

EVALUATION OF ELECTRONICALLY GENERATED EVIDENCE:
PRACTICE AND PROCEDURE*

Samuel E. Idhiahri Esq.
Chief Magistrate, FCT Judiciary

(Being a paper delivered at an Orientation Course for newly Appointed Magistrates at
the National Judicial Institute, Abuja, on the 10th July, 2019)

A. INTRODUCTION

Evidence, in legal terms, mean any species of proof legally presented at the trial of an issue, by the act of the parties and through the medium of witnesses, records, documents, concrete objects and the like.¹ The primary classification of evidence is into oral, documentary and real evidence. Oral (or *viva voce*) evidence is the verbal testimony in court which is offered as evidence of the truth of that which is stated while documentary evidence is the statement made in a document which is offered to the court in proof of any fact in issue. On the other hand, ‘real evidence’ means material objects, other than documents, produced for the inspection of the court for it to draw conclusion with respect to some facts in issue.²

There are further sub-classifications of evidence into primary and secondary evidence, direct, circumstantial and hearsay evidence etc.; the important point to note is that the sub-classifications are clearly forms in which oral or documentary evidence may be rendered. However, in practice, some of these classifications of evidence overlap; thus, oral evidence may similarly be described as direct evidence, hearsay or circumstantial evidence just as a document may be used as real evidence, primary or secondary evidence.

Our paper is titled ‘Evaluation of Electronically Generated Evidence: Practice and Procedure’. To properly cover the subject-matter, the paper is

*A wider version of this paper which included ‘admissibility of electronically generated evidence’ has earlier been delivered at a Refresher Workshop for Magistrates at the National Judicial Institute, Abuja on the 18th April, 2018.

¹ *Halima Hassan Tukur v Garba Umar Uba & Ors.* (2013) 4 NWLR (Pt. 1343) 90 SC per Ariwoola JSC

² See generally, Samuel E. Idhiahri, *Practice Notes on Evaluation of Evidence* (Imhanobe Law Books Ltd, 2015) 3, 4

divided into two principal segments. The first segment, subtitled ‘Definition, Taxonomy and Scope of Electronically-Generated Evidence’ dwelt on contextual clarification of the subject-matter, appraised issues of classification and explored the scope of the genre of evidence often described as electronic. The second segment is a discussion on the rules and principles that the court may deploy in ascribing weight to electronically generated evidence. However, the connecting rod between the two segments is the question of admissibility of electronically generated evidence, for evidence has to be admitted before it can be evaluated for weight. Consequently, the provisions of the Evidence Act, 2011 on the circumstances and conditions to enable such electronically generated evidence to be admitted have also been identified in the paper.

B. DEFINITION, TAXONOMY AND SCOPE OF ELECTRONICALLY-GENERATED EVIDENCE

Electronically generated evidence, or in fact what is electronic, is nowhere defined in the Evidence Act 2011 even though the word electronic is used about ten times in the Evidence Act in contexts we shall presently explore. Similarly, while ‘computer generated evidence’ is not stated in the Evidence Act, a computer is stated in the Act to mean ‘any device for storing and processing information’.³

Electronically or computer generated evidence has been variously defined. Stephen Mason proffered an all-embracing definition of electronic evidence 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’.⁴ Using the alternative description of ‘digital evidence’, another writer put it as information of probative value that is stored or transmitted

³ s258 Evidence Act

⁴ Cited by Akhihero, P.A. ‘Admissibility of Electronic Evidence in Criminal Trials: How Practicable?’ (Being Paper delivered at a General Meeting of the Magistrates Association of Nigeria, Edo State Branch on 23rd of July, 2013.

in binary form.⁵ The word ‘digital’ is commonly used in computing and electronics, especially where physical-world information is converted to binary numeric form as in digital audio and digital photography.

Based on the above, evidence is not only limited to that found on the ubiquitous computers but may also extend to include evidence on digital devices such as telecommunications or electronic multimedia devices. The e-evidence can be found in e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programme, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel’s electronic door locks, Digital video or audio files. Digital Evidence tends to be more voluminous, more difficult to destroy but easily modified, easily duplicated, potentially more expressive and more readily available.⁶

The takeaway is that, so as to avoid difficulty imposed by semantics, whether described as computer generated or electronically generated or e-evidence or document or digital evidence, the purport is to cover specie of evidence of forensic value tied to technology in their creation, storage, use and retrieval etc.

In tune with the above realities, the Evidence Act 2011 has given a wide and improved definition of ‘document’ to incorporate modern means of information storage and retrieval such as computer databases contained in hard drives, CD-ROMs, Magnetic Discs, Flash Disks, and Floppy Diskettes as well as Motion Pictures recorded in Videotapes, Cassettes, Compact Discs, Micro Films, Micro Fiches, etc.⁷ The precise provisions in s258(1) is that ‘document’ includes:

- (a) books, maps, plans, graphs, drawings, photographs, and also includes any matter expressed or described upon any substance by

⁵ Vivek Dubey, ‘Admissibility of Electronic Evidence: An Indian Perspective’, (2017) 4(2) *Forensic Res. Criminol. Int. J* <<http://medcraveonline.com/FRCIJ/FRCIJ-04-00109.pdf>> accessed February 21, 2018

⁶ *ibid*

⁷ Peter Oyin Affen, ‘Admissibility of Documentary Evidence: Matters Miscellaneous’ (Being Paper delivered at the 3-Day Workshop Organised by the Magistrates Association of Nigeria, FCT Chapter on June 29, 2016)

means of letters, figures or marks or by more than one of these means, intended to be used or which may be used for the purpose of recording that matter;

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

It is notable that the definition opened with the word ‘includes’, thereby enlarging the scope beyond only the circumstances mentioned. We must comment a bit on the inclusion of ‘photograph’ as a document. A distinction has to be made between where the device (such as a digital camera), which stores the photograph in binary form but cannot be visually understood, is itself brought before the court (in which case it will be primary evidence) and a situation where a digital photograph is printed, for it then becomes creation of an electronic record produced from the digital camera itself or produced with the help of a computer (in which case it is secondary evidence).⁸

C. ADMISSIBILITY OF ELECTRONICALLY GENERATED EVIDENCE

Preliminary Points

By way of introduction, we consider it helpful to briefly discuss the concept of admissibility of evidence, before zeroing-in on the admissibility of electronically generated evidence.

⁸ A digital photograph does not require any film or paper for its generation or storage unlike a traditional photograph that required some kind of analogous representation. See Aratrika Chakraborty and Anuradha Parihar, ‘A Techno Legal Analysis of Admissibility of Digital Photographs as Evidence & Challenges’ (2017) 3 (5) *Internationals Journal of Law* 13-18 <<http://www.lawjournals.org/download/189/3-5-14-149.pdf>> accessed February 23, 2018

Admissibility of evidence is the eligibility of particular pieces of evidence for reception as part of the evidence in a case. Admissibility means the character or quality which any material must necessarily possess for it to be accepted and allowed to be presented or introduced as evidence in court. Admissibility answers the question: should the court allow the material to be used as evidence by the party proposing to do so?

