ARTICLE :

An analysis of the judicial and legislative attitude to hearsay electronic data in South Africa

By Rilwan Mahmoud

Introduction

The South African procedural rules make a clear distinction between items of evidential value as either: an object that bears marks, symbols or writing (documentary evidence); or objects that fall outside this category, (real evidence).[1] Evidence is typically classified under one or more of three headings: as an object (real evidence), as a document (documentary evidence), or evidence from a witness (oral evidence).[2] South African jurisprudence considers that anything that contains the written or pictorial proof of information, regardless of the nature of the material upon which it has been printed or depicted, falls in the exclusive category of documents.[3] This group of items includes recordings, maps, photographs and a coin.[4] This has led to the definition of a document being held to be wide enough to include electronically generated computer printouts.[5] The rapid developments in the field of technology have caused several issues to be raised as to what category electronic evidence fits in for the purpose of determining admissibility and weight because 'the legal system does not always keep up with the pace of technological development'.[6] One unavoidable implication of this limitation on the South African judicial system is an exercise of extreme caution in the use of and value to be placed on evidence in electronic form.[7]

This paper examines the adequacy of the South African law of evidence by highlighting the legislative and judicial transition in dealing with the admissibility and weight to be accorded to electronic evidence.

Judicial attitude towards electronic data before the Computer Evidence Act

Prior to the codification of the Civil Proceedings Evidence Act 25 of 1965 (CPEA) and the Criminal Procedure Act 51 of 1977 (CPA), South African courts deliberated on electronic evidence. In *Balzan v O'Hara*,[8] the court was faced with determining whether a telegram constituted a written authority within the definition in section 1(1) of the Land

[1] D Van der Merwe, 'A Comparative overview of the (Sometimes Uneasy) relationship between digital information and certain legal fields in South Africa and Uganda', PER/PELJ (2014) 17(1), http://www.scielo.org.za/pdf/pelj/v17n1/08.pdf.

[2] P J Schwikkard and S E Van Der Merwe, *Principles of* Evidence (4th edn, Juta & Co Ltd Cape Town, 2016), 437-446. See, for example: *S v Brown* [2015] ZAWCHC 128 at [18]; *S v Meyer* [2017] ZAGPJHC 286 at 296-310.

[3] *Seccombe v Attorney General* 1919 TPD 270, at 272, 277-278; G P Van Tonder, 'The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective', a th s submitted in partial fulfilment of the requirements for the LLM degree in the Faculty of Law of the University of the Western Cape (2013), 18.

[4] *Protea Assurance v Waverley Agencies* 1994 (3) SA 247 (A) 249H I.

[5] *S v Harper* 1981 (2) SA 88 (D) 96C F.

[6] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', JILT 2009 (1), https://warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/watney .

[7] D Collier, 'Evidently not so Simple', (2005) *The Quarterly Law Review for people in business*, Vol 13(1). There have been numerous calls for the education of judges and lawyers on electronic evidence, in particular, Denise H Wong, 'Educating for the future: teaching evidence in the technological age' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 16 and Deveral Capps, 'Fitting a quart into a pint pot: the legal curriculum and meeting the requirements of practice' (2013) 10 *Digital Evidence and Electronic Signature Law Review* 23, https://journals.sas.ac.uk/deeslr/issue/view/310 .

[8] 1964 (3) SA (T) 1. See also, *Hersch v Nel*, 1948 (3) S.A. 686 (A.D.); *Luttig v Jacobs*, 1951 (4) S.A. 563 (O.P.D.) extensively discussed in Stephen Mason, *Electronic Signatures in Law* (4th edn, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2016), Electronic Signatures in Law: Fourth Edition | Humanities Digital Library (humanities-digital-library.org), 1.144.

Alienation Act in 1964.[9] The court opined that the telegram indeed constituted 'written authority' within the meaning of the section but only if the contract, which was concluded by the agents in this case, was a contract upon which they had the right authority to conclude on behalf of their principal; that is, one which the principals were authorized to conclude.[10] The content of the telegram was considered by the court to be a hearsay statement and common law principles of hearsay were applied to it.[11] The telegram in the *Balzan* case was examined under the common law classification of evidence and could only have fallen into one of three categories; oral, documentary and real evidence. The court elected to treat it as documentary hearsay because it was presented to the court for the purpose of proving the truth of its content. Where the individual who made the statement is not available on account of not being a party or not being called as a witness, it is deemed hearsay under the common law.[12]

