

ABUAD Law Journal (ALJ)

Vol. 9, No. 1, 2021, Pages 36-50 <https://doi.org/10.53982/alj.2021.0901.03-j>
Published by College of Law, Afe Babalola University Law Journal,
College of Law, Afe Babalola University, Km 8.5, Afe Babalola Way,
P.M.B. 5454, Ado Ekiti, Ekiti State, Nigeria ISSN: 2971-7027
www.abuad.edu.ng, abuadlawjournal@abuad.edu.ng

Proof by Electronically Generated Evidence under the Evidence Act (2011)

Adamu Idris Taanimu*
Halima Doma-Kutigi (PhD) **

Abstract

The underlying principle upon which the concept of weight of evidence is based is that the court is urged to confer probative value or otherwise on a document that is being tendered and received in evidence. An invitation to ascribe probative value to a document which is evidence before the court works on the assumption that the document has been admitted in evidence as an exhibit. This assumption or presumption is rebuttable as the admissibility of a document could still be a relevant factor in the course of final addresses, judgment or even on appeal. Two key factors are critical in respect of electronic evidence in judicial trials or proceedings. These are admissibility and weight of documents. However, while the Evidence Act (2011) creates a general framework regarding the weight to be attached to such electronic evidence, it does not set out any basis for the opposing party to be able to show that the produced electronic evidence falls short of any of the above factors for probability. The challenges a party seeking to show that the produced electronic evidence is not probable are enormous. Implicit in the factor for admissibility is the confidentiality of the electronic evidence. Using doctrinal approach through content analysis of Nigerian statutes, case law, and relevant literature, the paper examines the principles relating to the ascription of probative value or weight of electronic evidence as a means of proof of a particular fact in judicial proceedings. The paper finds that generally, it is difficult to detect where the product of an electronic device has been tampered with; and since the provisions of the Evidence Act, 2011 is not clear on the authentication of electronic documents, the chance that the courts are more likely to be misled by evidence produced through an electronic device is higher than a hard copy of the evidence. Accordingly, the paper recommends that the Act be amended to include detailed rules for presenting electronically generated evidence.

Keywords: Evidence, Electronic, Evidence Act, Probability, Document, Admissibility

1. Introduction

Proof is how a particular fact in issue is established in any judicial process. A fact in issue is established or proved by evidence. Facts are necessarily proved by oral evidence whereas documentary evidence, by judicial decisions now requires oral evidence to establish the connection or probative value of such documentary evidence. Two key principles come to play when considering the means by which a fact is established; these are admissibility and weight of evidence. Both principles apply to oral evidence. The principle regarding the admissibility of documents generally enables the court to receive the document in evidence. Admissibility does not mean “that the particular facts have demonstrated the proposition to be proved, but merely that it is received by the tribunal for the purpose of being weighed with other evidence”.¹

The probative value ascribed to the document is a different factor. By probative value, the court determines what weight to confer or ascribe to evidence that is to be tendered. The proof of electronic evidence, therefore, contemplates two principles of law, to wit admissibility and weight of evidence. Thus, the fact that a document is admissible is not synonymous with the document having probative value for the purpose of proof of the fact in issue. A document or piece of evidence is first admissible in proof of fact before its weight becomes in the adjudicatory process.

The Admissibility of the document *per se* does not ascribe weight or probative value to the document. In this article, we shall consider the various statutory provisions that form the basis of a court ascribing probative value or weight to an electronic document that has been received in evidence. We shall examine the principles relating to the ascription of probative value or weight of electronic evidence as a means of proof of a particular fact in judicial proceedings.

*Lecturer in the Department of Public Law, Faculty of Law, Bauchi State University Gadau, Bauchi State. Email:adamtaanimu90@gmail.com; Phone Number:08036042846

**Lecturer, Faculty of Law, Nasarawa State University, Keffi. Email: halimisi@yahoo.com. Phone Number:08065310185

¹ Dalby S, ‘Authenticity/Authentication Definitions and Sources’ Inter Pares Project (International Research on Permanent Authentic Records in Electronic System policy Cross-domain2004). www.interpares.org/...ws_macniel_claid_17_nov2005.pdf. Accessed on 6/10/2020.