The *Black's Law Dictionary*⁹ defined admissibility to mean the quality, state or condition of being allowed to be entered into evidence in a hearing, trial or other official proceeding. Thus, to be admissible means capable of being legally admitted or allowable or permissible as evidence or worthy of gaining entry or being admitted. Consequently, works on evidence has been dominated by the study of what can be or cannot be evidence; the discussion, therefore, usually revolves around inclusionary rules (by virtue of evidence becomes admissible) and the exclusionary rules (by virtue of which evidence becomes inadmissible).

In general, for evidence to be admissible, it must meet certain requirements, namely:

- (i) The evidence must be relevant;
- (ii) The evidence must be pleaded;
- (iii) Necessary foundation was laid as precondition for its admissibility e.g. photocopy of a lost document (see the proviso to s2);
- (iv) The evidence is not disallowed or excluded by the Evidence Act or under any other statute (s1(b) and s2);
- (v) It complies with requirements of law for its admissibility.

Relevancy of a piece of evidence is the relationship it has with the facts in issue in the case before a court and it is usually the surrounding circumstances that will determine the relevancy of a fact. However, not all relevant facts are necessarily admissible. What facts are relevant and admissible is governed by the Evidence Act, 2011 and this is illustrated in the opening provisions of the Act. Thus, evidence may be given in any suit or proceedings of the existence or non-existence of every fact in issue.¹⁰

⁹ *Black's Law Dictionary* (10th edn., 2014) 55, 56

¹⁰ s1

Similarly, evidence may be given of such other facts declared to be relevant by the Act;¹¹ such facts are those which fit any of the circumstances defined as relevant in Part II, ss4 to 13 Evidence Act, 2015.

Be that as it may, for such relevant facts to be admissible, they must not be too remote.¹² At the discretion of the court, evidence may be considered remote, because it is far removed or separated in time, space or relation to the fact in issue, or it is a question on the credit of the of the witness under cross-examination and deemed improper because the imputation which the question convey relates to matters so remote in time, or of such a character, that the truth of the imputation would not affect, or would only affect in a slight degree, the opinion of the court as to the credibility of the witness on the matter to which he testifies.¹³

It is known to be a cardinal rule of pleadings that for material facts to be admissible in evidence they must be pleaded. Therefore, where such facts are not pleaded, they are in law inadmissible in evidence, and where inadvertently or wrongly admitted, they go to no issue and should rather be disregarded as irrelevant to issues properly raised by the pleadings.¹⁴ Whereas the Evidence Act did not itself provide admissibility anchored on pleadings,¹⁵ it has contemplated the applicability of stipulations in other laws on conditions in which particular kinds of evidence may be admissible or inadmissible.¹⁶

Where necessary foundation is required to be laid as precondition for admissibility of an item of evidence, unless the foundation is laid, the evidence would be inadmissible.¹⁷ Thus, where a party intends to tender the photocopy of a document, he must adduce foundational evidence to satisfy s89(c) showing that the original has been destroyed or lost and in the case of loss, all possible search has been made for the document without success.

¹¹ *ibid*

¹² s1(a)

¹³ s224(2)(b)

¹⁴ *Aminu & Ors v Hassan & Ors.* (2014) LPELR-22008(SC)

¹⁵ Though it acknowledged the procedure of pleadings in ss123 and 174(2)

¹⁶ ss1(b), 2 and 3. See the Civil Procedure Rules of various courts e.g. Order 23 Rule 2 District Court Rules Cap. 495 LFN, 1999 (Abuja)

¹⁷ See the proviso to s2

There are also instances where there is absolute prohibition by law of the admissibility of some classes of evidence. In other words, for evidence to be admissible, it must not be such that is disallowed or excluded by the Evidence Act or under any other statute.¹⁸ Thus, under the Stamp Duties Act,¹⁹ it is provided that no instrument executed in Nigeria or elsewhere, relating to any property situate or to any matter or thing done or to be done in Nigeria, shall, except in criminal proceedings, be given in evidence, or be available for any purpose whatever, unless it is duly stamped in accordance with the law in force in Nigeria at the time when it was first executed.²⁰ Another common example is s3 Survey Act²¹ where it is stated that no map, plan or diagram of land, if prepared after the 16th day of May, 1918, shall, save for good cause shown to the court, be admitted in evidence in any court, unless the map, plan or diagram has been prepared and signed by a surveyor or is a copy of a map, plan or diagram so prepared and signed and is certified by a surveyor as being a true copy and has been examined by the Survey Department and bears the countersignature of the director.²²

Finally, where there are requirements of law to be complied with as condition for its admissibility, those requirements must be complied with before the evidence is admitted.²³ Thus, the Evidence Act has provided that it is only a Certified True Copy of a public document other than the original that is admissible.²⁴ However, for a document to be accepted as such a CTC, it must comply with the provisions of s104; that is, it must be shown that the prescribed legal fees were paid, that there is a certificate written at the foot of such copy that it is a true copy of such document or part of it as the case may be, that it is dated and that it is subscribed by such officer with his name and his official title and that it is sealed.

¹⁸ s1(b) and s2

¹⁹ Cap. S8, LFN 2004 s 22(4)

²⁰ We must however take note of the decision in *Okuwobi v Ishola* [1973] NSCC 168 that since the provision is principally intended for raising revenue, rather than reject the document as inadmissible, the court should have directed the document in question to be duly stamped and then received it in evidence.

²¹ Cap. 553 LFN 1990 (Abuja)

²² We should again note the approach of the Supreme Court in *Benjamin v Banigo* (1959) SCNLR 374 where the court adjourned the appeal hearing and sent the plan for the countersignature of the Director of Surveys to dispose that ground of appeal.

²³ s3

²⁴ s88, s89(e) and (f) and s90(1)(c)

Another preliminary point to make is that the law of evidence has long been guided by the rule of “best evidence” which is considered to have two basic paradigms – avoidance of hearsay and production of primary evidence. In the context of a document, it will be hearsay if the object of the evidence is to establish the truth of what is contained in the statement rather than merely to establish by evidence the fact that it was made.²⁵ By s38 of the Evidence Act, hearsay evidence is generally inadmissible except as provided under Part IV or under other provisions of the Evidence Act or any other Act. It is in this regard that the provisions of the Act on electronically generated avoided been caught by the hearsay rule.

The ancillary point is the well-defined distinction between primary and secondary evidence. As will be seen shortly, with computer based evidence the lines appeared blurred as device itself could be evidence.

