Journal of Law, Policy and Globalization
ISSN 2224-3240 (Paper) ISSN 2224-3259 (Online)
Vol.92, 2019

Appraisal of Admissibility of Electronic Evidence in Legal Proceedings in Nigeria

Peter Ademu Anyebe
Nigerian Institute of Advanced Legal Studies, University of Lagos Campus, Akoka, Lagos, Nigeria

Abstract
The use of computers in Nigeria has grown exponentially in the last decade. Financial transactions, communication systems, modern automobiles and so on depend on computers. It is now an electronic age where daily transactions are conducted on the platform of electronic devises. In the event of disputes, parties are bound to rely on electronic evidence. It is in view of this development that in order to adopt the international best practice, the Evidence Act, 2004 was repealed and replaced with Evidence Act, 2011 to accommodate the admissibility of electronic generated documents before the Nigerian courts. The focus of this paper is to examine the prominent provisions of the Act relating to admissibility of electronic evidence. It will equally appraise the proof of conditions for admissibility of computer generated evidence, admissibility of electronic evidence in legal proceedings in Nigeria and challenges in determining the probative value of electronic evidence. The paper concludes that the provisions of the Evidence Act, 2011 on electronic proofs are largely inadequate and therefore, there is the need to understudy other jurisdictions in order to adequately confront the challenges facing admissibility of electronic evidence in Nigeria.
Keywords: keywords, admissibility, appraisal, document, electronic, evidence, hearsay
DOI: 10.7176/JLPG/92-01
Publication date: December 31st 2019

1. Introduction

The advent of information technology has introduced humanity into an era of hi-tech communication on the digital platform. This is now the age of swift transfer of information, borderless transactions, electronic transactions (e-transactions). The automation has radically altered the landscape of human activities. These digital developments have also redefined the pattern of legal proceedings in courts of law across the globe. Therefore, it is imperative that the law must keep pace with modern developments (Akhihiero 2013). Thus, the use of computers and other forms of electronic storage and communications systems has risen sharply in commercial and financial transactions in Nigeria (Charles 2013). The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mail, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from electronic door locks, and digital video or audio files (Muzaffar 2013). Electronic evidence has therefore assumed a very important position in the adjudication of disputes or cases be they criminal or civil. The law of evidence in Nigeria made provisions for the admissibility of computer generated or electronic evidence through section 84 of the Evidence Act, 2011. Consequently, the enactment of the 2011 Evidence Act marks a watershed in the anal of Nigeria's legal system. It has not only provided for the admissibility of electronic and computer generated evidence but has located electronic and computer generated evidence within the realm of documentary evidence. Hence, like every other documentary evidence, electronic and computer generated evidence can be proved either by primary or secondary evidence. This paper takes a look at the appraisal of the admissibility of electronic evidence in legal proceedings in Nigeria. Such areas as concept of electronic evidence, sources of electronic evidence, proof of conditions for admissibility of computer generated evidence, admissibility of electronic evidence in legal proceedings in Nigeria, challenges in determining the probative value of electronic evidence and international best practice are briefly considered in the paper.

2. Clarification of concepts

2.1. Evidence

Evidence is the means by which facts are proved but excluding inferences and arguments (Aguda 1974). The learned author stated as follows:

> It is common knowledge that a fact can be proved by oral testimony by persons who perceived the fact or by the production of documents or by the inspection of things or places-all this will come within the meaning of judicial evidence. On a very broad view, it is sometimes, permissible to include in this list such other means of proving a fact as admissions and confessions, judicial notice, presumptions and estoppels

The Black's Law Dictionary defines the word evidence as:

> Any specie of proof or probative matter, legally presented at trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, concrete objects, etc., for the purpose of inducing belief in the minds of the court or jury as to their contention.

Any matter of fact that a party to a law suit offers to prove or disprove an issue in the case is known as evidence. It is a system of rules and standards that is used to determine which facts may be admitted, and to what extent a judge or jury may consider those facts, as proof of a particular issue in a law suit.

Evidently, evidence, during trial proceedings in the courts is taken during the course of interrogation of a person on oath or affirmation. The evidence of the witness is obtained by oral examination called the examination-in-chief. The witness is then examined on behalf of the opposite party in order to diminish or dismantle the effect of his evidence, under what is called, cross-examination. The party calling him in order to give an opportunity of explaining or contradicting any false impression produced by the cross-examination again examines him. This is called re-examination and it is necessarily confined to matters arising out of the cross-examination.

This pattern of eliciting evidence in Nigeria's courts follows whether the suit is civil or where there is accusation of a crime under a charge or information (Umezulike 2000).

The law of evidence in Nigeria is governed by the Evidence Act, 2011. It came into force on the 3rd day of June, 2011. It repealed the Evidence Act Cap E14 by its section 257. According to its long title, the Evidence Act, 2011, is an "Act to repeal the Evidence Act Cap E14, Laws of the Federation of Nigeria and enact a new Evidence Act which shall apply to all judicial proceedings in or before courts in Nigeria and for related matters."

