introducing evidence of certain facts necessary to make further evidence relevant, material and admissible. Onnoghen, J.S.C., refers to it as "pre-conditions laid down by law"[54a] The requirement of laying proper foundation for admissibility of evidence is not a new process introduced by the Evidence Act, 2011. It has been part and parcel of the law and practice of evidence in Nigeria but only known to be applicable to admissibility of secondary evidence. It is now embodied in section 84.

The first step in the process of laying foundation in respect of electronically generated evidence is to establish its relevance to the case under inquiry and identify it as what it purports to be. If the document is not relevant, that is the end of the inquiry. The basic principle of law that evidence that is not relevant is inadmissible is applicable to section 84. Exhibits 'D' and "L" in Kubor's case were rightly rejected because, according to the Supreme Court, no witness testified before tendering the documents, so there was no opportunity to lay the necessary foundations for their admission as e-documents under section 84 of the Evidence Act, 2011.

The main object of laying foundation for admissibility of electronically generated document under section 84 (2) is to authenticate it and establish the reliability of the computer that produced it. As a condition precedent to admissibility of a computer generated document, there must be evidence sufficient to establish or support a finding that the document in question is what the proponent claims it to be.[55] The authenticating witness is

to provide evidence about the process by which the electronically generated document was created, acquired, maintained and preserved without alteration or any change. For instance, where the issue of admissibility of a computer printout arises, the main task of an authenticating witness should be to show the court that the printout is a correct reflection of what was fed into the computer. It is also incumbent on the witness to predicate such facts on the relevance of the document sought to be tendered to the case being tried.

The proper functioning of the computer that produced a document is required to be established as a pre-condition under section 84 (2) (a). This is meant to ensure that the computer from which a document was generated is reliable. The reliability of the computer is established by the fact that there is evidence to show that it was used regularly to store or process information for the purposes of activities regularly carried on over a period. Under section 84 (2) (b), there must be proof that the document itself, produced by the computer, is reliable. The vulnerability of computer records to manipulation and tampering is directly in point here. Of course, a computer will only produce what is programmed into it. Evidence must, therefore, establish that the computer did exactly what it was instructed to do and the document produced in court consists of what was fed into the computer. If there is discrepancy between what is contained in the computer and what is produced, such document will be considered unreliable and the entire information could be found to be unacceptable.

The question of trusting the operation of the computer arises under section 84 (2) (c). A computer, without any form of manipulation, can malfunction. It may be affected by 'bugs' or infested with viruses. A malfunctioned computer has the tendency of producing inaccurate data. The law, therefore, requires foundational evidence to show that at the relevant time, the computer operated properly and if there was ever a time it malfunctioned it did not in any way affect the production of the document or the accuracy of its contents. Evidence of malfunction of a computer is relevant if it affects the way the computer processes, stores or retrieves the information used to generate the statement tendered in evidence.[56] The fourth condition under section 84 (2) (d) simply requires that the information contained in the statement was supplied to the computer in the ordinary course of its normal use.

Now, when can it be said that proper foundation has been laid for admissibility of electronically generated evidence under section 84? There is no hard and fast rule about this. The required foundation will vary with the facts and circumstances of each case. There is no "one size fits all" approach that can be taken when laying foundation for the admissibility of electronically generated evidence.[57] *In Lorraine v. Markel American Ins. Co.*[58] Judge Grimm remarks that any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the wide diversity of such evidence, there is no single approach to authentication that will work in all instances. Rather, as with the authentication of any kind of proffered evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the particular case.

A Case for a Liberal Approach

In treating the conditions set out in section 84 (2), it is suggested here that courts should adopt a liberal approach. Courts should not insist in the use of technical language in order to hold that a witness satisfies the stipulated conditions. What should matter to courts is whether or not the evidence of a witness, broadly speaking, substantially covers all the requirements set out in section 84 (2). If it does, the document should become admissible. In *R v Shephard* [59] the House of Lords while interpreting section 69 of PACE Act 1984 held that the said section can be satisfied by the oral evidence of a person familiar with the operation of the computer who can give evidence of its reliability and need not be a computer expert. Lord Griffiths affirms that:

> *Computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. I suspect that it will very rarely be necessary to call an expert and...in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly.*"[60]

In R. v Spiby[61] it was held that a hotel manager was competent to give evidence to satisfy the conditions in section 69 of the Police and Criminal Evidence Act, 1984 that the computer was working properly at the relevant time.

Meanwhile, two broad principles can be deciphered from the decision of the Supreme Court in *Kubor & Anor. v Dickson & Ors.*[62] First, Kubor's case has set a standard reference of compliance for admissibility of computer generated evidence under the Evidence Act, 2011. It is mandatory to fulfil all the conditions in Section 84. It also seems clear, from the decision, that fulfilment of the conditions is cumulative. This position is in tandem with that of the Supreme Court of India in *Anvar v Basheer*,[63] where the court held that computer output is not admissible without compliance with section 65B of the Evidence Act of India (as amended). The same conclusion was reached in *R. v. Shephard* [64] by the House of Lords.