(a) Admissibility as a Primary Document

Part V of the Evidence Act is headed ‘Documentary Evidence’. Under the subheading of ‘Primary and Secondary Documentary Evidence’, the Act in ss85 to 92 made a dichotomy between primary and secondary documents in terms of proof and admissibility. Section 85 opened by providing that the ‘contents’ of a document may be proved either by primary or by secondary evidence.

Whereas the Act provided that primary evidence means the document itself produced for the inspection of the court²⁶ and gave circumstances in which the contents of a document may be taken as primary evidence, there is no definition of secondary evidence. Rather, the statute gave a non-exhaustive²⁷ list of circumstances in which a document is secondary evidence.²⁸ Thus, we can deduce that every evidence fitting the definition of a document but which is other than the document itself or is any of the circumstances in s86(2) to (4) is secondary evidence.

²⁵ s37(b) and *Abadom v State* (1997) 9 NWLR (Pt. 479) 1

²⁶ s86(1)

²⁷ Considering the use of the word ‘include’.

²⁸ s87

The Act has provided that the contents of documents shall be proved by primary evidence except where deviations are permitted under the law.²⁹

However, distinct from the dichotomy made between primary and secondary evidence, the Act further made a dichotomy between ‘document’ and ‘copy of a document’ in its interpretation section,³⁰ in each case starting with the word ‘includes’, thereby enlarging the scope of the subject matter it qualifies or tends to qualify. When s258(1) and Part V of the Act are strictly construed together, secondary evidence is essentially a copy of a primary evidence, apart from counterparts of documents as against the parties who did not execute them and oral accounts of the contents of a document given by some person who has himself seen it,³¹ or where it is an admission in writing by the person against whom it is proved.³²

Thus, we may deduce that ‘document’ in s258(1) is intended as an extension of the definition of primary evidence while ‘copy of document’ is similarly an extension of the classes of secondary evidence, in this case specifically derived from the definition of document and giving the specific forms of secondary evidence contemplated.

In the context of the above provisions, when thus is computer or electronically generated evidence the primary evidence? To aid a resolution of this question the relevant provisions are extracted and produced below:

- (i) The document itself (s86(1)) is primary evidence. This will include cases where an otherwise secondary evidence is tendered in the form it came to be relevant to the fact in issue. This is irrespective that in its provenance it may have been computer generated.
- (ii) Where a number of documents have all been made by one uniform process, as in the case of printing, lithography, photography, computer or other electronic or mechanical process, each shall be primary evidence of the contents of the rest; but where they are all

²⁹ s88

³⁰ s258(1)

³¹ s87(d) and (e)

³² ss89(b) and 90(1)(b)

copies of a common original, they shall not be primary evidence of the contents of the original. (s86(4) and s87(b)).

- (iii) Document includes 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. (s258(1))
- (iv) Document includes 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. (s258(1))
- (v) Document includes any device by means of which information is recorded, stored or retrievable including computer output. (s258(1)).

To illustrate (i) above, if the claimant's case is that the defendant, in the course of negotiation over a parcel of land, gave the claimant photocopies of the title documents to reassure him of the genuineness of the land, for the purposes of proving that fact, the original or primary evidence is the photocopy given to the claimant and it shall be admissible as such.

Nowadays, almost everything in hardcopy is produced from a computer. Court processes, letters of appointment, letters of invitation etc. are produced from a computer. It is under the combined reading of s86(4) and s87(b) of the Evidence Act (i.e. (ii) above) that such documents, though computer produced are accepted as primary evidence without prior foundation. In such cases the use of the computer or electronic device did not add to, validate or strengthen the veracity of the contents but was merely a vehicle for the production of those contents for use by the maker.³³

In (iii) and (iv) above, the disc, tape, sound track or other device in which sounds or other data are embodied or the film, negative, tape or other device in which one or more visual images are embodied are primary

³³ In this case there is no 'storing' or 'processing' of the information.

evidence and could be tendered in the form in which they are. However, before they can rank as primary evidence, they must have been deployed in capturing the sound data or the visual images in their pristine origin, not as a subsequent device into which such sounds or visual images was transferred. Characteristically, the contents of the document, whether sound data or visual images, must be capable of being reproduced from it with or without the aid of some other equipment.

Finally, under (v) above, a device of whatever description, irrespective of its contents, is primary evidence if it is a means by which information is recorded, stored, processed or retrievable, including computer output. This categorization tallies with when a document may be classified as real evidence but as documentary evidence its usefulness is tied to its content. Where the document (device) is itself tendered in evidence, but is tendered along with copy in a readable form, the admissibility of the device enures for both, under the *majori continet in se minus* rule,³⁴ and thus no further test of admissibility need to be satisfied with respect to the copy.

Whereas, under the circumstances in (iii), (iv) and (v), the disc, tape, sound track or other device in which sounds is embodied or the film, negative, tape or other device in which one or more visual images are embodied, or any device on which information is recordable, storable or retrievable are *prima facie* primary evidence and hence admissible under s88, they are usually not in the form their contents can be comprehended by the court. Hence, unless they are accompanied by explanatory or demonstrative evidence, they are likely to be useless to the court and carry no weight.

(b) Admissibility as a Secondary Document

Secondary evidence is evidence other than primary evidence. The admissibility of electronically or computer generated evidence as secondary evidence is discussed under three subheads discussed below.

(i) Admissibility as copy under s258(1) Evidence Act, 2011

³⁴ The greater includes the less

Flowing from the definition of document in the interpretation section,³⁵ the Act similarly identified what may constitute a copy of a document. Thus, where the evidence in question is a disc, tape, sound track or other device in which sounds or other data (not being visual images) are embodied, the copy of such document would include a transcript of the sounds or other data embodied in it.³⁶ A transcript is a handwritten, printed, or typed record of something, e.g. a copy of the script of a broadcast program or a record of court proceedings. This also fits in with the definition of secondary evidence which includes ‘copies made from or compared with the original’.³⁷

Thus, for instance, if the original tape or disc is shown or appears to be in the possession or power of the person against whom the document is sought to be proved or has been destroyed or lost and in the latter case all possible search has been made for it,³⁸ then the transcript could be admissible without any further ado.³⁹ The only snag would be whether or not there would be sufficient evidence to authenticate the veracity of the transcript as to confer weight on it.

Similarly, where the document in question is a film, negative, tape or other device in which one or more visual images are embodied, a copy would include ‘a reproduction or still reproduction of the image or images embodied in it whether enlarged or not’. However, where the document is both a disc, tape, sound track or other device in which sounds or other data are embodied and a film, negative, tape or other device in which one or more visual images are embodied, a copy would include both ‘such a transcript together with such a still reproduction’.

The point here is that, in these circumstances, we have to relate back to the criteria for admissibility of secondary evidence in the place of the original in ss87, 88, 89 and 90 of the Evidence Act to determine whether or not the copy of document is admissible.