2. Proof by Electronic Evidence

The underlying principle upon which the concept of weight of evidence is based is that the court is urged to confer probative value or otherwise on a document that is being tendered and received in evidence. An invitation to ascribe probative value on a document which is evidence before the court works on the assumption that the document has been admitted in evidence as an exhibit. This assumption or presumption is rebuttable as the admissibility of a document could still be a relevant factor in the course of final addresses, judgment or even on appeal.²

Two key factors are germane considerations in respect of electronic evidence in judicial trials or proceedings. These are admissibility and weight of documents. Whereas sections 83 and 84 of the Evidence Act³(hereinafter the Act) provide for admissibility of such document, section 34 seemingly governs the concept of electronic evidence in respect of weight.

The Evidence Act recognizes this fundamental fact and has provided in section 34 certain factors relevant to assessing the weight to be ascribed to computer-generated evidence. The Act also by implication recognizes that proof of documents accommodates both admissibility and probative value of the document. Section 86 requires that the contents of documents may be proved by primary or secondary evidence. This generally explains how a party can prove the contents of a document, however, there are other provisions⁴ that prescribe the conditions that must be satisfied before the document can be proved.

3. Admissibility and Weight Distinguished

In general terms the fact that a document is an evidence connotes that the contents of the document are evidence before the court, for the consideration of the court, but it does not amount however to conclusive proof of the fact in issue.

²*Kubor v. Dickson* (2013)4 NWLR (pt1345)534. In this case, electronic documents were received in evidence without objection by the Respondents in the tribunal. On appeal to the Court of Appeal, the issue of the admissibility of the electronic documents having regards to section 84 of the Evidence Act became a factor for consideration. This appeal was determined on the sole basis of non compliance with section 84 of the Evidence Act.

³ Evidence Act 2011 (CAP E14 2004).

⁴ Section 83 and 84 of the Evidence Act.

The courts have severally held that documentary evidence is of no probative value in the absence of the maker of the document⁵ or body to testify on the document⁶ and is subject to cross-examination.⁷ The courts usually will hold that such documents were dumped on the court⁸ or that the documents amounted to documentary hearsay.⁹ This is the general principle laid down in respect of paper documents. However, the effect of these principles or decisions on electronic documents remains controversial. There is no express provision of the Evidence Act that has the effect of excluding the applicability of such principles to electronic documents. It is therefore correct to argue that electronic documents will be subject to similar decisions and would require the presence of the maker or any person to lead evidence on the electronic documents.¹⁰

4. Authentication of Electronic Evidence

Authentication, according to Kurzban, is basically satisfying the court that the contents of the record have remained unchanged, the information in the record is derived from the purported source, whether human or machine and that extraneous information such as the apparent date of the record is accurate.¹¹ The authenticity of the document or record is based on a statement made by a person who vouches that the data is reliable and that same has not been tampered with. Kurzban's definition of the concept of authentication ably sets out what is expected of the person certifying the data as authentic and what the court called to receive or rely on the document is expected to look out for in determining the weight to be ascribed to such evidence.

In criminal proceedings, the charge substantially forms the basis for determining the relevance of a particular which the document seeks to prove. This is more as section 84 of the Evidence Act seemingly relates to the admissibility of computer-generated evidence. In a strict sense therefore section 84 provides for the admissibility of electronic evidence and thus by section 84(4) of the Evidence

⁵ Ikpeazu v. Otti (2016) 8 NWLR (pt 1513) 38.

⁶ Omisore v. Aregbesola (2015) 15 NWLR (pt 1482) 205.

⁷ Ogboru v. Okowa (2016) 11 NWLR (pt 1522) 84.

⁸ Ladoja v. Ajimobi (2016) 11 NWLR (pt 1519) 87.

⁹ Belgore v. Ahmed (2013) 8 NWLR (pt 1355) 60.

¹⁰ See Section 34 of the Evidence Act 2011.

¹¹ Kurzban AS, 'Authentication of Computer-Generated Evidence in the United State Federal Courts' <www.ipmall.info/..sted>resources/IDEA/16 .Accessed 7/10/2021.

Act, the requirement of authentication is satisfied and this concept should ordinarily cease to be of any material relevance once the document or evidence is received in evidence as an exhibit.

Section 84(2) and (5) of the Evidence Act prescribes the manner or requirements for the authentication of a document. Section 84(2) contemplates oral testimony of a witness to explain the identity, nature origin and relevance of the document. Authentication is a matter of fact and not of law. It may therefore be proved by oral evidence as provided by section 84(2), or, by a certificate as provided for in section 84(5) of the Evidence Act. These provisions are seemingly alternatives to the other. The strict perspective to the requirement of authenticity having regards to the requirement of certification will be that the certification must not only be in writing accompanying the electronic evidence.