Second, Kubor's case seems to have established an important point in respect of section 84, to the extent that the conditions stated therein must be proved by oral evidence. This derives from a passage in the judgment where the apex court quotes the lower court with approval thus:

> *A party that seeks to tender in evidence a computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer must be called to establish the conditions set out under section 84 (2) of the Evidence Act, 2011".*[65]

The duty imposed under Section 84 (1) and (2) certainly requires anyone who wishes to introduce computer evidence to produce oral evidence that will establish that it is safe for the court to rely on such documents produced by the computer.

Section 84 (3) provides that the following computers shall constitute a single computer:

- a combination of computers operating over that period; or
- different computers operating in succession over that period; or
- different combinations of computers operating in succession over that period; or
- in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers.

Production of a Certificate under Section 84 (4)

Section 84 (4) of the Evidence Act, 2011 provides for the requirement of production a certificate of authenticity in order to satisfy the conditions set out in section 84 (2), signed by a person occupying a responsible official position. Such a certificate will be evidence of any matter stated in the certificate. The certificate must identify the document containing the statement, describe the manner in which it was produced, and also give such particulars of any device involved in the production of the document as may be appropriate for the purpose of showing that the document was produced by a computer. The certificate must also deal with any of the matters to which the conditions mentioned in subsection 2 relate.
The sub-section states:

> *84 (4). In any proceeding where it is desired to give a statement in evidence by virtue of this section. a certificate -.*
> *(a) identifying the document containing the statement and describing the manner in which it was produced;*
> *(b) giving such particulars of any device involved in the production of that document as may be appropriate for the purpose of showing that the document was produced by a computer:*
> *(i) dealing with any of the matters to which the conditions mentioned in subsection (2) above relate, and purporting to 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, shall be evidence of the matter stated in the certificate: and for the purpose of this subsection it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.*

Production of a certificate is an additional step required by the Evidence Act, 2011 to establish the fact that the computer that produced the document is reliable. It is not a way of avoiding or dispensing with the *viva voce* evidence of a witness who seeks to establish the foundation required under section 84 (2). Legal practitioners and prosecutors should now be aware that in addition to fulfilling the conditions stipulated under section 84 (2), they should submit a certificate of authentication under section 84 (4) in evidence. In *Jagdeo Singh v. The State & Ors*[66] while dealing with the admissibility of intercepted telephone calls in a CD and

CDR which were without a certificate under section 65B of the Indian Evidence Act, the court observed that the secondary electronic evidence without certificate is inadmissible and cannot be looked into by the court for any purpose whatsoever.

For the purpose of section 84 (4), a clarification is offered that it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it. One knotty issue that may arise in respect of application of section 84 (4), is a situation where a police detective recovers an incriminating document, that is electronically generated, from a suspect. How is such a document to be authenticated? Who issues the certificate of authentication under section 84 (4)?

There is yet no reported case in Nigeria in which section 84 (4) has been judicially considered as at the time of writing. The decisions of the Supreme Court in *Kubor & Anor v Dickson & Ors*[67] and *Omisore & Anor v Aregbesola & Ors*[68] have only emphasized the need for foundational evidence to be given and fulfilment of the conditions stipulated under section 84 (2) in order to render electronically generated evidence admissible.

For a proper understanding of what is involved in section 84 (4), it is expedient that the said subsection be read together with section 84 (1) and (2). If this is done, it becomes clear that it is mandatory that a certificate must accompany the electronically generated document that is to be tendered in evidence.[69] Even where CDs or DVDs are tendered, they must be accompanied by a certificate.[70] The electronic records involved in Anvar's case were some Video CDs containing the election propaganda announcements, interviews, and public meetings alleged to have been made by the respondent's side, which were originally recorded in mobile phones and movie cameras, and the same were transferred to computers, and by using the said computers as devices for data transferring, the CDs were produced. The Supreme Court of India explains the position by saying that an electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under section 65 B are satisfied.[71]

Emphatically, the point must be made here, that what is required under section 84 (4) is not certification of a document by mere stamping, but a certificate. The language of the subsection bears this point out very clearly. What is not clear, however, is whether or not the certificate can take the form of an affidavit. This is against the backdrop of the statement of affirmation required in section 84 (4) (b) (i) that "for the purpose of this sub-section, it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it." Under the Singapore's Evidence Act (as amended), authenticity of electronic records, reliability and accuracy of the process of their production can be established by affidavit. Our courts should find nothing offensive in the use of affidavits to establish the facts required under section 84 (4). After all, a certificate has been defined as "a document in which a fact is formally attested"[72]

Section 84 contains potentially volatile provisions that may likely raise many questions that are capable of engendering serious legal debates. Such arguments may ultimately find their ways to the courts where the courts would be tasked with the responsibility of pronouncing on them one way or the other. It, therefore, remains to be seen how courts in Nigeria would treat such issues as may be presented before them.