³⁵ s258(1)

³⁶ Logically, other types of copy are not excluded.

³⁷ s87(c)

³⁸ s89(a)(i) and (c)

³⁹ s90(1)(a)

(ii) Admissibility under s84 of the Evidence Act, 2011

This section in the Evidence Act is entirely new and has attracted robust analysis and commentary. Luckily for this writer, the Supreme Court of Nigeria in some decisions has considered the provisions of s84. Consequently, our discussion of the section shall take bearing from those Supreme Court decisions. Two of these cases are *Kubor & Anor. v Dickson & Ors.*⁴⁰ and *Dickson v Sylva & Ors.*⁴¹ We will set down the key excerpts relevant to s84 made by the Supreme Court in those decisions.

Kubor & Anor. v Dickson & Ors.

1. The admissibility of computer generated document or e-document down loaded from the internet is governed by the provisions of section 84 of the Evidence Act, 2011.
2. A party that seeks to tender in evidence a computer generated document needs to do more than just tendering same from the bar. Evidence in relation to the use of the computer *must* be called to establish the conditions set out under Section 84(2) of the Evidence Act, 2011. In other words, a party must fulfill the pre-conditions laid down by law, and if not such computer generated evidence or documents would be inadmissible.
3. Where documents are essentially public documents, they remain public documents and the fact that they are computer print outs or e-documents does not change their nature and character as public documents and it is settled law that the only admissible secondary evidence of public documents is a certified true copy of same.⁴²

The above excerpts are from the lead judgment of Onnoghen JSC. We note that in this case His Lordship rather treated the computer printout downloaded from the internet as public documents instead of as computer generated evidence. It is also noteworthy that specific reference was made only to s84(1) and (2) but nothing was said on the effect of s84(4).

⁴⁰ [2012] 10-11 SC 1

⁴¹ (2016) 7 SC (Pt. VI) 165

⁴² At 61

Perhaps, this is understandable given the explanation by His Lordship Dattijo Muhammad JSC that a consideration of the correctness or otherwise of the lower court's finding that the computer printouts are inadmissible would be an academic exercise since the ground of appeal to which the documents relate has been abandoned by the Appellants.⁴³ However, the reasoning in the lead judgment found support in the contribution of Hon. Justice Ogunbiyi when His Lordship stated that 'internet print out of the Punch Newspaper,... is by nature a secondary evidence of the original by reason of the provisions of sections 85 and 87(a) of the Evidence Act 2011'.⁴⁴

Dickson v Sylva & Ors.

1. Section 84 of the Evidence Act lays down the conditions for the admissibility of electronically generated evidence.
2. It is s84 and not s258 (the definition Section) of the Act that confers admissibility status on computer generated evidence.
3. Section 84 consecrates two methods of proof, *either* by oral evidence under s84(1) and (2) or by a certificate under s84(4). In either case, the conditions stipulated in Section 84(2) *must* be satisfied.
4. Irrespective of the foregoing, there is residual power on the 'Judge to require oral evidence in addition to the certificate'.
5. There is a distinction between admissibility of computer generated evidence and the weight to be attached. Whereas the requirement for admissibility is satisfied by complying with s84, for weight to be attached to it, the accuracy conditions in s34(1) (b) (i) and (ii) have to be complied with.
6. Demonstration of the computer generated evidence is with a view to conferring weight on the evidence, not to make it admissible. Hence, once the evidence itself has satisfied the provisions of s84, any device

⁴³ At 78

⁴⁴ At 80-81

required to demonstrate it is not necessarily required to comply with s84.

Again, the above excerpts are from the lead judgment of Nweze JSC. However, as acknowledged by His Lordship, what was in issue was not even the admissibility of evidence, but the narrow question whether s84 deals with the additional requirement of certification of gadgets for playing or demonstrating an already admitted piece of evidence in open Court.⁴⁵

Galadima JSC in his supporting judgment reiterated that ‘it is crystal clear that it is only with respect to the computer that “produces” the document, in this case the DVD (Exhibit P42B), that ought to be certified’.⁴⁶ Rhodes-Vivour JSC similarly opined that ‘A diligent examination of Section 84 of the Evidence Act reveals that the section does not say that the computer or electronic device used in playing the DVD in open Court requires certification, rather it is only the computer that *produces* the DVD - Exhibit ‘P42B’ that requires certification. Section 84 in the Evidence Act is all about ascertaining the authenticity of the device from which the exhibit was produced’.⁴⁷

In his contribution, Ngwuta JSC quoted the phrase ‘a statement contained in a document produced by a computer’⁴⁸ from s84(1), identified ‘statement’ and ‘document’ as the key words and drew a distinction between them, the statement being the content of a document, holding that, in the context of this case, ‘the DVD, Exhibit P42B, in so far as it is used to record and store information is a document and the information therein contained is a statement within the intendment of Section 84 of the Evidence Act’. His Lordship then made an analogy that producing the statement contained in a document produced by a computer which has been admitted in evidence is the same thing as providing the Court or Tribunal a document properly so called which has been admitted in evidence for the Court or Tribunal to read; once the conditions for

⁴⁵ At 197

⁴⁶ At 217

⁴⁷ At 222

⁴⁸ The same phrase was adopted by Nweze JSC in *Omisore & Anor v Aregbesola & Ors.* [2015] 15 NWLR (Pt. 1482) 205 to hold that s84 did not apply only to internet-generated documents.

admission of the document have been satisfied and the document, be it one produced by a computer or one properly so called, admitted, there can be no other requirement before the Court or Tribunal can make use of the statement contained in the document.⁴⁹

However, one question that agitates the mind is whether substantial compliance with s84 will suffice. Despite our industry, we were not able to find any authority in which the extent of compliance with s84 has become an issue. With respect to certification of a public document as Certified True Copy, in *Omisore & Anor. v Aregbesola & Ors.*,⁵⁰ it was held that ‘documents which, merely, had CTC stamps bearing engraved signatures on them without the subscription of the name and the official title of the officer who certified them, were not properly certified in conformity with the mandatory requirements of Section 104’. This is against the grain of the reasoning in *Daggash v Bulama*,⁵¹ where a government white paper which bore the date, signature and official title of the Secretary to the Government of Borno State was held to have been substantially certified in conformity with the provisions of the Evidence Act.

Of the same tenor as *Bulama’s Case* is the Supreme Court case of *Narindex Trust Ltd. v. N.I.M.B. Ltd.*⁵² Falling to be construed was whether the four conditions in s97(2)(e) of the repealed Evidence Act (same as s90(1)(e) in the Evidence Act, 2011) required as foundation for admitting secondary evidence when the document is an entry in a banker’s book has been satisfied. It was held that ‘It is not necessary according to law that the words of the section must be strictly followed word by word before secondary evidence of the entries in the ledger of the bank is admitted in evidence once there is substantial compliance’. Following the precedence in *Narindex*, we think and submit that what is required is substantial compliance and not exact compliance with the provisions of s84(2) or 84(4) as the case may be.

