

***ADMISSIBILITY OF ELECTRONIC EVIDENCE IN
CRIMINAL TRIALS. HOW PRACTICABLE?***

A PAPER PRESENTED BY

HON. JUSTICE P.A. AKHIHIERO

LL.B (Hons) Ife; LL.M. Lagos; B.L.

EDO STATE CUSTOMARY COURT OF APPEAL

***AT THE 2013 ANNUAL GENERAL MEETING
OF THE MAGISTRATES ASSOCIATION***

OF NIGERIA,

EDO STATE BRANCH

HELD ON

TUESDAY, 23RD OF JULY, 2013.

1. INTRODUCTION

The *Microsoft Encarta Dictionary, 2008 Edition* defines “evidence” as “something that gives a sign or proof of the existence or truth of something, or that helps somebody to come to a particular conclusion.”

Sir Rupert Cross explains that “the evidence of a fact is that which tends to prove it – something which may satisfy an inquirer of the fact’s existence. Courts of law usually have to find that certain facts exist before pronouncing on the rights, duties and liabilities of the parties, and such evidence as they will receive in furtherance of this task is described as “judicial evidence.”¹

Simply put, evidence is the means by which facts are proved.

The main source of our law of evidence in Nigeria is the Evidence Act of 2011 which applies to judicial proceedings in most courts in all the states of the Federation²

The Evidence Act classifies judicial evidence into three main categories: **oral evidence, real evidence and documentary evidence**. Oral evidence and real evidence are covered under Part VII of the Act, while documentary evidence falls under Part V. One other category of evidence which is not directly captured by the Act is what is referred to as **circumstantial evidence**. This is evidence offered to the court for the purpose of the court inferring there from, the existence of a fact in

¹ Cross on Evidence, 5th Edition, London Butterworths, 1979.

² See section 256, Evidence Act, 2011

issue.³ It is generally in the form of oral evidence. It is usually contrasted with “direct evidence” which is evidence offered by a witness in proof of the truth of the fact asserted by him.⁴

Essentially, this paper will focus on the aspect of documentary evidence, with particular emphasis on the admissibility of electronic evidence in criminal proceedings. We will examine the salient provisions of the Evidence Act in this regard.

The advent of information technology has introduced humanity into an era of hi-tech communication on the digital platform. We are now in the age of swift transfer of information, borderless transactions, electronic transactions (**e-transactions**), it is the age of unparalleled knowledge, mind boggling discoveries, the age of the internet with vast and awesome possibilities. The automation has radically altered the landscape of human activities. These digital developments have also re-defined the pattern of legal proceedings in courts of law across the globe. This is not unexpected. It is imperative that the law must keep pace with modern developments.

According to the **sociological school of jurisprudence**, the law should be an instrument of social engineering.⁵

³ T. Akinola Aguda: Law and Practice Relating To Evidence In Nigeria, 2nd Edition, MIJ Publishers, 1998.

⁴ Section 126 Evidence Act.

⁵ Roscoe Pound: Social Control Through Law, Transaction Publishers, 1942.

The enactment of the Evidence Act 2011 marks a watershed in the evolution of our legal system. One major area where the current Act has introduced radical changes is in relation to computer and electronically generated evidence. This aspect of our law has been in dire need of reform.

In the old case of *Esso West Africa Inc. v T. Oyegbola*⁶, the court observed that “*The law cannot be and is not ignorant of modern business methods and must not shut its eyes to the mysteries of the computer.*”

Also in the case of *Egbue v Araka*,⁷ Pats-Acholonu, JCA lamented that “*-----our Evidence Act is now more than 50 years old and is completely out of touch and out of tune with the realities of the present scientific and technological achievements. Most of its sections are archaic and anachronistic and need thorough overhaul to meet the needs of our times. But alas it is with us now like an albatross on our neck - - - -*”

In this presentation, the nature and the sources of electronic evidence will be examined. Furthermore, attention will be focused on the provisions of the Act governing the admissibility of electronic evidence particularly in criminal trials.