2.2. Electronic Evidence

Evidence generated by some mechanical or electronic process. Electronically generated evidence can be defined as the use of electronically, controlled machines or equipments either by wave of satellite or through cables computers and other forms of storage and communications systems as evidence in the court of law. Such evidence can be derived from e-mails, phone logs, POS and ATM transaction logs, social media records such as face book, twitter, whatsapp, instragram, you tube videos, Digital content in DVDS, CDS, Flash disks, Data retrieved from Clod Computing. A major characteristic of this class of documents is that unless printed, they are paperless and though contained in tangible objects are visible but intangible.

2.3. Admissibility

The conditions for the admissibility of evidence in civil proceedings are different from those one in criminal proceedings. In civil matters, the conditions for admissibility were stated by the Supreme Court in the case of *Torti v. Ukpabi* (2004) thus:

- Whether such evidence has been pleaded?
- Whether it is relevant?; and
- Whether its admissibility is not excluded by any rule of law?

It has been stated in *Pius v. State* (2012) that proof of evidence to some extent is to criminal matters what pleadings are to civil trials. In civil trials, where facts are not pleaded, they are inadmissible, while facts which are not stated in the proof of evidence may be tendered and admitted in criminal trials. The principle of law here however is that parties are bound by their pleadings. As such, evidence of facts not pleaded are not admissible. Even where they are admitted, they go to no issue (see *C.D.C Nig. Ltd v. S.C.O.A. Nig. Ltd* (2007). This was the principle of law stated in the case of *Amadi v. A-G*, (2012). Imo State where the court held that proof of evidence does not have to contain every bit of evidence that the prosecution requires as long as it contains relevant and sufficient facts to sustain a prima facie case against the accused person. Thus, in criminal trials, admissibility of facts, whether stated in the proof of evidence or not, is governed by relevance of such facts and other strict rules of admissibility relating to free and fair trial. Furthermore, a court in civil trial may have discretion whether or not to reject a piece of evidence that is inadmissible, but in a criminal trial, it is under a duty to reject such evidence (*Raimi v. Akintoye* (1963). Consequently, one can safely conclude that rules of admissibility are more stringent in criminal trials than in civil ones.

2.4 The concept of Electronic document

It must be pointed out that the Evidence Act did not expressly employ the phrase 'electronic document'. However, reference to electronic document in the Act can be gathered from section 258 (1) of the Evidence Act, 2011 which defines document as:

- Books, maps, plans, graphs, drawings, photographs, and also include 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;
- 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;

- 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;
- In the case of a document not falling within the said paragraph (c) of which the visual image is embodied in a document falling 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.

The same section defines "copy of document" as follows:

- In the case of a document 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;
- In the case of a document within paragraph (b) but not (c) of that definition, a reproduction or still reproduction of the image of images embodied in it whether enlarged or not;
- In the case of a document falling within both those paragraphs, such a transcript together with such a still reproduction; and
- In the case of a document falling within the said paragraph (c) of which a visual image is embodied in a document falling within the 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.

It is evident that from the combined effect of the definitions of "document" and "copy of a document", electronic evidence is not only restricted to computer generated documents. The scope of document as defined by the Act includes even "…sound track and other devices in which sounds or other data (not being visual images) are embodied…" such that transcript of sounds even from a transistor radio represent copy of a document, so much as visual images on television and by extension video conferencing images and sound tracks. Thus, in *Amitabh Bagchi v. Ena Bagchi, (*2005) the court held that physical presence of a person in court may not be required for purpose of adducing evidence and the same can be done through medium of video conferencing as definition of electronic records include video conferencing. Similarly, in the *State of Maharashtra v. Dr. Praful B. Desai*, (2003), the Supreme Court of India stated as follows:

> Video conferencing is an advancement of science and technology which permit seeing, hearing and talking with someone who is not physically present. The legal requirement for the presence of the witness does not mean actual physical presence.

It stands clear from the above definition that the present Evidence Act is a significant improvement on the definition of document under the repealed Evidence Act. (2004). The definition of document in the repealed Act was restricted to documents in analogue or physical format. It did not cover documents in digital format. This new definition has sufficiently bridged the gap between the digital world and the physical world (Ukpai and Oji 2014). In other words, some pieces of evidence that were hitherto inadmissible under the repealed Act can now be admitted under the present regimes. Information contained in electronic mails, text messages and other information contained in the mobile phones, digital cameras, video and audio tapes constitute electronic documents and are now admissible in evidence (Evidence Act 2011)

Document has been defined as something tangible on which words, symbols, or marks are recorded. For a better understanding, the Evidence Act of 1945 defined document to include Books, maps, plans, drawings, photographs and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means intended to be used or which may be used for the purpose of recording that matter. This definition was too restrictive (*Egbue v. Araka* (1996).

From the above, electronic document refers to information stored or transmitted in electronic or digital form or information stored in a computer. Computer is defined as: Computer means any device for storing and processing information, and any reference to information being derived from other information is a reference to it being derived from it by calculation, comparison or any other process.(*Kubor v. Dickson* 2013)

Bolaji Owasanye (2015) categorized electronic documents in terms of their uses as follows:

1. Information in digital format (including electronic records and digital media) used to prove allegations or argument;
2. Useable in internal investigation, trial before a tribunal or court and in civil or criminal actions;
3. Used to establish facts-prove or disprove allegations about events that have taken place, e.g. creating data on a device, deleting logs or database, establish consistency or continuity of an action or activity;
4. Electronic evidence is associated with computer forensics in different ways, viz:
    - Collecting the electronic evidence: identifying and extracting digital information that can be used to establish proof;
    - Protecting the electronic evidence: implementing controls to ensure the integrity of

information available in digital format, e.g. preserving a database or log book.