⁴⁹ At 229

⁵⁰ (2015) 15 NWLR (Pt. 1482) 205

⁵¹ (2004) 14 NWLR (Pt. 892) 144

⁵² (2001) 10 NWLR (Pt.721) 321

Finally, on the scope of the class of documents to which s84 may be applied, it was held in *Omisore & Anor. v Aregbesola & Ors.*⁵³ that it is not only internet-generated documents that are caught by the admissibility requirements of s84 of the 2011 Evidence Act but it will rather extend to every kind of computer generated evidence.

(iii) Admissibility under other Sections other than s84 Evidence Act

Apart from s84, there are sundry other provisions under which electronically based evidence are admissible under the Act. We will discuss the applicability of these sections below.

Statements made in the course of business

Admissibility of statements made in the course of business is a long accepted exception to the rule against hearsay. By s41 of the Evidence Act, when a statement consisting of an entry or memorandum is made by a person in the ordinary course of business in books and electronic devices kept in the ordinary course of business, such statement is admissible.

Upon a strict consideration of s41, by the use of the disjunctive ‘or’, it appears to us that ‘the ordinary course of business’ requirement may be unnecessary if the statement was made in the discharge of a professional duty, or as an acknowledgment written or signed by a person of the receipt of money, goods, securities or property of any kind, or of a document used in commerce written or signed by a person or of the date of a letter or other document usually dated, written or signed by such a person.

In any event, to be admissible, it must be shown that ‘the maker made the statement contemporaneously with the transaction recorded or so soon thereafter such that the court considers it likely that the transaction was at that time still fresh in his memory’.

Section 41 is a kindred of s51 which provides that entries in books of accounts or electronic records regularly kept in the course of business are admissible whenever they refer to a matter into which the court has to

⁵³ *Supra*

inquire, but such statements shall not alone be sufficient evidence to charge any person with liability.⁵⁴

Admissibility as Official Records

By s52 of the Evidence Act, an entry in any public or other official books, register or record, including electronic record stating a fact in issue or relevant fact and made by a public servant in the discharge of his official duty, or by any other person in the performance of a duty specially enjoined by the law of the country in which such book, register or record is kept, is itself admissible.

In like manner, where maps or charts so made are reproduced by printing, lithography, or other mechanical or electronic process, all such reproductions purporting to be reproduced under the authority which made the originals shall be admissible in evidence without further proof.⁵⁵

(c) Concluding remarks

As can be seen from the discussion thus far, whereas s84 has elicited the greatest commentary in the discussions on admissibility of computer generated evidence, there are sundry other provisions in the Evidence Act under which we have discussed admissibility of computer generated evidence. Thus, the relationship between these different sections is worth exploring.

Admittedly, s84 of the Act is specifically on the admissibility of a 'statement contained in a document produced by a computer' though other sections, similarly considered, randomly used words such as 'electronic device', 'electronic records' and 'electronic process'.

There are several rules of construction simultaneously at play here. Firstly, the law is that where there is a special provision in a statute, a later general provision in the same statute capable of covering the same subject matter is not to be interpreted as derogating from what has been specially

⁵⁴ It must be noted that whereas s41 used 'books' and 'electronic device', s51 used 'books of accounts or electronic records'. Consequently, s41 appears to be wider in scope and could be seen as subsuming s51.

⁵⁵ s151(3)

provided for individually, unless an intention to do so is unambiguously declared.⁵⁶ It is an accepted canon of construction that where there are two provisions, one special and the other general, covering the same subject-matter, a case falling within the words of the special provision must be governed thereby and not by the terms of the general provision.⁵⁷

The order in which provisions appear in legislation does not usually affect their relative importance. The last provision in the last schedule of an Act carries as much weight as every other provision in the Act. It is also the rule that each provision in an Act has the same weight and importance as every other provision unless it is clear that one is made dominant or subordinate to the other by the use of appropriate qualifying words such as ‘without prejudice’, ‘notwithstanding’ and ‘subject to’ etc.⁵⁸

Harmonious interpretation postulates that where there are more than one provision in a statute on a subject-matter, the statute should be read as a harmonious whole whenever reasonable, with separate parts being interpreted within their broader statutory context⁵⁹ such that effect can be given to both and that construction which renders either of them inoperative and useless should not be adopted except in the last resort.⁶⁰

Closely scrutinizing s84 Evidence Act, it is clearly not worded to be the only circumstances under which computer generated evidence would be admissible under the Act. What s84(1) provides is that ‘statement contained in a document produced by a computer’ ‘shall be admissible as evidence’ if the conditions sub-ss(2) and (4) are satisfied. This conclusion would have been different if the phrase used were ‘shall *only* be admissible as evidence’. In other words, s84 is essentially an enabling provision.

⁵⁶ *Jack v UNAM* (2004) 5 NWLR (Pt. 865) 208

⁵⁷ *F.M.B.N. v Oloho* (2002) 9 NWLR (Pt. 773) 475 per Uwaifo, JSC

⁵⁸ Parliamentary Counsel’s Office, ‘How to read legislation, a beginner’s guide’ (Government of Western Australia, 2011) 12, 27 <http://www.department.dotag.wa.gov.au/files/How_to_read_legislation.pdf> accessed March 20, 2018

⁵⁹ Larry M. Eig ‘Statutory Interpretation: General Principles and Recent Trends’ (Congressional Research Service, 2014) <<https://fas.org/sgp/crs/misc/97-589.pdf>> accessed March 20, 2018

⁶⁰ Rajkumar S. Adukia, ‘Interpretation of Statutes’ <<http://www.caaa.in/Image/Interpretation%20of%20Statutes.pdf>> accessed March 19, 2018

Therefore, in our opinion, s84 did not exclude the applicability of admissibility of computer generated evidence under other provisions of the Evidence Act nor are the requirements in s84, such as certificate, mandatory for purposes of admissibility under such other provisions.⁶¹ In fact there is a sound precedent in the decision of the Supreme Court in *Kubor & Anor. v Dickson & Ors.*,⁶² where computer generated documents or electronic-documents downloaded from the internet were rather taken as public documents and subjected to the test of admissibility of a certified true copy, instead of as an electronic document.

By way of analogy, the comparable provision to s84 in the Indian Evidence Act is s65B. In *Anvar P.V. v P.K. Basheer*⁶³ the Indian Supreme Court held that while ss61 to 65 of the Act deals with general documentary evidence, s65B only refers to one special subset i.e. electronic records, therefore making applicable the principle of *generalia specialibus non derogant*. It was further held that, more importantly, since s65B opened with a *non-obstante* clause, it alone guides admissibility of electronically generated evidence and a certificate is mandatory to the admissibility of the electronic record. The difference here is that there is no such *non-obstante* clause in s84 and its overall tone is not to make it superior to other provisions on admissibility.