ADMISSIBILITY OF DIFFERENT FORMS OF ELECTRONICALLY GENERATED EVIDENCE

(i). Emails

One of the new methods of communication introduced in this modern era of information technology is email. Email simply means electronic mail. It is usually sent from one person to another or several recipients, as the case may be, by electronic means through the use of computer. The process of sending an email operates in the same way as the traditional postal system. When an email is sent from a computer, it passes on to a number of Message or Mail Transfer Agents (MTA's). An MTA otherwise known as 'mail relay' is a "software that transfers electronic mail messages from one computer to another, using client-server application architecture."[73] It acts as the traditional post office. It "implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol"[74]. An email sent, is delivered into the email box of the addressee, similar to the traditional post office box. The addressee secures or protects the contents of the email box through a password that operates like the key of a padlock, by which access is gained into the box. Without the recipient of the email surrendering his password and thereby lifting all protection of privacy, the mail in question cannot be easily accessed.

A major characteristic of an email is that it carries the name by which the sender identifies himself in his email address (which may not necessarily be his real name). It also includes Internet Protocol address of the Internet Service Provider through whose medium the computer system from which the email was sent. It will also add the current time and date, the name of the MTA together as additional information at the top of the message.

Email has a forwarding system which allows for modification of its contents. Another feature of an email is that it is susceptible to what has been described as "after-the-fact alteration"[74a] Unknown to many, an email is somehow difficult to delete as the so-called 'deleted' data can still be discovered by computer experts. Radhakrishna explains what happens when an email is said to have been deleted: "Deleting" merely means that the computer entry in the disk directory is changed to a 'not used' status permitting the computer to 'write over' the 'deleted' data. Until the 'deleted' data is 'written over' it may be recovered"[75]

How is an email to be proved in evidence? The starting point is to draw attention to the provision of section 153 (2) of the Evidence Act, 2011 which provides for a presumption as to electronic messages. The court may presume the accuracy of an electronic mail message but shall not make any presumption as to the person whom the message is sent. In order to

render a printout of email admissible, conditions stipulated in section 84 (2) and (4) must be fulfilled. The fulfilment of the conditions translates to the fact that the following must be proved by credible evidence: (a) relevance, (b) authentication or identification of the email, (c) integrity of the email, (d) reliability of the computer that produced it and (e) production of certificate of authentication.

A witness who desires to tender an email message must proceed on the basis that such evidence is relevant to the issue under inquiry. According to Phipson, it is "correct… in deciding whether evidence of a fact is admissible, to ask first whether the fact is relevant…"[76] The general principle of law that "all evidence that is sufficiently relevant to an issue before the court is admissible and all that is irrelevant or sufficiently irrelevant should be excluded is applicable to emails.[77] In *Lorraine v. Markel*[78] it is stated that relevance is the first thing to be established for any potential piece of evidence, including electronic document. Once relevance has been established, the next step is to prove the authenticity of the email.

Electronic evidence generally must be authenticated or identified before it may be admitted. Authentication is simply a process of verification or identification that establishes that the particular document is what is purports to be. The onus is on the proponent of an email to authenticate it.

There are many ways by which an email may be authenticated. They include facts relating to the features the email bears. These include, amongst others, the date of the transmission of the mail, email address of the sender and the recipients, user name, nickname, screen name, web name, the subject of the mail. In *Manuel v, The State*[79] it was held that an email is properly authenticated if its appearance, contents, substance or other distinctive characteristics, taken in conjunction with other circumstances, support a finding that the document is what its proponent claims.

The testimony of an authenticating witness may be direct or circumstantial evidence. In *United States v. Safavian*[80] the following guidelines on the nature of circumstantial evidence required to establish the authenticity of an email were stated by the United States Court of Appeals, District of Columbia Circuit;

(i) that a witness or entity received the email
(i) that the email bore the customary information in the email
(ii) that the address of the recipient was consistent with the email address on other mails sent by the same sender.
(iii) that the email contained electronic signature of the sender
(iv) that the email contained matters known only to the alleged sender
(v) that the email was in fact sent as a reply to the sender
(vi) that following the receipt of the email, the recipient communicated with the alleged sender and the conversation reflected the sender's knowledge of the contents of the email.

The point has to be made here, with due emphasis, that the sending address of an email message is not conclusive evidence that the owner of the address sent the email, since an email message can be sent by persons other than the named person.[81] For example, a person with an unauthorized access to a computer can transmit email messages under the

computer's owner's name. Because of the potential for unauthorized transmission of email messages, authentication of emails requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.