- Presenting the electronic evidence: processing information in the context of events such that it is understandable in a tribunal or court of law.

3. Sources of electronic evidence

There are different techniques that are capable of creating evidence in digital format. The computer remains the primary source of electronic evidence. The computer here means any electronic device that accepts, processes stores and outputs data at high speed according to programmed instruction. In this sense, the term includes a range of gadgets such as mobile phones, cameras, music players, calculators, meters, ATM machines, traffic lights, car tracking devices, etc,.(Akhihiero) All these devices are computers in their own right in as much as they have a CPU, memory, input and output devices, screen and they are loaded with operating software. These devices are increasingly being used by individuals and organizations as part of their information technology infrastructure. They are used for the storage and processing of electronic data. Invariably, a huge chunk of electronic evidence emanate from these sources (Akhhiero). Other sources include the network where more than one computer may operate to generate data. There are different types of networks. They include the internet, which is a network that links computers all over the world by satellite and telephone, connecting users with other service networks such as e-mail and the World Wide Web. Other sources include intranet, wi-fi (wireless fidelity)-it uses the radio waves to transmit data and Bluetooth which connects the devices within a short range, using another radio frequency (Akhhiero).

a. Electronic Evidence in Nigeria before the Promulgation of Evidence Act, 2011

Prior to the Evidence Act 2011, the various laws on evidence from 1958 to 2011, were silent on the admissibility of electronic evidence. Admissibility of such evidence depended on fulfilling the requirements that governed the admissibility of documents generally, in their primary or secondary forms (Usoro 2016). In the late 1970, the Supreme Court in *Yesufu v. African Continental* Bank (1976), observed the inadequacy of the Evidence Act in a banking transaction on the admissibility of electronic evidence thus:

> Finally, while we agree that for the purpose of sections 96 (1) (h) and 37 of the Act, 'banker's books' and 'books of account' could include 'ledger cards', it would have been much better, particularly with respect to a statement of account contained in a document produced by computer, if the position is clarified beyond doubt by legislation as has been done in England in the Civil Evidence Act 1968. Section 5 subsections (1) and (2) of that Act provide that in any civil proceedings, a statement contained in any document produced by a computer would, subject to the rules of the court, be admissible as evidence of any fact stated therein of which direct oral evidence would be admissible, if it is shown that certain conditions are satisfied in relation to the statement and computer in question:
>
> - That the document containing the statement are produced by the computer during a period over which the computer was used regularly to store or process information for the purpose of any activities to store or process information regularly carried on over that period, whether for profit or not, by any body, whether corporate or not, or by an individual;
> - 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 the kind from which the information so contained is derived;
> - That throughout the material part of that period the computer was operating properly, if not, that any respect in which it was not operating or was out of operation during that part of that period was not such as to effect the production of the documents or the accuracy of its contents; and
> - That the information contained in the statement reproduces or derived from information supplied to the computer in the ordinary course of those activities.

However, in *Anyaebosi v. R.T.Briscoe (Nig) Ltd(*1978), the Supreme Court per Uwais JSC (as he then was) held that computer printout is admissible as secondary evidence if the conditions in section 97 subsections (1) and (2) of the Evidence Act are satisfied. Similarly, in *F.R.N v. Fani*-Kayode (2010) , the Court of Appeal followed *Yesufu v. ACB* and *Anyaebosi v. R.T.Briscoe* (1978) and held that the computer printout of a bank statement was admissible under section 97 (1) and (2).

4. Admissibility of electronic evidence in legal proceedings in Nigeria

a. E-mails;

E-mail 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. It is a form of communication that is set down in writing. It is not oral. It can be downloaded and as real as a hard copy of a letter or mail (*Continental Sales Ltd v. R. Shipping* 2013).

The process of sending an e-mail operates in the same way as the traditional postal system. When an e-mail is sent from a computer, it passes on to a number of Message or Mail Transfer Agents (MTA). An MTA otherwise known 'mail relay' is "software that transfer electronic mail messages from one computer to another using client-server application architecture". (Wikipedia 2019) It "implements both the client (sending) and server (receiving) portions of the Simple Mail Transfer Protocol" (Wikipedia 2019).

E-mails are generated by computers and as such, the conditions for reception of other computer generated evidence also apply to admissibility of e-mails. The Court of Appeal in the case of *Continental Sales Ltd v. R. Shipping Inc*., (2013) when faced with determining whether e-mail was a permissive means of communication as envisioned under section 76 (3) of the English Arbitration Act, 1996 that stipulated that a notice or other document may be served on a person "by any effective means", held amongst others that e-mail is a form of communication that is set down in writing and the fact that it is electronic is immaterial, adding that, it can be downloaded and it is as real as a hard copy of the letter or mail.