Be that as it may, our system being adversarial in nature, where the disputants are metaphorically considered to be in a duel with the court as an unbiased umpire, the court should let the parties raise the issues as to which of the various provisions of the Act they anchor the admissibility of an electronically generated evidence on or on which provision any objection to admissibility is based. It may then rule on admissibility within those narrow prisms. If the proponent does not know enough that he could have as well reclined on an alternative basis for admissibility, he should suffer in his ignorance.

⁶¹ We must also advert our minds to the principle of 'multiple admissibility'. It is a principle of evidence law to the effect that when evidence is admissible for one purpose it should not be rejected solely because it is inadmissible for some other purpose.

⁶² supra

⁶³ (2014) 10 SCC 473

D. ASCRIPTION OF WEIGHT TO ELECTRONICALLY GENERATED EVIDENCE

To weigh evidence means to assess the reliability and probative value of evidence that has already been determined to be relevant and admitted. The probative value of evidence is its value in assisting in determining the matters in issue. A piece of evidence may be given full weight, partial weight, more or less weight than other evidence, or no weight at all. One item of evidence is weighed against another evidence to determine which evidence is more reliable and, ultimately, the weight of the evidence will be used to determine whether the burden of proof has been discharged in given cases. The entire process of ascription of weight to evidence is synonymously referred to as the evaluation of evidence, defined as the assessment of evidence so as to give value or quality to it.⁶⁴

Ascription of weight is the exclusive domain of the *judex*. However, a judge cannot be capricious or whimsical about how he performs the task of evaluating evidence and ascription of weight to them. He must rather be deliberate, creative, imaginative, steeped in sound reasoning and pay heed to precedence. Thus, what we have done in this paper is to set out some guides that may be deployed in evaluating electronic or computer generated evidence. This has been done under three subheads. Firstly, we considered relevant provisions under the Evidence Act. Next we considered factors generally applicable to the evaluation of documentary evidence, and, lastly, we considered evaluation criteria peculiar to electronic or computer generated evidence.

(a) Factors for Ascription of Weight under the Evidence Act

Generally, by s34(1)(b) of the Evidence Act, in estimating the weight, if any, to be attached to a statement contained in a document produced by a computer, two indicia are relevant. The first is whether the root information from which the statement was produced was supplied contemporaneously with the occurrence or existence of the facts dealt with in that information.

⁶⁴ Idhiahhi, op. cit. 8,9

The second consideration is whether any of the persons concerned with either the feeding 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 the computer, had any incentive to conceal or misrepresent facts. To summarize, there must have been contemporaneity and want of bias in the origin and production of the statement produced from the computer.

Whether or not in a given case the court will consider that there was contemporaneity and lack of bias in the origin and production of the statement produced from the computer will depend on the nature of issues joined. If the opposite party did not, at the point at which such evidence is tendered, or, in the course of cross-examination of the witness through whom it was tendered, raise issues of contemporaneity or bias, there is no impediment on the court to act on such evidence as free of defect. On the other hand, if such issues were raised, the court will look to see how well they were answered before deciding on the value to attach to the statement. Obviously, if a certificate as required in s84(4) is produced to the court, *sans* other adverse factors that may assail such evidence, it is to be taken as contemporaneous and free of bias.

The Act recognizes the validity of an electronic signature in lieu of manual signature.⁶⁵ Such an electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

In evaluating evidence, presumptions⁶⁶ also come in aid of courts. Thus, by s153(2), the court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission, though it shall not make any presumption as to the person to whom such message was sent.

⁶⁵ s93(2)

⁶⁶ See Part X ss145 to 174 on different kinds of presumption in the Evidence Act

Finally, by s34(2), the fact that a statement is computer generated, contemporaneous and free of bias of the human agent will not by that fact alone satisfy a requirement for corroboration. However, for purposes of determining whether or not a person drove beyond maximum speed, the evidence of a duly authorized officer of the relevant authority who was at time of the commission of the offence operating any mechanical, electronic or other device for the recording of the speed of a moving vehicle, the record of such device being additionally tendered in evidence against the defendant, shall not require further corroboration.⁶⁷

(b)General Factors for Ascription of Weight to Documents

By the definition of documents in s258(1), it is now established it covers computer or electronic evidence. Thus, the usual factors deployed in evaluating documentary evidence apply with equal force to such electronic evidence. A potpourri of these factors is listed below:

- (i) The more the making of a document is synchronous to the happening of the matters or things of which it is a record of, the weightier such a document. To be ‘contemporaneous’ was held to mean ‘occurring during the same period of time’.⁶⁸
- (ii) The older the document or the closer it is in its making to the time period in which the events it recorded occurred, the more the weight to be ascribed to the document.⁶⁹
- (iii) Where a document is shown not to be genuine and legal, it is of no forensic value and no right can be hoisted upon it.⁷⁰ The mandate of an illegal thing is void.⁷¹
- (iv) Whether the document in question involves multiple layers of hearsay or whether indeed the original was a cumulative document which could impact on the reliability of the record.
- (v) The more relevant a document is to the fact in issue, in time and circumstance, the more weight it ought to attract while the more

⁶⁷ s203(1)

⁶⁸ *Ojibah v Ojibah* (1991) 5 NWLR (Pt. 191) 296 SC

⁶⁹ *Fatoyinbo & Ors. v Williams & Ors.* (1956) NSCC 79

⁷⁰ *Ojibah v Ojibah* (Supra)

⁷¹ *Rei turpis nullum mandatum est*

remote a document is to the fact in issue, the less weight it merits.⁷²

- (vi) What is the source of the document? Is the source indubitable and accord with logic and common sense?⁷³
- (vii) Failure to produce evidence in support of the origin of documents will entitle a court to draw inferences invoking section 167 (d) of the Evidence Act.⁷⁴
- (viii) Where two or more documents claim a common source, both documents purporting to vest conflicting rights in respect of the same subject-matter on different persons the first in time prevails.⁷⁵
- (ix) A document will attract more weight if there is evidence that all the parties concerned, or their privies, were involved in its making as against when it was the unilateral document of one party, unless it is against the interest of the person making it.⁷⁶
- (x) Document produced from proper custody attracts more weight as it is presumed to be genuine. Production of a document from proper custody confers on such document greater probability of accuracy.⁷⁷
- (xi) Whether the document is authenticated by the maker or someone else and whether the document is of a kind which is self-authenticating e.g. deeds and other notarized instruments, certified copies of public records, official publications including statutes, newspapers or periodicals, and, labels, signs, trade inscriptions or other inscriptions indicating ownership, control or origin.⁷⁸
- (xii) Possible bias of the author and his relationship to the parties.