The next stage is to give evidence relating to the integrity of the email. To admit a printout of an email in evidence, the proponent must show the integrity of the email. It must be established that the email is complete in the form intended and free from error or fabrication. The proponent needs to prove that the hard printout of the email is consistent with the one in the computer. Proof of facts about the reliability of the computer that produced the email is also required as foundational evidence. One way by which a witness can show that the computer is reliable is evidence that the computer was working properly when the document was produced. A certificate shall be tendered under section 84 (4) of the Evidence Act 2011. This is a mandatory requirement. The certificate must be in conformity with section 84 (4).

(ii). Short Messaging Service (SMS)

Short Messaging Service (SMS) is a text messaging service component of the phone web or mobile communication system which uses standardized communication protocols to allow exchange of short messages popularly known as text messages. It is another form of electronic message by which a cell phone or hand-held device is used to send personalized electronic messages to another cell phone. The practice of sending text messages to family members, acquaintances, friends and foes e.t.c., has been on the increase. Research has shown that in 2010 alone, an estimated 6.1 trillion text messages were sent at an average of over 200,000 messages per second.[82]

Most text messages are drafted at the spur of the moment thereby providing pieces of evidence that can be raw, uninhibited and highly incriminating. The use of mobile phones in the commission of crimes has also become very rampant. Call data records (CDR) obtained from cell phones now constitute important tools to track criminals even when they are on the move.

The same principles of admissibility of emails are applicable to text messages. A text message is admitted in evidence on the basis of a proper foundation being laid for its authentication. The proponent of the text message should be able to authenticate it, which means that he should be able to identify the text and the person who transmitted the message.

The easiest way to authenticate a text message is to have the opposing party admit that he sent it. This is on the basis of the principle that what is admitted need no proof. Like emails, text messages have certain seemingly self-authenticating features. For instance, a text message is marked with the sender's cell phone number. Nonetheless, given the possibility of a third party intervention by which such a message could be generated under the guise of the named sender, courts have been weary in attributing a text message exclusively to the person to whom the phone number is assigned. Indeed, the underlying reason for authentication requirement is the possibility that a third party could have used the cell phone to send a text

message. Therefore, a text message may not have originated from the person who appears to have sent it.

(iii). Tapes and Video Recordings

Tape records, video films etc., are parts of modern technological devices that make the probability of truth highly certain. They are admissible in evidence if properly tendered. Tape-recording can be used in court to corroborate the statements of a person who deposes that he had carried on conversation with a particular person. A previous statement of a person which has been tape-recorded can also be used to test the veracity of the witness and to

It is now beyond any dispute that tapes and other sound recordings are documents. There are legislative and judicial authorities to support this standpoint. Section 258 (1) of the Evidence Act, 2011 now defines 'document' to include video and audio tapes. The Court of Appeal affirms that the video recordings admitted in *Obatuga & Anor v. Oyebokun & Ors*[83] are documents. The same conclusion was also reached in *Federal Polytechnic Ede & Ors v. Oyebanji*.[84] Tape recording of conversations and other sounds are, therefore, admissible as statements contained in a document produced by computers. A transcript of the recording will also be admissible as a copy under section 258. From the decision of the Court of Appeal, in Oyebanji's case, the following guidelines are decipherable for admissibility of tape recordings:

(i) Foundation must be laid that will make the tape recording admissible in evidence.

(ii) Evidence must be led to show that the tape recording is authentic.
(iii) Proof that the voice is indeed that of the person it purports to be.
(iv) Proof that the tape was in proper custody all the time such that there was no opportunity for anyone to tamper with it.

Identification of the voice in tape recorded conversation is of paramount importance for purposes of admissibility. Where the voice recorded is not audible the accuracy of the recording cannot be said to have been established. In *Venkatesan v. State*[85] the conversation was not audible throughout and was broken at a very crucial place. It was held that the accuracy of the recording was not proved, and the voices were also not properly identified. In the circumstances, the court concluded that it would not be safe to rely on the tape-recorded conversation as corroborating the evidence of the prosecution witness.

(iv). Digital Photographs

For many years now, photographs have been admissible in evidence in Nigeria on proof that they are relevant to the issues involved in the case. It has also been the practice to tender the negatives along with the photographs as proof that the prints are taken from the negatives untouched. Photographs have always been treated as documents reproduced by means of

mechanical and chemical devices. Calling the photographer or offering expert testimony about how a camera works almost has never been required for traditional film photographs.

Today, however, most photographs taken and offered in evidence at trials are digital photographs. They are not made from films, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present serious challenges of authentication. This is particularly so as they are a form of electronically produced evidence, capable of being manipulated or altered. Indeed, unlike photographs made from films, digital photographs may be 'enhanced'. Digital image 'enhancement' involves removing, inserting, or highlighting an aspect that the technician wants to change. It, therefore, becomes imperative that before a digital photograph may be admitted, requisite foundation must be laid to prove its authenticity.