The application of common law principles to address issues of documentary evidence and rules regulating the admission of hearsay was addressed in *Vulcan Rubber Works (Pty) Ltd v South African Railways and Harbours.*[13] In that case, a statement was tendered as evidence by an official in charge of the harbour, stating that the department had made certain investigations to trace the appellant's bales of rubber. The court, relying on the common law principle that hearsay evidence can be admitted if it falls within a list of exceptions, excluded the evidence because the official's statement about the reports that he had received from other harbour officials, was hearsay in nature.[14] It fell into this category because it was a statement tendered to prove the truth of the matters stated in it, and was made by a person who was not a party to the case and was not called as a witness.[15]

The need to codify evidentiary procedural rules to address these issues became apparent. This led to the introduction of the CPEA. The legislation was modelled after the old English Evidence Act of 1938 and was drafted before the prominence of, and with little consideration of, electronic devices.[16] This was followed by both the CPA and the Law of Evidence Amendment Act 45 of 1988 which were necessary additions to the rules of procedure of South Africa (Law of Evidence Amendment Act (subsequently referred to as 'EAA')).[17] Perhaps because electronic devices were not nearly as popular then as they are today, the CPEA contained little or no direct legislation on the evidence of an electronic nature. The relevant references to the nature of evidence in the CPEA was the definition of a document which included, books, maps, plans, drawings, and photographs. Also, in this regard, the CPEA defined a statement as a representation of facts, whether made in words or otherwise.[18] The CPEA also stated that in any civil proceedings any statement made by a person in a document tending to establish that fact shall, upon production of the original document, be admissible as evidence of that fact.[19] Section 34 of the Act included a proviso requiring that the person who made the statement either had personal knowledge of the matters dealt with in the statement or made the statement in the performance of a duty to record information supplied to him by a person who had personal knowledge of the matters made in the statement.[20] Section 34(4) states as follows:

> 'A statement in a document shall not for the purposes of this Section be deemed to have been made by a person unless the document or the material part thereof was written, made or produced by him with his own hand, or was signed or initialled by him or otherwise recognized by him in writing as one for the accuracy of which he is responsible.'[21]

[9] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues' (Issue Paper 27, Project 126, 2010).
[10] South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010).
[11] South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010).
[12] *S v Holshausen* 1984 (4) SA 852 (A).
[13] 1958 3 SA 285 (A).
[14] *S v Holshausen* 1984 (4) SA 852 (A).
[15] *S v Holshausen* 1984 (4) SA 852 (A).
[16] D Van der Merwe, *Information and Communications Technology Law* (LexisNexis, Durban, 2008), 122.
[17] D Van der Merwe, *Information and Communications Technology Law*, 122.
[18] Section 33 CPEA.
[19] Section 34(1) CPEA.
[20] CPEA, sec 34.
[21] CPEA, sec 34 (4).

An apparent trait of these rules was the presumption that all documents must be made by a person and the admissibility of documents was heavily predicated on that presumption.[22] On the estimation of the weight to be attached to them, the CPEA reflects the same attitude thus:

> 'Section 35(1) In estimating the weight to be attached to a statement admissible as evidence regard shall be had to all the circumstances from which any inference can reasonably be drawn as to the accuracy or otherwise of the statement, and in particular to the question of whether or not the statement was made contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not the person who made the statement had any incentive to conceal or misrepresent facts.'[23]

The enactment of the CPA brought about a much wider definition of a 'document'.[24] Its definition included 'any medium upon which information is created and preserved'.[25] The CPA also defined documents in relation to entries in accounting records to include a 'recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored'.[26] The provisions of sections 33 to 38 of the CPEA also applied to criminal proceedings.[27] The implication that the admission of evidence in electronic form is contingent on a personal link to the evidence will necessarily make all electronically generated evidence fall under the class of hearsay evidence. The EAA redefined hearsay evidence to be evidence of which the weight to be ascribed to it is predicated upon the credibility of an individual other than the person presenting such evidence to the court.[28]

The EAA also provided exceptions to inadmissible hearsay evidence in both civil and criminal proceedings. These exceptions are (i) instances where each party against whom the evidence is sought to be used, agrees to the admission of it,[29] (ii) where the person whose credibility is required for the ascription of probative value to the evidence, testifies at the same proceedings, and (iii) where the court is convinced that admitting the evidence (although it is hearsay) will be in the ultimate interest of justice.[30] In reaching this conclusion, the factors a court is required to consider include: the type of proceedings, the classification of the evidence, the reason that the evidence is being presented, the ascription value of the evidence, the purpose for which the evidence is not tendered by the individual upon whose credibility the weight of the evidence is predicated on, any prejudice that a party might incur upon the admission of the evidence, and other factors which should be taken into account.[31]