In proving an e-mail in an evidence, section 153 (2) of the Evidence Act, 2011 comes handy. It 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. Therefore, in order to render a printout of e-mail admissible, conditions stipulated in section 84 (2) and (4) must be fulfilled-.i.e.-a)relevance b) authentication or identification of the e-mail, c) integrity of the e-mail, d) reliability of the computer that produced it and e) production of certificate of authentication.

A witness who desires to tender an e-mail message must proceed on the basis that such evidence is relevant to the issue under inquiry. According to Phipson (2007), it is "correct …in deciding whether evidence of a fact is admissible, to ask first whether the fact is relevant…" 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 e-mails (Collin Tapper 2010).

Electronic evidence generally must be authenticated or identified before it may be admitted. Authentication simply means a process of verification or identification that establishes that the particular document is what is purported to be. There are many ways by which an e-mail may be authenticated. They include facts relating to the features the e-mail bears. These include amongst others, the date of the transmission of the e-mail, e-mail address of the sender and the recipients, user name, nickname, screen name, web name, the subject of the mail Collin Tapper 2010).

In the United States, e-mails have been held to be admissible business records when they are timely recorded, regular activities, they memorialize events and conditions and they have no indicia of untrustworthiness (L.L.C v. Dell 2009).

E-mails are also subject to the authentication required of electronic evidence before admissibility. On the whole, the guidelines for authentication of e-mails are as follows:

- That a witness or entity received the email;
- That the e-mail bore the customary information in the e-mail;
- That the address of the recipient was consistent with the e-mail address on other mails sent by the same sender;
- That the e-mail contained electronic signature of the sender;
- That the e-mail contained matters known only to the alleged sender;
- That the e-mail was in fact sent as a reply to the sender; and
- That following the receipt of the e-mail, the recipient communicated with the alleged sender and the conversation reflected the sender's knowledge of the contents of the e-mail (United States v. Safavian 2012).

b. 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 (Online Business Dictionary 2019).

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 weakness inherent in the IT systems of the bank to perpetrate the fraud. He attributes no negligence to himself. The onus thereafter shifts to the bank. How is this onus to be discharged? (Evidence Act 2011). The bank must produce evidence that the payment transaction was authenticated. i.e. the bank must demonstrate –a)-the method it uses to verify the use of the debit card and ATM or online banking account, and b)-how all of the personalized security features (PIN, password) work; c)- that the transaction was accurately recorded and entered in the payment service provider's accounts; d)- that the transaction was not affected by a technical breakdown or some other deficiency; e)-the bank must prove that the

payment transaction was authorized by the payer; f)-evidence must be produced that the customer's card was inserted into the machine and the customer's PIN was keyed in; g)- that the customer or a person authorized by the customer was responsible for carrying out the transaction (Evidence Act 2011). Thus, in the Nigerian case of Geoffrey Amana v. United Bank for Africa (UBA) PLC (2011),-Court held that based on the circumstance of the facts and evidence in the case, the withdrawal of the sum of #149,000.00 from the account of the claimant was unauthorized, and the bank, who has the duty of care to ensure that the funds of the customer in its custody are safe, and should only be withdrawn upon due authorization by the customer. The bank had failed in the discharge of its duty of care towards the claimant and was therefore liable in negligence. Also, of importance, is the case of Benjamin Agi v. Access Bank PLC (2014) the case was dismissed as the claimant/appellant failed to prove that the respondent was negligent in failing to safeguard his funds and allowed unauthorized withdrawal of the appellant's money with an ATM debit other than the one issued to the appellant by the respondent bank.

5. Proof of Conditions for admissibility of computer generated evidence under section 84 of the Evidence Act of 2011

Electronic evidence are *sui generis*. Therefore, in determining the admissibility of electronic evidence, the court has to look beyond the conditions for admissibility of evidence in civil and criminal trials stated above. Hence, the court must resort to the provisions of section 84 of the Act. In effect therefore, admissibility of a computer generated document or document downloaded from the internet is governed by the provisions of section 84 of the Evidence Act, 2011. Basically, section 84 of the Evidence Act makes elaborate provisions for the admissibility of electronically generated evidence. It provides as follows:

"84 (1) In any proceedings a statement contained in a document produced by a computer shall be admissible in 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) are satisfied in relation to the statement and computer in question

(2) the conditions referred to in subsection (1) 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 purpose of any activities regularly carried on over that period, whether for profit or not, by anybody, whether corporate or not, or by any individual;

(b) that over that period there was regularly supplied to the computer in the ordinary course of those activities information of the kind contained in the statement or of the kind from which the computer was operating properly or, if not, that in any respect in which it was not operating properly or was not of operation during that part of that period was not such as to affect the production of the document

Or

the accuracy of its content; and

(3) where over a period the function of storing or processing information for the purposes of any activities regularly carried out 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 matter involving the successive operation over that period, in whatever order , of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer shall be construed.

Accordingly, it is provided that:

(4) in any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say:

(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;

(c) 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 in 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."

Arising from the above, the four (4) conditions for admissibility of a computer generated evidence under section 84 (2) are as follows:

- That the statement sought to be tendered was produced by the computer during a period when it was in regular use;
- That during that period of regular use, information of the kind contained in the document or statement was supplied to the computer;
- That the computer was operating properly during that period of regular use, and
- That the information contained in the statement was supplied to the computer in the ordinary course of its normal use (Litigation Newsletter 2015).