⁷² *Ezekwesili & Ors. v Agbapuwonwu & Ors.* (2003) 9 NWLR (Pt. 825) 337 at 375

⁷³ *Otun & Ors. v Otun & Anor.* (2004) 14 NWLR (Pt. 893) 381

⁷⁴ *Dughuma v Andzenge*(2007) All FWLR (Pt. 385) 499 at 524.

⁷⁵ *Auta v Ibe* (2003) 15 NWLR (Pt. 837) 247 SC

⁷⁶ *Akibu & Ors v Oduntan & Ors.* (2000) 7 SCNJ 189

⁷⁷ *Ogbunyiya & Ors. v Okudo & Ors.* (1979) NSCC 77

⁷⁸ *Nasiru Garba Dantiye & Anor. v Ibrahim Yushua'u Kanya & Ors.* (2008) LPELR-4021 (CA) per Oredola JCA it was said that 'Basically, an unsigned or irregularly signed document is worthless and entitled to ascription of no weight at all in law. What is more, such a document binds no one'.

- (xiii) Specificity of the documentary evidence; as a measure of conclusiveness, a document ought to be unambiguous, decisive and unequivocal in the facts it seeks to establish instead of being entirely remote and conjectural such that its true context could only be ascertained by an enquiry into fresh collateral matters.⁷⁹
- (xiv) Consistency of the documentary evidence with the oral evidence in the case.
- (xv) Whether the document constitutes an admission,⁸⁰ such as a tweet or SMS that has been admitted by the sender.
- (xvi) Whether there was a sponsoring witness who was available for cross-examination and was cross-examined on it.⁸¹ Whether there was a failure to apply the confrontation rule.⁸²
- (xvii) While the language in which a document is written is irrelevant to its admissibility except where it is deemed hearsay, unless a document is written in English language or it is translated into English language, no probative value can be ascribed to it.⁸³

(c) Technical Factors for Ascription of Weight to Electronically Generated Documents

Computers or electronic devices are technical materials. The greatest challenge in relying on electronic records or computer based evidence is reliability. Electronic data is said to be easy to create copy, alter, destroy, and transfer from one medium to another. In short by their nature they can be easily manipulated, thus making their accuracy and reliability always suspect, and hence, creating a conflict between their relevance and admissibility.

The evidence obtained from the use of computers is not the usual run-off the mill evidence and so to ascribe value to it, some considerations must apply. We have thus set out factors that may apply to all computer or

⁷⁹ *MAT Holdings Limited v United Bank for Africa Plc.* (2003) 2 NWLR (Pt. 803) 71

⁸⁰ *Olale v Ekwelendu* (1989) 4 NWLR (Pt. 115) 327

⁸¹ *Odumade v Ogunnaike & Anor.* (2010) LPELR-4809 (CA)

⁸² *Esika & Ors. v Medolu* (1997) 2 NWLR (Pt. 485) 54.

⁸³ *Damina v State* (1995) 8 NWLR (Pt. 475) 573 SC, *Idowu v State* (2011) LPELR-3597 (CA) and *Asiniola v Fatodu* (2009) 6 NWLR (Pt. 1136) 184 at 198 CA

electronic based evidence and in doing so may discuss different rules applying to some specific kinds of electronic or computer based evidence.

(i) The Chain of Custody

As with real evidence, the court will be more persuaded about the premium to place on electronically generated evidence if it is supported by a defensible chain of custody record, which establishes the handling and movement of evidence before, during and after collection. An unbroken chain of custody is reason to confer valuable weight on the evidence. Any mishandlings of the collection and transfer of electronic data can adversely impact the weight given to the evidence by the court. Thus, establishing that data moved from point A to point B, and only from point A to point B, is important to show that the data was not at risk for being tampered or altered. Through a chain of custody form it can be seen the entire log of who handled those data or evidence involved and for what purpose. In majority of cases, issues as to chain of evidence may also likely arise if there are discrepancies as to the key characteristics of the items of evidence, e.g. its quality and quantity.

Where the evidence shows that the evidence was at one time in the chain in the custody of somebody who could have a motive to tamper with it, it calls for circumspection from the court. Similarly if there was an unexplained hiatus, such that between point A and point B, there was an interval in which the custody of the data could not be accounted for, the court will have to exercise caution in relying on such evidence.⁸⁴ The chain of custody of each piece of evidence, where the relevant evidence is the aggregation of several pieces, must be carefully documented.

When considering chain of custody of electronically generated evidence or evidence generally, the evidence of the systems in place to assure the integrity of the evidence while in custody will attract great weight to it. Hence, given the ubiquity of some electronic devices, for

⁸⁴ In *State v. Mason*, 144 N.C. App. 20 (2001) the court noted that there was no evidence of the chain of custody of the video between the time it was burned to a CD and the time it was shown at trial and hence ruled that it was insufficient authentication that a loss prevention manager testified that the video shown at trial was the same one he had viewed shortly after the incident.

instance, it will be considered advantageous if, for purposes of preserving the chain of evidence, the unique identification numbers were shown to have been recorded, thereby discharging this burden if there are many caches of similar looking or similarly identified disks that are in custody, and there is no way of distinguishing between them, or if they are mixed up.

(ii) Best Evidence Rule

The conditions under which the electronic record was made include date, time, location, people present, and other relevant conditions. The best evidence rule requires that the original document (recording) be admitted into evidence if it is available since digital recordings are very susceptible to alteration.⁸⁵ The rules of preference dictates that where a particular kind or character of evidence exists and is usually self-executing or self-sufficient and therefore considered to enjoy a higher degree of integrity, some other evidence of different or similar kind or character that usually depends on the existence or want of some other evidence or circumstances for the value ascribable to it or is considered more liable or susceptible to contamination or distortion, will succumb or yield weight to the former specie of evidence if the latter asserts anything contrary to it.⁸⁶

(iii) Metadata for authentication

Metadata, which is frequently referred to as “the data about data,” is electronically-stored evidence that describes the history, tracking, or management of an electronic document. Metadata includes the hidden text, formatting codes, formulae, and other information associated with an electronic document. For a typical document, metadata also includes, inter alia, the name of a file, its location on the computer’s hard drive, the file extension, dates of creation and modification, and names of users who have permission to open or alter a file. The use of properly preserved and collected metadata of any electronic document can be used to bolster a

⁸⁵ Swati Mehta, ‘Cyber Forensics and Admissibility of Digital Evidence’ (2012) PL January S-23
<http://www.supremecourtcases.com/index2.php?option=com_content&itemid=5&do_pdf=1&id=22821>
accessed February 23, 2018

⁸⁶ Idhiarhi, op. cit. 459, 460

proponent's likelihood of having such evidence properly authenticated and worthy of weight. The use of encryption on a computer will strengthen the authenticity of the relevant information and reduce the burden on the litigant in introducing the information into evidence.⁸⁷

By way of illustration, the metadata of an image that a digital camera records can include the dimensions of the image, the file size and location, the make and model of the camera used to take the photograph, the focal length and ratio, exposure time, and the dates the photo was taken, last modified, and last opened. Some cameras even have internal GPS chips that record the precise location the picture was taken. The date and time stamping in the camera can establish the proof of fact in issue.