The Supreme Court only recently had the opportunity to address this issue and resolved that the proof of authenticity of electronic evidence can be established by either reference to oral evidence or by a certificate. In *Dickson v Sylva*¹², his Lordship, Nweze, JSC. Opined that:

In actual fact, section 84 of the Evidence Act, consecrates two methods of proof, either by oral evidence under section 84 (1) and (2) or by certificate under section 84 (4). In either case, the conditions stipulated in section 84(2) must be satisfied. However, this is subject to the power of the judge to require oral evidence in addition to the certificate.

His lordship placed reliance on the decision of Lord Griffiths in *R v. Shephed*¹³, wherein he said;

Proof that a computer is reliable can be provided in two ways: either by calling oral evidence or by tendering a written certificate subject to the power of the judge to require oral evidence.

¹² (2017)8NWLR(pt1567)167at203.

¹³ (1993)1 ALL ER225.

In contrast, the Indian position regarding electronic evidence does not support the above view. Karia¹⁴ placed reliance on the position of the Supreme Court of India, which had in the case of *Anvar PK v. Basheer&Ors*¹⁵, overruled the decision in the case of *Navjot Sandhu*¹⁶, and held that electronic evidence must be accompanied by the certificate in terms of section 65(b) obtained at the time of taking the document. By this decision, the Supreme Court of India, by re-interpreting the application of sections 63 and 65 of the Evidence Act correctly reflected the letters of the Evidence Act, thus redefining the evidentiary admissibility of electronic records. It is important to reiterate the fact that the provisions of the Nigerian Evidence Act are substantially in particular with the Evidence Act, applicable in India. The Judicial approach of the courts in India will be a relevant factor in determining the applicable principles in Nigeria. Under the Australian Evidence Act, Authenticity seems to be a principle more for the ascription of the weight of evidence. Thus, in *Australian Competition and Consumer Commission v Air New Zealand Ltd (No2)*¹⁷, Perram J Stated that:

....there is no provision of the Evidence Act which requires that only authentic documents be admitted into evidence. The requirement for admissibility under the Act is that evidence is relevant, not that it is authentic.

Thus, on some occasions, the fact a document is not authentic will be what makes it relevant, i.e; in a forgery prosecution. The complexity of the device and evidence will determine the nature of the weight to be ascribed to the evidence.

4.1. Electronic Mail (E-Mail)

Email messages represent personalized messages or communications between the addressee and the sender. The primary means of authenticating email messages is by evidence of the recipient of the sender. The authentication can be by direct

¹⁴ Tejas Karia, Akhil Anand and Bahaar Dhawan, 'The Supreme Court of Indian re-defines the admissibility of electronic evidence in india' Digital Evidence and Electronic Signature Law Review(12(2015)37.

¹⁵ (2014)10 SCC473.

¹⁶ (2005)11SCC600.

¹⁷ (2012)FCA1355(30 November2012)cited in Standfield, AR 'Authentication of Electronic <Evidence>'eprints.qut.edu.au/.../1/Allison standfield-thesis .pdfaccessed on 28/10/2020>.

or circumstantial evidence. This may be by the appearance, contents, substance, internal patterns or other distinctive characteristics taken in conjunction with circumstances.

O' Donnell¹⁸ posits that evidence in support of the authenticity of emails could be by affidavit. In his view in several instances, courts have excluded e-mail evidence not because the e-mail was clearly inauthentic, but because the evidence was not submitted to support its authenticity in the face of a challenge.

Guy¹⁹ identified different methods by which e-mails can be authenticated for admissibility purposes. These include; by any of the following by

- i) Authentication, which may be through the evidence of the sender or recipients of the email message;
- ii) Evidence as to the integrity or trustworthiness of the email system, process or sever “describing a process or system and showing that it produces as an accurate result”.