It is paramount to recognize that photographs fall within the category of documents within the meaning of section 258 of the Evidence Act, 2011. They are excluded from the meaning of copies of documents under the same section. Accordingly, photographs are no longer to be treated as secondary evidence, as it was the practice under the old Evidence Act[83] Section 86 (4) of the Evidence Act, 2011 also buttresses this position. The subsection provides in part, that 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 mechanic process, each shall be primary evidence of the contents of the rest.

The principal requirements to admit a digital photograph into evidence, essentially, are relevance and authentication. Unless the photograph is admitted without objection, the party tendering it must be prepared to offer testimony that the photograph is an accurate representation of the scene or object it captured. This usually means someone must testify that the photograph accurately portrays the scene as viewed by the witness. The evidential value of a memory card usually tendered along with a digital photograph is yet to be statutorily or judicially established. It is, surely, not one of the requirements of the law to render such a document admissible under section 84 of the Evidence Act, 2011.

(v). Social Media

The term, 'social media' is an umbrella term. It is the integration of technology with social interaction to create value. It rests on Internet tools that enable shared community experience through multidirectional conversations that create, organize, edit, combine, and share content.[84] Examples of social media sites are Facebook, Twitter, Linkedln, Myspace, WhatsApp, Google Plus+, Meetup, Faceparty, Faces.com, Instagram, Netlog, MyLife, amongst others. Social networking websites permit their members to share information with others. Members create their own individual web pages (their profiles) on which they post personal information, photographs, and videos and from which they can send and receive messages to and from others whom they have approved as their "friends." Anyone can create a Facebook or MySpace profile at no cost, as long as he or she has an email address and claim to be over the age of 14.[85]

The existence of social media sites has facilitated easy connections and interaction with individuals around the world. Regrettably, these social media sites have also become vehicles by which all kinds of evils are perpetrated, from the simple to the most heinous.

Criminals now take advantage of such relationships to perpetrate crimes. The case of Cynthia Osokogu, who was alleged to have been gruesomely murdered by her Facebook friends, Okwumo Nwabufor and Olisaeloka Ezike, is in point here. Cynthia was a post-graduate student of Nasarawa State University, Keffi, Nigeria. She also engaged in business. She was the only daughter of her parents. Cynthia was described by newspaper reports as a pretty, vibrant and enterprising young lady.[86] It was also reported that she met two University of Lagos undergraduates on the Facebook and befriended them. She had chatted with these "friends" for several months on the Facebook. In the course of their conversations, they developed friendship and a level of trust. The so-called friends invited Cynthia to Lagos to purchase new stock for her business. They promised to pay her flight ticket and hotel bills. Cynthia trusted her "friends". On arrival in Lagos, the "friends" picked her at the airport and drove her into Cosmilla Hotel. At the hotel, her drinks were drugged. The "friends" robbed her of the money she brought for her business and raped her overnight. At the end, they strangled her to death and tied her to the bed in the hotel room. They then left the hotel and quickly deleted her name from their Facebook friends' list. The alleged killers were eventually identified through the use of CCTV in the hotel.[87] The trial of the two persons suspected to be Cynthia's Facebook friends and killers is on-going at time of writing. Personal information, messages, photographs, and videos posted on social medial sites can be useful at trials. For instance, in the case involving the alleged killers of Cynthia the laptop of one of the suspects containing the obscene pictures of the deceased has been tendered and admitted in evidence by the trial court.[88]

The key issue in respect of admissibility of social media messages and posts is typically one of authorship. The question usually revolves around whether or not what was posted originated from the account holder. On its own, the fact that a message bears the name of a person or posted in his user's account is not sufficient to authenticate the communication as having been authored or sent by that person. There have been instances of account holders disclaiming posts on their Timelines. Like emails, a third party may have sent such posts. There must, therefore, be some confirming circumstances sufficient to permit the inference that the purported sender was in fact the author. It is also important to note that there is so much flexibility in the operation of social media sites, such that anyone is free to create a profile page using whatever name he or she chooses; so the mere existence of a profile page in someone's name does not necessarily reflect that the purported creator had anything to do with its creation. Such postings do not require a unique user name and password.

(vi). Automated Teller Machine (ATM)

Automated Teller Machine (ATM) is "a computerized machine that permits bank customers to gain access to their accounts with a magnetically encoded card and code number. It enables the customers to perform banking operations without the help of a teller such as to withdraw cash, make deposits, pay bills, obtain bank statements and effect cash transfers."[89]

ATM machines are scattered in every nook and cranny of cities and towns, allowing customers easier access to their accounts. Anyone with a debit or credit card will be able to access most ATMs. Usually, if a customer uses a machine operated by his bank, he pays no fee, but accessing funds through a unit owned by a competing bank will usually incur a small fee.[90]

Litigation involving ATM may take many forms. The most rampant usually takes the form of allegation of unauthorized withdrawal of funds using a customer's ATM card. The underlying supposition of the proponent is that a thief took advantage of the negligence of the bank and the weaknesses inherent in the IT systems of the bank to perpetrate the fraud. He attributes no negligence to himself. The onus, thereafter, shifts on the bank. How is this onus to be discharged?