Next, I will embark on a consideration of some aspects of the Act which may require further legislative reforms. I will round up the presentation with an overview of our response to these new initiatives and articulate my views on the way forward.

⁶ (1969) 1 N.M.L.R. 194 at 198

⁷ (1996) 2 NWLR (Pt. 433) 688 at 710 - 711

2. NATURE AND SOURCES OF ELECTRONIC EVIDENCE

Electronic evidence and computer forensics are relatively recent additions to the means of proof in legal proceedings. Unlike many other forensic disciplines that were introduced into the trial process with little or no legal debate, electronic evidence has sparked considerable and often controversial debates among legal professionals. According to Stephen Mason,⁸ different legal systems reacted in different ways to this new challenge. Some felt the need to introduce new legislation specific to digital evidence.

Others tried to establish a ‘closest match’ to existing evidentiary concepts and applied the rules by analogy. In some jurisdictions, both strategies were applied. Whatever the approach, it is expedient to identify the nature and sources of this type of evidence.

This type of evidence has been variously described as ‘*electronic evidence*,’ ‘*digital evidence*’ or ‘*computer evidence*’. All these terms are interchangeable. The adjectives used may shed some light on the nature of the evidence in question. The word ‘**electronic**’ has been described as “*relating to, using, or accessed through a computer or computer network*”⁹ Also ‘**digital**’ is defined as “*processing, storing, transmitting, representing or displaying data in the form of numerical digits, as in a digital computer*”¹⁰ Of course, the same **Microsoft Encarta Dictionary** defines a ‘computer’ as “*an electronic device that accepts,*

⁸ Mason: *Electronic Evidence*, 2nd Edition, Lexis Nexis, Butterworths, 2010, p. 21.

⁹ Microsoft Encarta Dictionary supra

¹⁰ See Microsoft Encarta supra

processes, stores and output data at high speed according to programmed instructions". From the above definitions, it can be seen that all the alternative adjectives are quite interwoven.

The learned author, Stephen Mason proffered an all embracing definition of electronic evidence to cover both civil and criminal proceedings. According to him, it can be defined as "*Data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.*"¹¹

This definition of Mason has three identifiable elements that highlight the nature of electronic evidence.

In the first place, it covers all forms of evidence that are created, manipulated or stored in a device that can be classified as a computer. Secondly, it aims to include the various forms of devices by which data can be stored or transmitted. This aspect is wide enough to include devices such as **mobile phones, digital cameras, video recorders, ATM machines, satellite devices, car tracking devices** etc, etc. The third element involves the process of adjudication in the court. This part of the definition relates to the aspect of relevance and admissibility of the evidence.

¹¹ Mason: Electronic Evidence supra p. 25

2.2. ELECTRONIC DOCUMENTS

An important form of evidence in legal proceedings is proof by documents. It is pertinent to note that as we progress in this digital dispensation, we are beginning to witness a paradigm shift in the nature of documents. We are fast moving from the traditional mode of **paper documents** to **documents in digital formats**. What is called **electronic documents**.

We must have a sound understanding of the nature of electronic documents in order to appreciate the legal provisions regulating their reception in evidence. Presently, a single document can be in **soft copy** (digital format) and **hard copy** (analogue format). This is not really a case of original copy and duplicate copy, or a question of primary evidence and secondary evidence. Rather it is more or less a case of the two sides of the same coin. This is the dynamics of the present dispensation.