There is no doubt that there are different means by which emails can be proved in evidence. Guy's view falls into the category of the prominent means of proof of email messages. These are similarly applicable to electronic evidence in general. Section 84(2) and (4) of the Evidence Act, set out the requirements to be met for authentication of electronic evidence in general. Emails being a species of such evidence will conform to the proscription set out therein²⁰. This presumption is rebuttable. It is necessary to note that this presumption relates only to the nature of message transmission in terms of the content. The presumption does not extend to the delivery of the message. Thus the court will not presume that the electronic message was delivered to the person to whom it is addressed. The presumption raised by this provision relates therefore to the integrity of the content of the message as it the fed into the computer of the originator thereby eliminated by a third party in the message.

4.2. Text Messages

¹⁸ O'DonnellB, 'Authenticating Email Discovery as Evidence
<<http://www.depo.com/authenticity-email.html>> accessed on 18/10/2018.

¹⁹ Guy RT, 'Effective Use of Email Messages in Witness Examination
'<https://www.bng.com/effective-ofe-mail-messages-in-witness-witness-examination> accessed on 12/12/2018.

²⁰ See section 153(2) Evidence Act 2011.

Text messages are messages transmitted by personalized cellular phones. The authentication process for text messages is similar to E-mail. Authorship of the text message is fundamental to the authenticity of the message. Ownership of the cell phone from which the message is sent is prima facie evidence or proof of the authorship of the message. Circumstances that will justify ownership range from proof of previous exchanges of communication between the parties, to the contents of the text messages showing that the parties are conversant with the matter discussed.

The weight to be placed on such electronic evidence in respect of text messages will be determined by the strength of the proponent of the evidence being able to satisfy the requirement of authenticity, reliability, and confidentiality, and raise the presumption that the author of the text message is the owner of the cellular number used to send a message. Where the opposing party is unable to lead evidence impeaching any of the elements in section 34(1) (b) (c)(i) (ii) and section 83(5) of the Evidence Act, or that the document does not satisfy the elements of confidentiality, integrity, and authenticity, such document or evidence will not be ascribed weight.

Section 34 of the Evidence Act empowers the court to take into account circumstances as may be appropriate in determining the weight to be ascribed to electronic evidence. The court will therefore be entitled to place reliance on evidence showing that a text message or email message does not bear the addresses of the sender, does not contain the signature of the sender, or does not bear an internet protocol (IP) address.

4.3. Computer- Stored Documents

These are documents stored in the computer system from which the same is generated as a hard copy. These stored documents are retained information in the hard or software of the system. The documents or information could sometimes be deleted from the system, but still retained in the memory of the system. The authenticity of such information or document can be made by a witness who can testify as to his seeing the information or document in the computer system. There is no express or specific provision in the Evidence Act setting out factors that will qualify for the authentication of such document.²¹

²¹ Pendleton A, Admissibility of Electronic Evidence: A New Evidentiary frontier
mnbenchbar.com/...admissibility-of-electronic-evidence. Accessed 29/10/2018.

Instructively, Pendleton draws a fine distinction between computer-stored documents and computer-generated documents. This follows that they are not the same. In his view, computer-stored documents are entirely statements by persons and, if offered or proven their truth, can be considered hearsay. However, because computer-generated materials are not statements by persons, but rather are the product of the machine itself operating according to a program, they do not fit the definition of “hearsay”.²²

4.4 Automated Teller Machines (ATM)

Nwamara²³ defines an Automated Teller machine as a device by which a person can obtain access to his account remotely by undertaking a number of transactions in the nature of such as cash withdrawal, money transfers between accounts, and obtaining a balance of the account to pay for goods and services. Automated Teller Machines and the data or information contained therein are similar products of electronic devices and therefore electronic evidence. By the nature of their functions or operations, ATMs are mainly for the purpose of dispensing cash to customers. Thus, as a corollary to the efficient performance or security of such devices, there are attached to such ATM premises video recording (CCTV) of transactions. These video recordings help in ascertaining specific transactions where the issues arise regarding the authenticity of who actually undertook a particular transaction.²⁴

These devices are self-activating and the question of authorship of the transactions carried out through the device will not be resolved as in the case of text or email messages. The required evidence will therefore be that of the bank through its officer as in the case of other electronic evidence emanating from the bank. The evidence of authentication therefore will emanate from the bank.

4.5. Social Networks Messages

Social networks are websites created and permitting members of the site to share information or posts with others who may not necessarily be members of the site. These posts or information posted by members such as photographs, videos, and

²² Ibid.

²³ Nwamara T A & Nwosu C, Law of Electronic Evidence in Nigeria, Aba, Law and Educational Publishers Limited, 2012.315.