The bank must produce evidence that the payment transaction was authenticated. This in turn means that the bank must demonstrate: (a) the methods it uses to verify the use of the debit card and ATM or on-line banking account, and, (b) how all of the personalized security features (e.g. PIN, password) worked.

The bank must further prove that the transaction was accurately recorded and entered in the payment service provider's accounts. It must also show that the transaction was not affected by a technical breakdown or some other deficiency. Above all, the bank must prove that the payment transaction was authorized by the payer. To do so, the bank must produce evidence to show that the customer's card was inserted into the machine and the customer's PIN was keyed in, and that the customer, or a person authorized by the customer, was responsible for carrying out the transaction.

The sense behind this procedure is that if the software reports that the customer's card was inserted into the ATM and the customer's PIN was keyed in, then it follows that the customer's card was used and the correct PIN was keyed into the machine. Taking this logic one stage further, the bank then assumes that the customer was physically at the ATM, or somebody authorized by him. Where the customer claims he was not responsible for the transactions in dispute, the bank tends to claim that the customer was grossly negligent, in that not only did he allow a thief to get hold of the card, but that the thief took possession of both the card and PIN. The underlying premise is that the technology of the bank is not only perfect, but it cannot be undermined in any way.

Two cases illustrate the attitude of Nigerian courts to litigations involving ATM transactions. The first is *Geoffrey Amano v United Bank for Africa (UBA) PLC*[91] *and* is *Agi v Access Bank Plc.*[92]

(vii). INEC Smart Card Reader Machine

One of the innovations of the 2015 general elections in Nigeria was the introduction of the use of Smart Card Reader (SCR) technology by the Independent National Electoral Commission (INEC). Its existence is rooted in paragraph 13 of the Approve Guidelines and Regulations for the Conduct of 2015 General Election.

There are varieties of card readers but the one designed for INEC is a portable electronic voter authentication device, configured to read the Permanent Voter Cards (PVCs) issued by INEC. The card reader device was designed specifically for authentication of eligible voters

before voting. INEC smart card reader is not a voting machine. It only verifies the authenticity of the PVC of a prospective voter. It is used to scan the PVCs in order to verify the identity of a voter in a polling station. Thereafter, the name of the voter is cross-checked in the Register of Voters. It is not the means by which a voter is accredited but a kind of screening exercise carried out before accreditation.

INEC smart card readers surely qualify as 'computers' within the meaning of the word in section 258 of the Evidence Act, 2011. Accordingly, any data generated by such card reader intended to be tendered as evidence in court must fulfil the conditions for admissibility stipulated under Section 84 of the Evidence Act, 2011. Any output of the card reader must be duly authenticated. Its integrity must be proved to the extent that it is securely preserved and not made vulnerable to any form of manipulation. The integrity of the device must also be established as it must be found to be reliable. This, invariably, is a function of its performance in authenticating PVCs. A certificate under Section 84 (4) is also required to be produced to render such evidence admissible. The standard required to prove these facts should be minimal. The evidence of experts may not be required in all cases. The evidence of a witness who is familiar with the use of the device ought to be taken as sufficient.

Matters that pursued to the Supreme Court in relation to the smart card technology concern the following:

1. Whether or not irregularities occasioned by the use and /or non-use of card readers can constitute grounds for questioning an election. See: *All Progressive Congress v. Agbaje & Ors*[93]
2. Whether or not card readers can substitute, overthrow or replace voters' registers. *Shinkafi & Anor v. Yari & 2 Ors.*[94]
3. What purpose is a card reader meant to serve? *Shinkafi & Anor v. Yari & 2 Or*[95] *Nyesom v. Peterside & 3Ors*[96]*; Okereke v. Umahi & 2 Ors; Emmanuel v. Umana*[97]
4. The rationale behind the principle of preference of voters' registers over card readers in matters relating to accreditation. *Okereke v. Umahi & 2 Ors*[98]

CONCLUSION

Now that it has become undeniable that we live in the age of computer and information technology, the range of electronic evidence that may be tendered in legal proceedings is limitless. It ranges from simple electronic documents and records through files on digital cameras to complex behaviour of computers attached to the Internet etc. It is commendable that the Nigerian Legislature ultimately, though belatedly, made provisions for admissibility of electronic evidence in the Evidence Act, 2011. All the same, the following observations and recommendations can validly be made.