The Evidence Act of 2011 has taken cognisance of this radical change in its definition of a “document” under section 258(1) thereof. It is defined to include:

“(a) books, maps, plans, graphs, drawings, photographs and also includes any matter expressed or described upon any substance by means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter;

- (b) *any disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it; and*
- (c) *any film, negative, tape or other device in which one or more visual images are embodied so as to be capable (with or without the aid of some other equipment) of being reproduced from it.*
- (d) *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 above definition is a significant improvement on the definition of the word ***document*** under section 2, of the previous Evidence Act which simply stated that it “*includes books, maps, plans, drawings, photographs and also includes any matter expressed or described upon any substance by means of letters, figures or marks by more than one of these means, intended to be used or which may be used for the purpose of recording that matter.*”

It is evident that this definition was restricted to documents in the physical format. It did not cover documents in the digital format.

The new definition has sufficiently bridged the gap between the digital world (which appears so unfamiliar to the uninitiated) and the physical world (with all the familiar trappings of paper documentation). The present legislation has introduced the legal profession to the reality of the current regime of electronic data management. We must come to terms with the concept of documents in electronic format that is made visible to the human eye on a screen or a print out. What was previously filed in physical form is now filed in digital form accessible only electronically, unless they are printed out.

2.3. SOURCES OF ELECTRONIC EVIDENCE

The point must be made that there are different techniques that are capable of creating evidence in digital format. We will succinctly identify some of these sources to enable us appreciate more, the nature of this form of evidence, before we consider the legal machinery for its admissibility.

Generally speaking, the computer can be regarded as the primary source of electronic evidence, For the purpose of this write up, the term ‘**computer**’ is used in the generic sense to encompass any *electronic device that accepts, processes, stores and outputs data at high speeds according to programmed instructions.*¹² In this sense, the term includes a range of gadgets such as mobile phones, various forms of personal digital assistant (PDA), cameras, music players, calculators, meters, ATM machines, traffic lights, car tracking devices etc, etc. All these devices are computers in their own right in as much as they have a CPU, memory,

¹² See Microsoft Encarta Dictionary supra

input and output devices, screen and they are loaded with operating software. These devices are increasingly being used by individuals and organisations 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.

Sometimes these computer devices operate to generate electronic evidence on standalone basis. For example, a single desktop computer in an office may generate such evidence without any connection to any other system.

At other times, more than one computer may operate together to generate the data. Such an arrangement is called a **network**. 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.

Another form of network is the **intranet**. This looks like a smaller version of the internet. It is a computer network within an organization. It normally utilises the World Wide Web conventions and is accessible only to authorised users within the organisation.

A recent development in the field of networking is the introduction of wireless networking. Wireless networking is also known as **Wi-Fi**, meaning wireless fidelity. This form of technology uses radio waves to transmit data.

Another wireless technology, known as **Bluetooth** actively connects devices within a short range, using another radio frequency band.

All these are some of the sources of electronic evidence. With modern technological developments the sources of such evidence are being proliferated by the day.

3.1. ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL TRIALS

In this segment, we will step out of the library and move into the court room. We want to examine the legal rules and procedures involved in the admissibility of electronic evidence in criminal trials. Here we are dealing with practical situations that may arise in court. This is the pith and substance of the presentation.

In Nigeria, the omnibus statute regulating the admissibility of evidence in criminal trials is the **Evidence Act, 2011**. This is unlike some foreign jurisdictions where they have separate legislations for civil and criminal proceedings. For example, in Britain, they have **Civil Evidence Act of 1995** to regulate civil proceedings and the **Police and Criminal Evidence Act of 1984** for criminal proceedings. In Ireland, they have the **Civil Law (Miscellaneous Provisions) Act, 2008** for civil matters and the **Criminal Evidence Act of 1992** to regulate Criminal Proceedings.

We shall consider the provisions of our Evidence Act regulating the admissibility of all forms of electronic evidence. We will make reference to

judicial pronouncements on relevant sections of our Act. Where we do not have local decisions on the point, we shall refer to the decisions of foreign courts on similar provisions.