Furthermore, section 84 (4) requires that the party who seeks to tender a computer generated statement or document shall file a certificate:

- Identifying the document or statement;
- Describing the manner of its production;
- Stating the particulars of the device used in the production of the document, and
- The certificate shall 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.

Section 84 (4) is the authentication certificate. Authentication certificate is a requirement of the law relating to the admissibility of electronic evidence aimed at ensuring authenticity of a piece of electronic evidence before admissibility. Thus, any piece of electronic evidence that does not comply with this legal requirement is not admissible in evidence (Omisore v. Aregbesola 2015).

The provision was lifted from paragraph 8 of Schedule 3 to the English Police and Criminal Evidence Act, 1984. This is indeed a very liberal provision to dispense with the viva voce evidence of the witness who seeks to establish the foundation required under 84 (2) of the Act. From the operation of the sister provision under the English Act, it was discovered that the certificate envisaged under this provision need not be signed by an expert. From the lead judgment of Lord Griffiths, the person need not be an expert to give the required evidence. His Lordship stated as follows:

> …proof that the computer is reliable can be provided in two ways either by calling oral evidence or by tendering a written certificate in accordance with paragraphs 8 of Schedule 3, subject to the power of the judge to require oral evidence.

The conditions stipulated under section 84 of the Evidence Act regarding the admissibility of electronic evidence are mandatory. Therefore, where they are not properly laid before the court, such evidence will be rejected. Thus in the case of Akeredolu & Anor v. Mimiko & ORS (2013), he Court of Appeal held as follows:

> 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.

In order to lay proper foundation in respect of electronically generated evidence under section 84 of the Evidence Act, 2011, there must be proper foundation laid. Establish its relevance to the case under inquiry (the main object here is to authenticate it and establish the reliability of the computer that produced it).

However, under the Nigerian law, there are basically four evidence standards electronic document must satisfy to be admissible in evidence: -

- the document must be pleaded-this is not applicable to criminal cases-see Ohochukwu v. AG, Rivers State (2012)
- the document must be relevant to the fact in issue, -see section 1 of the Evidence Act; and Haruna v. AG, Federation (2012)
- the document must be admissible in law; the document is to satisfy the conditions enumerated under section 83 of the Evidence Act, 2011
- the document must satisfy the requirements of authentication (section 84 Evidence Act, 2011). Authentication means satisfying the court thus:
- that the contents of the record have remained unchanged;
- that the information in the record does in fact originate from its purported source, whether human or machine; and
- that extraneous information such as the apparent date of the record is accurate.

6. Evaluation and ascription of probative value to Electronic Evidence

In the case of Adesina v. Ojo (2012), it was held that to admit a piece of evidence is one thing, and to estimate the weight to be attached to it is another. Thus, a piece of electronic evidence may be admissible in evidence but when put in the crucible of evaluation and ascription of probative value may be found to be worthless.

Therefore, in estimating weight to be attached to a statement produced by a computer, there are certain guidelines laid down by the law to be followed. To this effect, section 34 (1) (b) provide as follows:

> 34. (1) In estimating the weight, if any, to be attached to a statement rendered admissible as evidence by this Act, regard shall be to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement, and in particular-
>
> (i) the question whether or not the information which the statement contained, reproduces or is derived from, was supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information, and
>
> (ii) the question whether or not any person concerned with the supply of information to that computer or with the operation of that computer or any equipment by means of which the document containing the statement was produced by it, had any incentive to conceal or misrepresent facts.

Simply put, section 34 provides that in estimating the weight to be attached to electronic evidence, the court has to consider whether the information contained in the statement in question was supplied contemporaneously to the fact in issue and whether the person to whom such information was supplied has incentive to conceal or misrepresent facts (Momodu 2016). Furthermore, in estimating the weight to be attached to electronic evidence, the manner in which it was obtained is of utmost important. Thus, by section 14 of the Evidence Act, the court has discretion to exclude improperly obtained evidence. However, section 15 of the Evidence Act (2011) provides some matters court must take into account under section 14 thus:

> 15. For the purposes of section 14, the matters that the court shall take into account include-
>
> * The probative value of the evidence;
> * The importance of the evidence in the proceeding;
> * The nature of the relevant offence, cause of action or defence and the nature of the subject matter of the proceeding;
> * The gravity of the impropriety or contravention;
> * Whether the impropriety or contravention was deliberate or reckless;
> * Whether any other proceeding (whether or not in the court) has been or is likely to be taken in relation to the impropriety or contravention; and
> * The difficulty, if any, of obtaining the evidence without impropriety or contravention of law.

It should be noted that section 84 of the Evidence Act, 2011 is taken after section 65B of the Indian Evidence Act of 1872 which was a substantial reproduction of section 69 of the English Police and Criminal Evidence Act of 1984. In summary therefore section 84 of the Evidence Act 2011 deals with the admissibility of statements in documents produced by computers. While subsection (2) sets out the conditions that are to be satisfied in relation to the statement and computer in question, subsection (4) makes provision for a certificate of authentication.