²⁴ *Agi v. Access Bank* (2014) 9NWLR (pt1411) 121.

personal information or message received from other platforms may be shared. The point should be stressed here that this shared information may not represent the truth of the fact shared. They could also constitute the basis of offences committed contrary to penal laws. Proof of these writings in civil and criminal trials will be required as evidence. Such evidence can only be retrieved from the websites upon which they were posted. Proof of authorship of the post can be established from the evidence of a participant of the network identifying the person who posted the information by the name used to identify him and the accuracy of his posting with a person so identified.

4.6. Data & postings

These are information appearing on websites. They could be posted on private (individual or corporate) or government sites. For purpose of proof, the printout of such webpages is admissible upon due authentication as electronic evidence. As in other types of electronic evidence, the opposing party is at liberty to lead contrary evidence to impeach the genuineness of the system or the information posted therein. There are nothing specifically delimiting categories of postings and the nature of evidence required to prove, challenge or rebut the evidence proffered in support of the posting.

On the other hand in respect of private websites, additional proof of authentication shows the origin of the post and the means by which the information was generated or produced. Evidence of the authenticity of the website can be preferred by the manager of the website who will lead evidence to establish the time the information was posted.

Pendleton²⁵ considered four steps as an analytical framework for the admissibility of website data, social network communications, postings, email, text messages and computer-stored/Generated Documents. These four steps were categorized as:

- i) Authenticate or identify,
- ii) Hearsay or Not
- iii) Relevant and not unfairly prejudicial
- iv) Not privileged communication.

²⁵ Pendleton(n21).

Whereas these concepts may literally seem relevant only to the issue of the admissibility of e-documents, the consideration of these concepts impact also on the weight to be placed on such documents. In this regard, therefore, it follows that the admissibility of the e-document does not render these concepts inconsequential when the weight to be ascribed to the document calls for consideration of judgment by the court. The relevance of admissibility therefore in respect of considering the principles or the rules behind the concepts is for the sole purpose of ascertaining whether the documents can be allowed for consideration before the probative value become a factor for consideration. Notably Common to each of these means of communication. Text messages, Emails, and website data are the possibility of manipulation by third parties. This, therefore, raises the issue of authorship of such documents, hence the requirement for the authentication of these documents.

5. Weight of Electronic Evidence Under the Evidence Act

Once electronic evidence is admitted in the course of trial, the judge is obliged to determine the evidential weight to ascribe to the evidence. This is also known as the probative value of the evidence. This usually is ascertained or assessed in the course of the judgment of the court during the period of evaluating the evidence before the court²⁶.

Section 34 of the Evidence Act provides in general terms rules applicable to assessing the weight of evidence. According to Mgbeahuru,²⁷ the purpose of section 34 (1) (b) (i) (ii) is to eliminate the possibility of giving weight to an accurate document or anonymous fabrication.

Citing the case of *Ekiti Independent Electoral Commission v. PDP*²⁸, where Onyemenana, JCA, decided the possibility of easy manipulation with modern information communication technology, Mgbeahuru opined that there is no gainsaying that electronic evidence can be fraudulently created, tampered with, or manipulated²⁹. Accordingly, section 34(1) (b) of the Act, makes

²⁶ Okoreaffia & Anor v. Agwu & Anor (2008) 12 NWLR (pt 1100) 165. See also section 34 of the Evidence Act 2011.

²⁷ Mgbeahuru UM, 'Documentary Admissibility in a Frontloading Regime Paper and Digital Perspective' Lagos, Lyon Quest Frontiers Ltd 2016. 366.

²⁸ (2013) LPELR 20311.

²⁹ Mgbeahuru (n26) 366.

provision for the factors considered in determining what weight is to be ascribed to oral and documentary evidence.

The applicability of different approaches in determining the weight to ascribe to each type of electronic evidence, will therefore be based on the power or discretion conferred on the court by section 34 of the Act. Judicial decisions seem to support the view that different approaches are applicable. In *Lorraine v. Markel American Ins Co*³⁰, the court expressed the view that:

...as with the authentication of any kind of profound evidence, the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstance of the particular case.