In the first place, the provisions relating to admissibility of electronic evidence under the Evidence Act, 2011 is grossly inadequate. It is a far cry from the provisions of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce. The definitions of some basic terms that are missing in Evidence Act, 2011 are contained in the Model Law. They include: 'Originator' of a data message, 'Addressee' of a data message, 'Intermediary' with respect to a particular data massage, 'Information system' etc. Other terms that are not legally defined but require to be defined include 'certificate', 'electronic communication' 'digital signature' and 'electronic records'. These terms are of

common usage in the electronic world such that failure to define them may pose some definitional problems in the nearest future.

Secondly, the definition of 'computer' as contained under section 258 of the Evidence Act, 2011 is limited in scope. A more comprehensive definition of 'computer' is found in Section 34 of the National Information Technology Development Agency Act 2007. Therein, 'computer' is defined as:

> *Any electronic device or computational machinery using programmed instructions which has one or more of the capabilities of storage, retrieval, memory, logic, arithmetic or communication and includes all input, output, processing, storage, software, or communications facilities which are connected or related to such devices in a system or network or control functions by the manipulations of signals, including electronic, magnetic or optical, and shall include any input, output, data storage, processing or communication facilities directly related to or operating in conjunction with any device or system or computer network.*

This definition is strongly recommended to be incorporated into the Evidence Act.

Thirdly, the definition of 'banker's books', under section 258 is anachronistic and should be revisited. It is recommended that the definition of banker's books in the English Banking Act 1979, which is the same as that of the Indian Information Technology Act 2000 be adopted. Section 9 (2) of the said Banking Act 1979, defines 'banker's books' in the following terms:

Banker's books include:

> *Ledgers, day-books, account books and other records used in the ordinary business of the bank, whether those records are in written form or are kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism.*

This definition is technologically neutral and will take into account future advancement in technology regarding banking business.

Fourthly, there are no detailed rules for presenting electronically generated evidence under the Evidence Act, 2011. Provisions requiring authentication of electronic documents should be spelt out in the manner it is done under the USA Federal Rules of Evidence (FRE). Only when such rules are in place will the law on admissibility of electronic evidence be applied with some measure of certainty.

Fifthly, the status of printouts should now be statutorily defined to remove every form of ambiguity. In this regard, the status of printouts as defined in Rule 1001 (1) of the Federal Rules of Evidence of the United States of America is strongly recommended. Therein, it is stated: *"...If data are in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an "original".*

The ball is, once again, in the court of the Legislature to consider these recommendations. In matters concerning legislation, the courts are not in any stead to act. In *UBA v. Tejumola & Sons,* Obaseki, J.S.C., puts it most succinctly:

> *...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 over-step its bound and trespass upon sacred province 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*[99].

It is, therefore, incumbent upon the National Assembly to show sufficient interest on these issues as a matter of utmost urgency. The National Assembly should appreciate that we live in a changing world which requires a changing law. In a progressive world, the law cannot afford to be static.

References

1. Paper delivered at the Refresher course organized for Judicial Officer by the National Judicial Institute (NJI) from 14th – 18th March 2016.
2. Judge of the High Court of Justice, Kogi State.
3. Mason, S., (2007) Sources of digital evidence. In Mason, S. (Ed) Electronic Evidence: Disclosure, Discovery and Admissibility (1st ed.). Butterworth .
4. Ibid. P. 22.
5. (2007) 5EFCLR 204
6. P. 228
7. No 0410648 of July 24, 2006
8. Supra
9. Supra
10. (1969) NMLR 198
11. Ibid. PP. 216 – 217

11(a) (1976) 4SC 1

12. Ibid. P. 13
13. See Alhaji Yusufu v. Egbe (1987) 2NWLR (Pt 56) 341.
14. See Nwana v. Federal Capital Development Authority (1999) 10 CLRN 63
15. Supra
16. Supra
17. (2003) 13 NWLR (Pt 834) 216
18. Per Salami, JCA (as he then was) PP 216 - 217
19. (1987) 3NWLR (Pt 59) 108
20. (2010) LPELR 4689 (CA)
21. Ibid P. 23

22. Supra

23. (2010) 14 NWLR (Pt 1214) 487

24. (1995) 9 NWLR (Pt 419) 324

25. (2004) 3 NWLR (Pt 861) 516

26. Supra

27. P. 543

28. Ibid

28a (2003) FWLR (Pt 145) 661

29. Supra

30. Case No FHC/L/523c/08 of 26/3/2009 (unreported).

31. Supra

32. See Tobi, JSC in Araka v. Egbue (2003) 17 NWLR (Pt. 848) 1

33. (2012) LPELR – 9725 (SC)

34. (2013) LPELR – 21474 (CA)

35. (2012) LPELR 19696 (CA)

36. (2014) LPELR 22344 (CA)