Section 84 of the Evidence Act stipulates the requirements for admissibility of electronic evidence in Nigeria: oral testimony and tendering of certificate of authentication which are mandatory. However, there are emerging issues that are yet to be judicially and clearly settled. Some of the issues are:

- The section assumes that evidentiary document must still be printed. It ignores expanded definition of ‘document’ in section 285, E/A
- What is certificate within the context of section 84 (4) of the Act?
- Is it only experts that are qualified to sign authentication certificate?
- It is the requirement of section 84 (4) that the authentication certificate 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. What happens where the evidence sought to be authenticated is to be tendered against the interest of the person or company in charge of the computer?
- Who satisfies the conditions stipulated in section 84 of the Act?-Network administrator, IT Manager, Supervising Officer; Data Processor; HOD or just any designated officer within an organization?
- Therefore, rigid application of certification will occasion injustice and ignore modern development in technology as noted in Esso West Africa v. Oyagbola (1969) -the law cannot be and is not ignorant of business methods and must not shot its eyes to the mysteries of the computer.
- What is the procedure to be adopted when the electronic evidence to be tendered is produced by the adverse party’s computer and he is not willing to issue a certificate of authentication of his computer?
- What if the computer, which was utilized in producing the document, was not secured and has been manipulated and has its content undermined by a virus?

In Dr. Imoro Kubor v. Hon. Seriake Dickson (2014), the Supreme Court examined the provisions of sections 84, 34 (1) (b) and 258 of the Evidence Act, (2011) in respect of the concept of document and the admissibility of electronic evidence.

Facts of the case

The case was an election petition matter. The appellants challenged the election and return of the first respondents as the Governor of Bayelsa State during the February 11, 2012 governorship election. One of the documents tendered by the appellants was a computer printout of the online version of the Punch Newspaper and other document from the website of the Independent National Electoral Commission (INEC), being the 3rd, while the electronic version of The Punch Newspaper was admitted and marked Exhibit "D", the document from INEC ''s website was admitted and marked Exhibit "L". However, the appellants did not satisfy the conditions laid down in section 82 (2) of the Evidence Act, 2011 in respect of the admissibility of the electronic evidence.

The matter went on appeal based on the lack of satisfying the conditions laid down under section 84 (2) of the Evidence Act where the Supreme Court decided thus:

> 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 admissions 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 computer generated documents 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.'
>
> I agree entirely with the above conclusion. Since the appellants never fulfilled the pre-conditions laid down by law, Exhibits "D" and "L" were inadmissible as computer generated evidence.

Justice Ogunbiyi, JSC (as he then was) reasoned further that the electronically generated documents were in the nature of secondary evidence and that both documents being public documents needed to have been certified before being tendered in evidence.

This case is the locus classicus on the point for now but it presents fresh dilemma as it ignores role of technology and impact of e-governance, e.g. INEC website. It further implies that electronic alerts and e-mails of bank transactions have no value without certification.

It is important to note that Kubor's case has set a standard reference of compliance for admissibility of computer generated evidence under the Evidence Act. It is mandatory to fulfill all the conditions in section 84. It also seems clear, from the above decision that fulfillment of the conditions is cumulative. However, the question to be asked is, does the mere satisfaction of section 84 of the Evidence Act automatically entitle the document to be ascribed weight by the court? The answer lies with the hurdles posed by section 34 (1) (b) of the Evidence Act that has to be passed. The section provides thus:

(a) The question whether or not the information which the statement contained, reproduced or is derived from, was supplied to it, contemporaneously with the occurrence or existence of the facts dealt with in that information; and

(b) The question whether or not any person concerned with the supply of information to that computer or any equipment by means of which the document containing the statement was produced, had any incentive to conceal or represent the fact. Failure to comply with these conditions would result in the evidence being expunged.

One thing is clear. The above decision underscores two vital points: a. it recognizes and endorses the use of electronic evidence in Nigeria; b- it reiterates the conditions for the admissibility of electronic evidence. Section 84 (1) of the Act is to the effect that in any proceedings, 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 section 84 (2) of the Act are satisfied.

7. Admissibility of electronic evidence in Nigeria: Challenges in determining the probative value of electronic evidence

a. Electronic evidence and hearsay rule

It is interesting to note that unlike the position under the repealed Evidence Act wherein the exclusion of hearsay evidence in judicial proceeding was not explicitly stated, but rather inferred from the combined provisions of sections 77 and 79 of the Act, section 38 of the Evidence Act, 2011, explicitly codifies the general rule of exclusion of hearsay evidence in all judicial proceedings to which the Act applies. Thus, by virtue of section 38 of the Evidence Act, "hearsay evidence is not admissible except as provided in this Part or by or under any other provision of this or any Act". It is clear from a literal interpretation of this provision that the admissibility of hearsay evidence is permissible either under the Act itself or by virtue of the provisions of any other Act of the National Assembly. Thus, the statement of exclusion of hearsay evidence under section 38 of the Evidence Act,

2011 is subject to exceptions provided in the Act or any other Act of the National Assembly.