Twitter metadata fields capture information such as timestamp for the creation date for individual tweets, the geo-location coordinates from where the tweet was sent, and the user's name. In like manner, Facebook metadata authenticating fields of information may include similar data: user ID, account ID, the date a post was created, name of a user a wall post is directed to, and a unique identifier of a message thread.

Be that as it may, caution is still advised and the court is advised to look for consistency in the information contained in the metadata with other evidence before ascribing weight. There is a caveat that metadata may not be entirely dependable for several reasons. It can be easily altered or it may not have been saved as accurate in the first place. There can also be instances where the date and time of the camera are already set incorrectly in the first place. Another case is when an image is transferred from the camera to the computer; it then reflects the date and time when the image was created in the computer not the original date of creation in the camera. Similarly, merely opening or resaving an image file also changes dates in the metadata of the image.

(iv) Expert Opinion for Authentication

⁸⁷ See *State v. Levie*, 695 N.W.2d 619 (Minn. Ct. App. June 10, 2005) where admission of testimony of a computer forensic expert about defendant's computer usage and the presence of an encryption program on his computer deemed admissible

Experts are persons specially skilled in a field of science or art who offers the court their opinion on their field of expertise to enable the court form its own opinion.⁸⁸ The existence of an accepted expert's opinion regarding computer related evidence may be ground for the court to accord great weight to the electronically-generated evidence.

An expert may explain why the content of the data generated by or derived from a computer is to be trusted or not to be trusted. Relying for instance on video evidence without expert interpretation risks failure to reach the correct conclusions based on the evidence or worse, reaching the wrong conclusions. Forensic analysis must present accurate results to the court. In order to do so the computer forensic expert must have good skills and knowledge on computer forensics and also digital forensic science. Forensic examiners must be able to explain in detail about the analysis conducted and learn how to quantify and account for the resulting uncertainties which include the system clock of the computer which represents the time, date and sequence of events.⁸⁹

An expert's evidence may be bolstered by demonstrative evidence, such as computer generated animations. Animations are themselves not evidence or purport to be scientific recreations of an actual event but are thought of as visual aids used in support of witness testimony with the purpose of helping the court understand a witness's testimony.

The proponent must however 'establish that the facts or data on which the expert relied in forming the opinion expressed by the computer animation are of a type reasonably relied upon by experts in the subject area', and that 'the computer animation [is] a fair and accurate depiction of that which it purports to be'. Additionally, the opposing party must be afforded the opportunity for cross-examination; the animation at issue may be without value where the expert whose opinion the animation illustrated

⁸⁸ s68

⁸⁹ Duryana Mohamed, 'Computer Evidence: Issues And Challenges In The Present And In The Future' p15 <http://irep.iium.edu.my/8321/1/computer_evidence_by_Dr_Duryana_Mohamed_2011.pdf> accessed February 21, 2018

never testified and the defendant had no opportunity to cross-examine him.⁹⁰

In contrast, computer simulations are considered substantive evidence. The computer itself is the expert. Simulations are computer-generated models or reconstructions based on scientific principles, created by entering data and engaging in computer-assisted analysis in accordance with widely accepted methodology. Rather than depicting a witness's testimony in the manner of an animation, simulations form conclusions based on raw data which the court may rely on and form an opinion.

(v) Evidence of Technical Integrity of Computer-Stored Records

For purposes of reliability and weight, proof of the integrity of computer record may correlate to the extent that computer related evidence is free of five possible errors. These are errors in perception, errors in input, errors associated with inadequate hardware security, errors caused by hardware, and errors associated with computer software.⁹¹

'Errors in perception' refers to mistakes which occur when computer operators misread information being put into the computer. 'Errors in input' occur when typographical mistakes are made. 'Inadequate hardware security', denoting the possibility of tampering, potentially affects the reliability of computer stored records, though it can be a problem with both manual and electronic record keeping systems. The last two problems, involving the reliability of hardware and software, are peculiar to computers themselves. Hardware means the computer equipment and peripherals; the equipment and devices that make up a computer system (hardware) as opposed to the programmes used on it, which is the software. Particularly, errors in software protocol could cause mistakes and inaccuracies in computer-stored or produced information.

⁹⁰ Fred E. (Trey) Bourn III and Victoria Webster, 'The Use of Computer-Generated Animations and Simulations at Trial' 83(4) *Defence Counsel Journal*

<<https://www.iadclaw.org/publications-news/defencecounseljournal/the-use-of-computer-generated-animations-and-simulations-at-trial/>> accessed February 23, 2018

⁹¹ Randy Snyder, 'Assuring the Competency of Computer-Generated Evidence,' (1989) 9(105) *Computer L.J.* 103 at 105

<<https://repository.jmls.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1434&context=jitpl>> accessed February 23, 2018

With errors in perception and errors in input, they are ever present regardless of the system used, but are tempered by the presumption of reliability pertaining to business records that assumes keeping the records in the regular course of business assures accuracy. More importantly, the court will look to see if there is evidence that the computer system is designed to contain sub-systems to catch input errors. While it is unlikely that an error-checking system will detect all mistakes, such systems decrease the number of errors in the business records.

With inadequate hardware security, the court will look to see what nature of house-keeping and security management are in place to keep away unwelcome interference with the computer and keep it from impacts that could cause it to malfunction. With hardware and software reliability, a certificate under s84(4) would readily confer reliability unless neutralized by cross-examination. Hardware carries out standardized mechanical procedures, which are relatively easy to test. The more the number of software applications in a computer, the greater the risk of inaccuracies bred by one. Similarly, software is constantly updated and hence the more up-to-date the software is, the more reliable the computer and the information obtained from it is taken to be. In the same way, for instance, the presence of anti-virus or computer content protection programmes will confer further credibility on computer related evidence.

E. CONCLUSION

We conclude by underscoring that we operate an adversarial system. Consequently, it is not the duty of the court to raise matters of inadmissibility or non-compliance with conditions precedent unless the evidence sought to be tendered is inadmissible in any event. It is for the opposite party to raise the objection and if no objection is raised to the non-compliance to the conditions, it would be taken as having been waived, and the evidence can be properly admitted.⁹² We thank you for listening.

⁹² *Oghoyone v Oghohone* (2010) All FWLR (Pt. 543) 1884 at 1861