Before the enactment of the Computer Evidence Act (CEA), the admissibility and weight to be accorded to electronic evidence were not issues that had been addressed in legislation. However, courts had to deal with evidence in electronic form in several cases, which in turn highlighted the insufficiencies of both the CPA and the CPEA in this regard.[32] It became apparent that it might be absurd and counterproductive to apply certain documentary rules to computer generated evidence as well as to consider a computer as a document based on the definitions in both the CPA and CPEA.[33] In *Narlis v South African Bank of Athens*,[34] Holmes JA identified the difference between electronically generated evidence and documentary evidence by his famous words, 'a computer, perhaps, fortunately, is not a person'.[35] In this case, the court considered whether section 34 of the CPEA provided for the

[22] CPEA, sec 33 and 34.
[23] CPEA, sec 35(1).
[24] The Criminal Procedure Act 51 of 1977.
[25] CPA, sec 221(5).
[26] CPA, sec 236(6).
[27] CPA, sec 222.
[28] Section 3(4) Law of Evidence Amendment Act 45 of 1988.
[29] EAA, sec 3(1)(a).
[30] EAA, sec 3(1)(a).
[31] EAA, sec 3(1)(a).
[32] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A) at 577 and *S v Harper* 1981 (2) SA 88 (D) 96C F. In both cases, the application of rules of documentary evidence as well as the nature of a computer and its printouts were addressed.
[33] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A), at 577.
[34] 1976 (2) SA 573 (A).
[35] *Narlis v South African Bank of Athens*1976 (2) SA 573 (A), at 577. This distinction does not take into account the nuances of evidence in electronic form, as set out in chapter 4 'Software code as the witness' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures* (5th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School

admissibility of statements in computer printouts, in particular, computer printouts of bank statements.[36] The bank wanted to use the entries in its banker's book as evidence to show that an overdraft facility had been granted. The court examined the validity of the ledger cards and statements and considered them in terms of section 34(4) of the CPEA which states that:

> '[A] statement in a document shall not for the purposes of this Section be deemed to have been made by a person unless the document or the material part thereof was written, made or produced by him with his own hand, or was signed or initialled by him or otherwise recognized by him in writing as one for the accuracy of which he is responsible.'[37]

The court decided that a bank statement stored on an electronic device did not fulfil the admissibility requirements because it cannot constitute a statement in a document made by an individual.[38] Whether computer printouts are documents within the meaning of 'document' in section 221(5) of the CPA, the scope of the definition of a document and the extent of its application were also considered in *S v Harper.*[39] On the question of whether the definition of a document under section 221 of CPA includes a computer printout of information recorded and stored on a computer in the course of a business,[40] Milne J held as follows:

> '[T]he computer print outs consist of typed words and figures and would, *prima facie*, clearly fall within the ordinary meaning of the word document... It seems to me necessarily envisaged that, because of the development of modern commerce and the necessity to store records relating to large sums of money and large numbers of people, special provisions would have to be made making evidence admissible that would not be able to be subject to the ordinary rigorous test of cross examination. In so doing the Legislature has, in addition to stipulating compliance with the above pre requisites [in terms of s 221], also enjoined the matters which are to be taken into account in estimating the weight to be attached to the statements, and I refer to the provisions of ss (3). It seems to me, therefore, that it is correct to interpret the word "document" in its ordinary grammatical sense, and that once one does so the computer printouts themselves are admissible in terms of s 221.'[41]

Another question that was considered in this case was whether the definition of a document in the CPA, which is much wider than the CPEA (this is peculiar – if anything one would expect the civil position to contain a broader definition) and includes 'any device' by which information is recorded or stored,[42] includes a computer itself.[43] On this, Milne J opined as follows:

> 'The extended definition of "document" is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than mere storage or recording of information… Even if the Section could be interpreted to mean that what must be produced is that part of the computer on which information is recorded or stored, that would mean the tape or disc on which it was stored, and this would be meaningless unless the electronic impulses on that tape or disc were to be translated or transcribed into a representation or statement intelligible to the ordinary human eye – or perhaps ear. The Section does not refer to the product of the device, nor does it refer to any document produced by the device, it refers to the document itself being produced.'[44]

Following the establishment of the South African Law Reform Commission in 1973 (by the South African Law Reform Commission Act 19 of 1973), the review of the rules of evidence was set into motion with the primary intent of

---

of Advanced Study, University of London, 2021), Open Access at https://humanities-digital-library.org/index.php/hdl/catalog/book/electronic-evidence-and-electronic-signatures .

[36] *Narlis v South African Bank of* Athens 1976 (2) SA 573 (A), at 577.

[37] Section 34(4) CPEA.

[38] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).

[39] 1981 (1) SA 88 (D) 95.

[40] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).

[41] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).

[42] CPA, sec 221(5).

[43] *S v Harper* 1981 (2) SA 638 (D).