Electronic evidence is viewed as specie of documentary evidence and as such the rule against admissibility of hearsay evidence applies to electronic generated evidence. Thus, direct electronic generated evidence must be given by the maker. If it is a record compiled and fed into a computer, the person who computed the record is the maker for the purposes of tendering and admissibility of the document. Computer generated evidence is therefore said to be hearsay evidence where:

> The document or the printout sought to be tendered is not what the computer stored and processed itself in an automatic manner or produced at the trial by the maker and the veracity of such a document is in issue (Chijioke 2017)

b. Electronic Documents-Exceptions to Hearsay Rule

Section 41 of the Evidence Act provides for an exception to the hearsay rule that relates to electronic evidence when it is a statement made in the ordinary course of business. It provides as follows:

> 41. A statement is admissible when made by a person in the ordinary course of business, and in particular when it consists of any entry or memorandum made by him in books, electronic device kept in the ordinary course of business, or in the discharge of a professional duty, or of an acknowledgement written or signed by him of the receipt of money, goods, securities or property of any kind, or of the date of a letter or other documents usually dated, written or signed by him.
>
> Provided that the maker made the statement contemporaneously with the transaction recorded or so soon thereafter that the court considers it likely that the transaction was at the time, still fresh in his memory.

Also, under the business record exceptions to hearsay rule, section 51 of the Act provides that the electronic records regularly kept in the course of business are admissible whenever they refer to a matter before the court, but such statements alone shall not be sufficient evidence to charge any person with liability. Equally, section 52 of the Evidence Act makes electronic records made by public servants admissible if made in performance of their duties.

c. Susceptibility to alteration/electronic documents can be manipulated

This is another challenge to the probative value of electronic evidence in Nigeria. Such questions as; will the court accord an original e-mail the same probative value as a forwarded copy of that e-mail?, will the court accord the PDF copy of a document the same probative value as a non protected word version of the said document? According to Usoro (2016), the courts will be very cautious in attaching weight to the forwarded e-mail or a non-protected word version of a document even it complies with section 84 of the Evidence Act and admitted in evidence because such documents are susceptible to editing and may be different in content from the original versions.

A computerized document that is sought to be tendered in evidence must necessarily undergo judicial scrutiny under section 84 (2). This is due to the fact that electronic records are very easy to tamper with. They are generally very vulnerable to manipulation. Hence, Justice Tobi, J.S.C in the case of Araka v. Egbue (2003) alluded to this in respect of admissibility of secondary evidence under section 97 (2) of the old Evidence Act (2004) when he held as follows:

> 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.

What Tobi, JSC, refers to as 'photo-trick' can, in modern parlance, take the form of 'enhancement', super-imposition, modification, excision or alteration (Ajileye 2016) In the same vein, Onyemenam, JCA, in Ekiti State Independent Electoral Commission & ORS v. PDP & Anor (2013) stated that:

> With our modern 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.

We can 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. The nefarious activities of hackers have also become notorious. The relative success of such hackers in intruding into the operations 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.

However, the provisions of the Cybercrime Act have given a clue to the above scenarios thus:

> A person who, with intent and without lawful authority, directly or indirectly

> modifies or causes modification of any data held in any computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than N7,000,000.00 or both.

8. Electronic Printouts: whether primary or secondary evidence

Section 2 of the Evidence Act (2011) defines a document as follows:

> Documents include books, maps, plans, drawings, photographs and also include matter expressed or describe upon any substances by means of letter, figures or marks or by more than one of these means, included to be used or which may be used for the purpose of recording the matter.

The Act suggests that the categories of documents are not restricted to those specified under the provision of section 5 of the Act which therefore suggests that nothing in this Act shall:

a) Prejudice the admissibility of any evidence which would apart from the provision of this Act is admissible.

Primary evidence connotes the original document while secondary evidence includes any evidence other than the original document. The general position of the law is that contents of documents may be proved by primary or secondary evidence. By section 88 of the Evidence Act (2011), the main rule remains that documents shall be proved by primary evidence. Primary evidence means the document itself produced for the inspection of the court. However, given the expanded meaning of 'document' under section 86 of the Evidence Act (2011) , the following are documents and can be produced in court as originals: disc, tape, sound track or any device in which sounds or other data (not being visual images) are held and from which data may be reproduced. By section 86 (4) (Evidence Act 2011) where a set of documents are made by a uniform process, all are regarded as originals.

9. International Best Practice

In the United States, the discovery of Electronically Stored Information (ESI) is specifically provided for in the United States Federal Rules of Civil Procedure. It provides for in r 34 (a) that a party may request the production of any designated electronically stored information stored in any medium from which information can be obtained either directly or after it has been translated into a reasonably usable form by the responding party.

Rule 34 (a) (1) (A) of the rules provide:

(a) In general, a party may serve on any other party a request within the scope of rule 26 (b)-
  (1) To produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control
    (A) Any designated documents or electronically stored information-including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations-stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form.

Also, in the United States of America, the case of Lorraine v. Markel American Insurance Company (1976) provided five evidence standards electronically stored information must satisfy before they are admitted in evidence. These are:

- Is the information relevant?
- Is it authentic?
- Is it hearsay?
- Is it original or, if it is a duplicate, is there admissible secondary evidence to support it?; and
- Does its probative value survive the test of unfair prejudice?