37. Tur, JCA, in Hallmark Nigeria Ltd & Anor v. Gomwalk (2015) LPELR – 24462 (CA) P. 60

38. Section 258 (1) of the Evidence Act, 2011.

39. Ibid.

40. Section 153 (2)

41. (2003) 7 SCNJ114

42. Ibid P. 126

43. (2013) LPELR – 20411 (CA)

44. Ibid P. 37

45. John, M.A. (1992) Computer Printouts as evidence: Stricter foundation or presumption of reliability ON LINE.

46. Ibid.

47. Supra Araka v. Egbue

48. (2013) 4 NWLR (Pt. 1345) 534

49. (2013) LPELR – 20532 (CA)

50. Per Jombo – Ofo, JCA at P. 30

51. Supra

52. Per Onnoghen, JSC PP 577 – 578

53. Op. cit

54. Ibid 'n.p.'

55. Lorraine v. Market American Ins Co. 241 FRD 534 (D.Md 2007)

56. See D.P.P. v. Mckeown (1997) 1 ALL ER 737

57. (Supra)

58. Judge Emily Miskel (2015) Admitting electronic evidence under existing rules www.emilymiskel.com/.../electronically-stored-information-a-z-acquire-e

59. (1993) 1 All ER 225

60. Ibid P. 231

61. (1990) Cr APP. R. 186

62. Supra

63. (2014) 10 SCC 473

64. Supra

65. P. 578

66. CRL A. 527 of Feb 2015, Retrieved from: indiankanoon.org/doc/35565129/

67. Supra

68. Supra

69. See Anvar v. Basheer (Supra)

70. Ibid

71. Ibid.

72. *Black's Law Dictionary* (9th ed.) p.255

73. Wikipedia. Retrieved from: https://en.wikipedia.org/wiki/Message_transfer_agent

74. Ibid.

74a. Radhakrishna. G. (2015) Challenges in admitting and authenticating emails. Proceedings-Kuala Lumpur International Business, Economics and Law Conference 6, Vol. 4 April 18 19, 2015 held at Hotel Putra, Kuala Lumpur, Malaysia. Retrieved from: http://klibel.com/wp-content/uploads/2015/04/KLIBEL6_Law__8_ruJE75P067.pdf

75. Ibid. P18

76. *Phipson on Evidence* (Supra) P. 106

77. See Collin Tapper (2010) *Cross and Tapper on Evidence* (12th ed.). P. 64. Oxford University Press

78. Supra

79. No. 12-09-00454-CR. Tex.App.-Tyler 2011. Retrieved from: https://cases.justia.com/texas/...appeals/12-09-00454-cr.pdf?...13239709

80. No. 09-31 Decided May 13 2011. Retrieved from: http://caselaw.findlaw.com/us-dc-circuit/1567340.html

81. Lorraine v. Markel American Insurance (supra)

82. See: Justin (2010). *200k SMS sent every second earning operators$812k per minute.* Report (International Telecommunications Union (ITU) Report). Retrieved from: http://mobilemarketingwatch.com/report-200k-sms-messages-sent-every-second-earning-operators-812k-per-minute-10453/.

83. (2014) LPELR – 223 44 (CA).

84. Serrat, O. (2010) S*ocial media and the public sector. Retrieved from Http://digitalcommons.ilr.cornell.edu/egi/viewcontent.egi?article=1191&context=intl*.

85. (1980) Cr LJ 41. Retrieved from: http://indiankanoon.org/doc/1099094/

86. Ada, A. (2012). Young Nigerian woman Cynthia Osokogu murdered by Facebook friends in Lagos. *The African Times*. August, 21, 2012 Retrieved from: http://africansuntimes.com/2012/08/young-nigerian-woman-cynthia-osokogu-murdered-by-facebook-friends-in-lagos-nigeria/.

87. Dania, O. (2014, July 01). Cynthia Osokogu: Court admits video evidence. *Vanguard.* Retrieved from: http://www.vanguardngr.com/2014/07/cynthia-osokogu-court-admits-video-evidence-2/.

88. Ibid.

89. Online Business Dictionary. Retrieved from: http://www.businessdictionary.com/definition/automated-teller-machine-ATM.html.

90. Currently, a sum of N65 is charged in Nigeria after the third transaction when the customer uses the machine of a bank other than his own bank

91. Reported at page 114 of the Section on (Legal Practice) Law Journal Vol. 3, 2013

92. (2014) BNLR 23 P. 135

93.(2015). CAR 23

94. SC. 907/2015. Delivered on 8th January, 2016
95. Ibid.

96. SC. 1002/2015, Delivered on 12th February, 2015. P. 47

97. Emmanuel v. Umana SC.1/2016. Delivered on 15th February, 2016

98. SC. 1004/2015. Delivered on 5th February, 2015

99. (1988) 5SC 264 at 293