3.2. RELEVANCY

It is an elementary principle of the law of evidence that before considering the admissibility of any piece of evidence, it must be shown to be relevant. Section 1 of the Evidence Act provides that “*1. Evidence may be given in any suit or proceedings of the existence or non-existence of every fact in issue and of such other facts as are hereafter declared to be relevant, and of no other*”

In the recent case of *Ogu v M.T. & M.C.S. Ltd*,¹³ the Court of Appeal maintained that “*the admissibility of evidence is governed by the provisions of section 6 of the Evidence Act (now section 1 of the 2011, Act). Once a piece of evidence is relevant, it is admissible in evidence irrespective of how it was obtained. In other words, admissibility of evidence is based on relevance. A fact in issue is admissible if it is relevant to the matter before the court. In that respect, relevancy is a precursor to admissibility.*”

The use of the phrase “-----in any suit or proceeding” in section 1 of the Act implies that the principle of relevancy is not restricted to civil proceedings. It also applies to criminal proceedings. The authorities on the point are legion. See the following: (i) **Samuel Thomas v C.O.P.**,¹⁴

¹³ (2011) 8 NWLR (Pt. 1249) 345

¹⁴ (1949) 12 WACA 490

(ii) **Akinmoju v The State**,¹⁵ **Emeka v The State**,¹⁶ and

(iii) **Nweke v The State**¹⁷

In essence, the starting point in the admissibility of any piece of electronic evidence is to first determine whether the evidence is relevant to the trial. If it is relevant then you proceed to the next stage.

3.3. ADMISSIBILITY

We must note that the parameters for the admissibility of evidence in civil proceedings are not the same as in criminal proceedings. In civil cases, the criteria for admissibility are: whether such evidence has been pleaded; whether it is relevant; and whether it is admissible in law.¹⁸ In criminal matters where pleadings are not exchanged, admissibility is governed, by relevance of such evidence and other strict rules of admissibility relating to a free and fair trial. In essence, the rules of admissibility are more stringent in criminal proceedings. Take for example, the requirement of voluntariness as a prerequisite for the admissibility of a confessional statement pursuant to sections 28 and 29 of the Act. Furthermore, a court in a 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.¹⁹

¹⁵ (2000) FWLR (Pt. 11) 1893

¹⁶ (1998) 7 NWLR (Pt. 559) 556

¹⁷ (2001) FWLR (Pt. 40) 1595

¹⁸ See: Okonji v Njokanma (1999) 12 SCNJ 259 at 273 – 275;and Danniya v Jomoh (1994) 3 NWLR (Pt.334)

609 at 617

¹⁹ See Raimi v Akintoye (1986) 3 NWLR (Pt.26 97; and Dagaci of Dere v Dagaci of Ebwa (2006) All FWLR (Pt. 306) 786.

Coming to the issue of the admissibility of electronic evidence, we must understand that electronic documents are **sui generis**. They are very unique documents in a class of their own. The admissibility of electronic evidence has always presented a very special challenge in the process of adjudication. There are several controversial areas that are quite uncertain and unsettled. We will examine some of these thorny areas.

3.4. DETERMINING THE RELEVANCE OF AN ELECTRONIC DOCUMENT

As we have observed, relevancy is the precursor to the admissibility of any piece of evidence. A preliminary problem is how to determine the relevance of electronic documentary evidence. How do you convince the court that a document that is yet to be downloaded from an electronic device is relevant to the proceedings when that document is not visible to the court? Some of these documents are captured in electronic devices such as a conventional PC, mobile devices, ATM machines, storage devices like CD-ROMS, DVD, Zip drives, USB, Flash drives, internet or intranet sources etc., etc.

In determining the relevance of such electronic evidence, it is necessary to first of all establish that the electronic document is what it purports to be and carries an accurate representation of the data or information which is relevant to the proceedings. This raises the salient question of the **authenticity of the evidence**. This means that the document needs to be **authenticated** by an extrinsic

source before it can be admissible. Now, the document cannot speak for itself. Consequently, the party seeking to rely on it must adduce evidence that confirms that the document is what it purports to be in terms of its source (origin) and its substance (what it represents). The issue of **authentication** is a matter of leading evidence to satisfy the requirements of the Act in this regard.