10. Conclusion

There is no doubt that the Evidence Act, 2011 has fully recognized the admissibility of electronic and computer generated evidence**.** Thus, Nigeria has moved close to global best practice. The new Act no doubt partly resolves reliability and admissibility of computer records, reliability and admissibility of forensically analyzed and located data (Owasanoye 2015). However, this paper has raised some issues which need more responses to ensure smooth practice of the new regime. Accordingly, reliance must be placed on persuasive decisions from other jurisdictions to make the Nigerian law of evidence to grow as the admissibility in evidence and computer generated evidence is yet to be fully mastered in Nigeria.

References

Aguda, A, *The Law of Evidence in Nigeria* (1974), p. 11

Ajileye, A.O., "Admissibility of Electronic Evidence in Civil and Criminal Proceedings", being a paper delivered at the Refresher course for Judicial Officers by the National Judicial Institute (NJI) from 14th-18th March

2016
Akhihiero, P.A. "Admissibility of Electronic Evidence in Criminal Trials, How Practicable"? Being a paper presented at the 2013 Annual General Meeting of the Magistrates Association of Nigeria, Edo State, from 23rd of July, 2013
Charles C.A, "An Examination of the Concept of Electronic Funds Transfer System in Electronic Banking and the Law"
Chijioke, C.O., "Admissibility of Electronic Generated Evidence in Nigeria: Issues and Responses", in *International Journal of Advanced Scientific Research*, Vol. 1, 2017, pp. 77-78
Evidence-Legal definition of evidence, available at http://legal-dictionary.thefreedictionary.com/evidence, accessed on 1 April 2019
Evidence Act, Cap. E14, Laws of the Federation of Nigeria, 2011
Muzaffar, S.A. "The Admissibility of Modern Electronically Evidence in Criminal Cases under Islamic Law" Public Lecture Series , delivered at Faculty of Sharia & Law, Slains Islam University, Malaysia (USIM) 2013
Meaning of E-mail on Wikipedia; also available at https://en.wikipedia.org/wiki/Message_transfer_agent accessed on 10 May 2019
Momodu, B, *Court-Room Rapid Reference Handbook, Vol. 4, Electronic Evidence* (Benin City: Momodu Law Publishing, 2016), p. 30
Umezulike, I.A.. "Recording of Evidence and Judgment Writing", in *Essays in Honour of Professor C.O.Okonkwo,* in Nwauche E.S, and Asogwa F.I., (eds) (PortHarcourt: Jite Books, 2000), p. 273
Online Business Dictionary, available at http://www.businessdictionary.com/definition/automated-teller-machine-ATM.html accessed on 13 May 2019
Owasanye, B, "Admissibility of Electronic Evidence in Nigeria", being a paper presented at the Ogun State Bar and Bench Forum, Abeokuta, 2015, p. 78
Ukpai M.C., and Oji, E.O., "Admissibility of Electronic Evidence Under the Nigerian Evidence Act, 2011", in *International Journal of Research* (IJR) Vol. 1, 2014
Tapper, C(2010) "Cross and Tapper o Evidence" (London: Oxford University Press, 2010) (12th ed), p. 64
Usoro, M.E., Commentary on the Paper, 'Electronic Evidence in Admiralty Practice', being a paper delivered at the 14th International Maritime Seminar for Judges, Sheraton, Abuja, from 31st May to 1st June 2016, p. 2
Adesina v. Ojo (2012) LPELR 15347
Amadi v. A-G, Rivers State (2012) 9 NWLR (pt. 1306) 419
Amitab Bagachi AIR 2005 Call II
Anyaebosi v. R.T.Brisco (1978) 3 NWLR (pt. 59) 84 at 96-97
Araka v. Egbue (2003) 7 SCNJ 114
Benjamin Abi v. Access Bank Plc (2014) 4 NWLR (pt. 1345) 534-594
C.D.C Nig. Ltd v. S.C.O.A Nig. Ltd (2007) 30 W.R.N 81
Continental Sales Ltd (2013)LPELR 20532 (CA)
Ekiti State Independent Electoral Commission v. P.D.P (2013) LPELR-2041 (CA)
Egbue v. Araka (1996) 2 NWLR (pt. 433) p. 688
ESSO W.A. v. Oyagbola (1969) 1 NMLR 194
F.R.N. v. Fani Kayode (2010) 14 NWLR (pt. 1214) 481
Haruna v. A.G. (2012) AII FWLR (pt. 630), p. 1377
Kubor v. Dickson (2013) 4 NWLR (pt. 1345) 534
.L.C. v. Dell Inc. , 621 F. Supp 2d 1173, 1186 CD Utah 2009
Loraine v. Markel (1976) SC 17; (AIR 1975 SC 1788
Maharashitra v. Praful AIR 2003 SC 2053
Ohochukwu (2012) 10 NWLR (pt. 1309) 552
Omisore v. Aregbesola (2015) 15 NWLR (pt. 1482) 205
Pius v. State (2012) LPELR 15347 (CA)
Raimi v. Akintoye (1986) 3 NWLR (pt. 26), 27
Yesufu v. African Continental Bank Ltd (1976) AIINLR 264 at 273-274
Sales Ltd v. R. Shipping Inc (2013) 4 NWLR (pt.) 67
United States v. Safavian 4351, Supp. 2d 36 at 40;