6. Circumstances Which May Affect Accuracy

The Evidence Act in general terms sets out factors to be considered by the court in determining the evidential value of the evidence, either oral or documentary. Sections 34 in general terms also empower the courts to have regard for all circumstances. Such circumstances must however be for the purpose of drawing an inference or making deductions as to the accuracy of the statement contained in the document. Therefore, every circumstance which forms the basis of the inference of the court must be shown to have an effect on the possibility of affecting the accuracy of the statement. There is no requirement of any actual fact. Where such facts exist and the court can draw its inference as to the effect on accuracy, the court is entitled to place reliance on such as a basis for justifying the weight to be ascribed to such evidence.

In respect of computer evidence, it is incumbent on the court to have recourse to such inference but not limited to the factors set out in subsection (b) of section 34 which deals with the circumstances, existence, or otherwise of the contemporaneity of the making of the statement.

7. Supply of the Evidence to the Computer Contemporaneously With Fact in Issue

In determining the weight ascribable to an electronic piece of evidence, the court will need to take into account as part of the circumstances surrounding the

³⁰241 FRD.534at544(Dmd2007)<<https://casetext.com/case/Lorrainev.marketLorraine-americanins-co>>assessed on 26/10/2021.

provenance of the document, and the time of making the document. It is important to note that section 34 requires that this circumstance be read conjunctively with the requirement of the creditability of the person recording the event or inputting the data.

In interpreting the purport section 34, Amupitan³¹ opines that the court must take into consideration the accuracy or otherwise of the evidence, the contemporaneousness evidence with the facts stated and whether the maker had any incentive to conceal or misrepresent facts.

In addition to determining the timing of the document origin and the data inputted, by the court will have to further ascertain the role of the person recording the information- as an eyewitness or based on facts within his knowledge or based on information supplied to him. In each of the roles of the person recording or inputting the data, the basic consideration is whether the person is credible. The credibility of the person will be assessed on the strength of his disposition to conceal information.³²

8. Oral Evidence to Support Electronic Evidence

The effect of tendering electronic evidence without the maker testifying and being subjected to cross-examination with regard to the weight to be attached to it is for the purpose of ascertaining the truthfulness or veracity of the contents of the document.³³

8.1 Production of Evidence

The Rules of Court make provisions for different means by which action can be commenced. This is substantially a matter of procedure. The Evidence Act does not however seem to accommodate the respective means or procedure of trial. Whereas where pleadings are involved, it is generally understood that in the course of trial oral evidence will be adduced and the requirement of admissibility of electronic evidence will become a relevant factor in the course of tendering such evidence, this is not generally the case in proceedings conducted by affidavit evidence, such as Originating Summons, Petitions, Motions and the like.

³¹ Amupitan JO, Evidence Law: Theory and Practice in Nigeria(Innovative Communications2013)417.

³²See sections 84(3) (4) and 34 of the Evidence Act 2011.

³³ A.G Oyo State&Ors v. Fairlakes Hotels Ltd& Anor (1989)5NWLR (pt121)255, and also section 84 of the Evidence Act.

9. Conclusion

No evidence, Oral, documentary, or electronic is produced for the fun of it. Every piece of evidence is expected to establish or prove the case of the party. A party relying on the pieces of evidence does so believing that it will prove a fact in issue between the parties. The same proposition applies to electronic evidence.

The Evidence Act expressly provides for matters required to prove the admissibility of computer evidence. These factors can be surmised as authenticity, reliability, and integrity. These factors are expected to be established or proved by the party proposing or relying on the electronic evidence. The party opposing the admissibility is restricted to taking objection to the non-existence of the factors and not otherwise.

While the Act creates a general framework regarding the weight to be attached to such electronic evidence, it does not set out any basis for the opposing party to be able to show that the produced electronic evidence falls short of any of the above factors for probability. The challenges a party seeking to show that the produced electronic evidence is not probable are enormous. Implicit in the factor for admissibility is the confidentiality of the electronic evidence. Where the electronic evidence cannot be verified to be confidential in the sense that it is not easily accessed by a third party without authority, such evidence is not likely to be admitted as this will affect the integrity test.

The same factors will form the basis for a challenge to the weight of such evidence. Where a party seeks to show that particular electronic evidence lacks confidentiality or its integrity cannot be substantially guaranteed, this will affect the weight the court will ascribe to such a piece of evidence. It must be noted that this is no mean task, as it is more difficult to detect where the product of an electronic device has been tampered with. The chance that the courts are more likely to be misled by evidence produced through an electronic device is higher than when a hard copy of the evidence is used.