Basically, **section 84 of the Act** makes elaborate provisions for the admissibility of electronically generated evidence. The section provides as follows:

“84 (1). 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 subsection(2) of this section 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 that period was not such as to affect the production of the document

or

the accuracy of its contents; and

- (c) *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 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,

(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 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.”*

The sum total of the foregoing provisions is that it is *sine qua non* to lay down the evidential foundations of the electronic evidence before the evidence can be admissible in legal proceedings. Naturally, the nature of the evidence required to determine the authenticity of electronic evidence will differ from case to case. In the English criminal case of *R v. Shepherd*²⁰, Lord Griffiths observed 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 that 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”.

It is pertinent to observe at this stage that the remarks of Lord Griffiths in the above case involved the requirement to comply with **section 69 of the English Police and Criminal Evidence Act of 1984**. Incidentally, our own section 84 of our Act was lifted verbatim from section **65B of the Indian Evidence Act of 1872 (as amended in 2003)**, which was a substantial reproduction of section 69 of the English Police and Criminal Evidence Act of 1984.

The tests of authenticity of electronic evidence will also depend on the source and type of electronic data. Electronic data exist in a variety of formats.

²⁰ (1993) A.C. 380; (1993) 1 All E.R. 225

For example, there are applications such as word processing and databases. There are other applications that enable a user to obtain access to the internet and email. Also, there are other data emanating from mobile telephones, storage device and drives. There are large scale devices like mainframe computers which cannot be moved into any court hall. For such a device you must rely on output such as the print outs. Here you may require the evidence of the expert in charge of that mainframe device.

The salient consideration on the issue of the admissibility of electronic evidence therefore, is to determine whether a **proper foundation** has been laid to meet the requirements of section 84 of the Act. If a proper foundation is laid, the electronic evidence will be received in evidence. If the foundation is not laid, the evidence ought to be rejected.

Unfortunately, in view of the recent age of this Act, our superior courts are yet to make pronouncements on the application of the provisions of the Act. Presently, there is a dearth of cases on the point. In the course of my research, I came across only one case decided by the Supreme Court on the point. It is the case of **Dr. Imoro Kubor & Anor v Hon. Seriake Henry Dickson & Ors**²¹ In the said case, the appellants were challenging the election of the 1st respondent as the Governor of Bayelsa State in the February 11, 2012 governorship Election. At the Election Petition Tribunal, the learned counsel for the Petitioner/Appellant tendered from the Bar, a computer printout of the online version of the Punch

²¹ (2013) 4 NWLR (Pt.1345), 534

Newspaper and another print out from the website of the Independent National Electoral Commission. The counsel for the respondents did not object to the tendering of the two documents and they were admitted and marked as Exhibit “D” and “L” respectively.

On appeal the admissibility of the two exhibits was seriously challenged on two grounds. Firstly that they were public documents which ought to have been certified and secondly that the documents having been tendered from the bar, evidence were not adduced to meet the foundational conditions stipulated in section 84(2) of the Act. It was contended that the documents ought to be expunged from the records.

The Supreme Court agreed with these submissions and held *inter alia* as follows:

“Admissibility of a computer generated documents or document downloaded from the internet is governed by the provision of section 84 of the Evidence Act -----A party that seeks to tender in evidence a computer –generated document needs to do more than just tender same from the bar. Evidence in relation to the use of the computer must be called to establish the above conditions ----- Since the appellants never fulfilled the pre-conditions laid down by law, exhibits “D” and “L” were inadmissible as computer-generated evidence.”

This case appears to be the **locus classicus** on the admissibility of electronic evidence for now. The decision of the Supreme Court is in line with the decisions from other foreign jurisdictions. A consideration of some of such decisions will confirm this fact. In the English case of *R v Dean*²², it was argued on appeal that since there was no evidence that the naval computer databases in question were at the relevant time operating properly, the evidence on the searches on those bases generated from them was inadmissible under section 69 of the Police and Criminal Evidence Act, 1984. The Court of Appeal rejected this submission, holding that since there had been no known reported problems with the databases, an officer who had carried out the search was qualified to give evidence of the real ability or accuracy of the databases. Similarly, in *R. v Spiby*²³, 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. The argument that only an engineer who had been servicing the computer or another expert in the field was the competent person to give such evidence was rejected by the Court of Appeal.

The position is the same in the United States. In the case of *United States v Linn*²⁴, it was an appeal in a matter relating to the admissibility of computer printout of telephone call logs from a hotel telephone. The appellant contended that the witness who was the Director of Communications of the hotel was not an

²² (1998) 2 CAR 171

²³ (1991) CLR 199

²⁴ 880 F. 2d 209 (9th Cir. 1989)

expert witness. It was argued that under cross-examination, the witness could not explain the differences between computer menus, databases and codes. Rejecting this argument, the court held that by failing to raise any issue on the proper working of the computer but rather dwelling on the competence of the witness, the defence missed the opportunity of shifting the burden to the prosecution to prove that the computer was working properly.

From the line of authorities considered so far, it is evident that it is not only an expert that is qualified to adduce evidence to lay the foundation necessary for the admissibility of electronic evidence. While we commend the liberal approach of the courts, the point must be made that each case must be considered in the light of its peculiar circumstances. Situations may arise where only the evidence of an expert may suffice.

Authenticating electronic evidence is an exercise of the court's judgment and it involves a delicate act of *balancing the risks of acceptance against its benefits*²⁵

The principles are not so clear cut. This is period of gestation. Commenting on the obscurity and uncertainty in this regards, the **Queensland Law Reform Commission** observed thus:

*“With evidence produced by devices or systems,
however, the courts appear to have required
that the trial judge be satisfied*

*presumably, on the balance of probabilities
as to the accuracy of the technique and
of the particular application of it”²⁶*

The bottom line in the issue of authentication however is that the court must be satisfied that the evidence adduced is sufficient to lay the foundation as enshrined in section 84 of the Act. The rationale is to have some checks and balances in place to ascertain the history of how the data have been managed, which leads to the assertion that the data have not been modified, altered, replaced or corrupted and must therefore be genuine.

²⁵ Gregory, JD, “ Authentication Rules and Electronic Records”
Ontario, Canada, Canadian Bar Review, November, 2001.

²⁶ The Receipt of Evidence by Queensland Courts: Electronic
Records Issues Paper WP No. 52 Queensland LRC, August, 1998.

3.5 AUTHENTICATION CERTIFICATE

Section 84(4) of the Evidence Act provides 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 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”*

This provision was lifted verbatim from **paragraph 8 of Schedule 3 to the English Police and Criminal Evidence Act, 1984**. This is indeed a very liberal provision that appears 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 in the case of **RV Shepherd** (Supra), the person need not be an expert to give the required evidence. According to His Lordship, “...*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 para 8 of Sch. 3, subject to the power of the Judge to require oral evidence.*”²⁷

In my candid view, the courts should exercise some caution in the application of this provision on the use of a certificate of authentication. This liberal approach may be abused by unscrupulous parties. The provision is not stringent enough to prevent abuses. It is suggested that where the court is to rely on a mere certificate to lay foundation for the admissibility of electronic evidence, the certificate should be issued by an expert. This will be in tandem with the usual trend of such certificates under the Act. See for example the provision on the opinion of expert witnesses in **section 68 to 71 of the Act**.

The quality of the certificate issued pursuant to section 84(4) is further whittled down by the concluding phrase that “...*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*”. This will give room for all kinds of quacks and mediocres to issue certificates to the best of their knowledge and belief. The will be quite unfortunate.

CONCLUSION

We live in an electronic age where everyday transactions are conducted on the electronic platform. The digital technology has compressed the world into a **global village**. The masses have embraced information technology. The use of electronic devices like GSM mobile phones is no longer the preserve of the elites or the wealthy.

The illiterate rural farmer can now place order for fertilizer from his farm with the aid of his cell phone. The market women now transact their business on electronic platforms like ATMS and other **e-payment** arrangements.

The volume of electronic data is on the increase. Most of these transactions are captured by electronic devices. In the event of dispute, parties are bound to rely on electronic evidence. In essence, electronic evidence has come to stay.

In the course of this presentation we have come to appreciate the fact that the emergence of electronic evidence has presented new challenges. In the area of criminal law, there is an alarming increase in the wave of **cybercrimes**. The crimes range from **advance fee fraud, credit card frauds, online prostitution, illegal gambling, child pornography, blackmail, cyber stalking**, even culminating in murder as we can see in the recent case of **Cynthia Osokogu**. The young lady was raped and murdered by her **face book** friends.

In the light of these developments, the recent enactment of the 2011 Evidence Act to guarantee the admissibility of electronic evidence is a step in the

right direction. In the prosecution of many of these crimes electronic evidence will feature very prominently.

Take for example the **Cynthia Osokogu case** where a post graduate student residing in Nasarawa State was lured online *via* **face book** interactions to her untimely death in the hand of some hoodlums in Lagos. The trial of the suspects is bound to be a hi-tech trail where electronic evidence will be downloaded from the **face book website** to prove the premeditated actions of the suspects. One wonders how the trial would look like if the Evidence Act has not been updated.

It is in this vein that we must emphasize the need for **computer literacy** for all the members of the legal profession. It is quite unfortunate that in this dispensation we still have some lawyers and even judicial officers who cannot boot a computer. Some cannot even use their GSM to send text messages. They cannot send or receive e-mails. Some do not even have an e-mail address. They have a morbid fear of anything relating to the computer – **CYBERPHOBIA**. Since we are now talking about electronic evidence, we all must be computer literate. In a paper which I delivered in the law week of the Benin Branch of the NBA in 2009, I opined that *“Very soon, the concept of literacy will be redefined in consonance with the dictates of the digital age. The ability to read and write can no longer be the sine qua non for classifying a person as either literate or illiterate.*

Computer literacy will be the determining factor”²⁸.

Furthermore, there must be continuous IT training for all those involved in the administration of justice. This leads us to a more crucial aspect. Our courts need to be fully updated with IT facilities. The system should be upgraded to meet the current exigencies. The **court procedures should be fully automated** for optimum performance.

Courts should be equipped with **digital recording facilities** and should be **on line real time**. Otherwise, our manual system of operation may pose a threat to this new regime of electronic evidence.

Take for instance where the court needs to access a website to view a piece of electronic evidence?

Suppose the court is not internet ready, what happens? That becomes a clog in the wheel of justice. We must be prepared!

On the whole, we have examined the modalities for the admissibility of electronic evidence in criminal trials.

We have examined the legal framework introduced by the Evidence Act of 2011. All things considered, the provisions of section 84 are quite laudable. If the proper foundation is laid electronic evidence can be admitted in evidence in criminal trials. We have considered some authorities from some more advanced jurisdictions. The foreign decisions have shed some light on some grey areas.

It is left for us to take up the challenge. Even if we do not have the benefit of foreign decisions, we can **break new grounds**. There must be a starting point. I close with the immortal words of my mentor **Lord Denning (Master of the Rolls)**:

“What is the argument on the other side? Only this, that no case has been found in which it has been done before.

That argument does not appeal to me in the least. If we never do anything which has not been done before, we shall never get anywhere. The law will stand still whilst the rest of the world goes on: and that will be bad for both”²⁹.

Hon. Justice P.A. Akhiero
LL.B (Hons) Ife, LL.M. Lagos, BL
www.nigerianlawguru.com
peterakhiero@yahoo.co.uk