[44] *S v Harper* 1981 (2) SA 638 (D).

codifying 'the law of evidence of South Africa and to unify it all under one statue.'[45] The Commission soon realized the impracticality of a complete overhaul of the law of evidence, noting that attempts in other jurisdictions to enact a law regulating electronic evidence have required much more money and expert involvement than what was readily available to the Commission.[46] The Commission then decided to ascertain which aspects of the law of evidence were unsatisfactory and to formulate suggestions for their reform.[47] In April 1982, the South African Law Commission reviewed the admissibility of computer generated evidence and published the 'Report on the Admissibility in Civil Proceedings of Evidence Generated by Computer: Review of the Law of Evidence' (Project 6, April 1982).[48]

In acknowledging the degree of the reform required, the Commission considered the possibility of amending section 34 of the CPA to include the admissibility of electronic records. It also acknowledged that a solitary amendment such as this would not address all of the issues surrounding the admissibility of electronic records.[49] The report recommended that specific provision should be made for computerized records which were reflected in the draft bill proposed by the Commission.[50] The report was presented to the Minister of Justice, and the CEA – largely based on the draft bill proposed by the Commission – entered into law.[51] The CEA was, however, only applicable to civil proceedings.[52]

The reception and challenges of the Computer Evidence Act

The CEA required that for a computer printout to be admissible as evidence and for sufficient weight to be attached to it, such a printout must be presented with an affidavit for the purpose of authenticating it.[53] The purpose of the affidavit was to authenticate the computer printout.[54] The authenticated computer printout became a form of a document.

The authenticating affidavit was required to include the following:

> (i) confirmation that the computer printout in question had been produced by a computer;
>
> (ii) the veracity of additional information describing the nature, sources, and purpose of the data from the computer;[55]
>
> (iii) certification that the computer was accurately supplied with the information recorded in the printout;
>
> (iv) the computer was not affected by any malfunctions and disturbances that may have altered the data on the printout so as to affect its reliability, and
>
> (v) that no other reason has presented itself to question the probity and reliability of the information reflected on the printout.[56]

The deponent to the authentication affidavit was required to state their knowledge and experience of computers, particularly regarding the daily operation of the computer in question.[57] The deponent was also required to show

[45] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[46] South African Law Commission Report, Project 6 Review of the Law of Evidence (October 1986), [1.1]-[1.2].
[47] South African Law Commission Report, Project 6 Review of the Law of Evidence (October 1986).
[48] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[49] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[50] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[51] South African Law Reform Commission Report, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues', paragraph 5.
[52] South African Law Reform Commission Report, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues', paragraph 5.
[53] Section 1 CEA, 1983.
[54] Section 1 CEA, 1983.
[55] Section 2(1) CEA, 1983.
[56] Section 2(1) CEA, 1983.
[57] CEA, sec 2(3).

that he had access to and control of the computer during the ordinary course of business and employment and if not, it was necessary for the individual with control and access of the computer at the time in question and in the ordinary course of his business to provide an additional affidavit.[58]

On the admissibility of the authenticated computer printouts in civil proceedings, the CEA provided as follows:

> '3(1) In any civil proceedings an authenticated computer printout shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible...
>
> (2) It shall suffice for the purposes of Subsection (1) if an affidavit which accompanies the computer printout in question as contemplated in the definition of 'authenticated computer printout' in Section 1 (1), on the face of it complies with the provisions of Section 2 which apply to an affidavit of the nature in question.'[59]

The CEA also provided for the evidential weight of computer printouts once they had passed the hurdle of authentication and admission by providing as follows:

> '4(1) An authenticated computer printout shall have the evidential weight which the court in all the circumstances of the case attaches to it ...
>
> (2) In order to assess the evidential weight of an authenticated computer printout, the court may (a) take account of anything contained in the authenticating affidavit or a supplementary affidavit; (b) on the application of any party to the proceedings require the deponent to the authenticating affidavit or a supplementary affidavit or any other person to testify orally on any topic relevant to such question, whether or not any such affidavit covered it'[60]

It soon became apparent that the intent of the drafters of the CEA to simplify and streamline the rules regulating admissibility and weight to be attached to electronic evidence was compromised, mainly due to an overcautious attitude in requiring a higher level of authentication.[61] Such over caution only perpetuated the myth of untrustworthiness of electronic information by the judicial system. Storm puts it thus:

> 'Requiring an extensive and technical foundation as a prerequisite for admissibility only perpetuates the judicial myth that electronic record systems are inherently less trustworthy than conventional systems. It increases the complexity of trials and diminishes efficiency in judicial rulings on admissibility. It also unfairly burdens the proponent of a computer record.'[62]

The CEA only applied to civil proceedings. This necessitated several calls for legislation relating to the admissibility of computer evidence in criminal proceedings.[63]

Another area on which the CEA failed to shed light was a computer's ability to create and analyse data messages with little or no human influence even though the CEA defined the term 'processing' to include 'treatment by calculation, compilation, arrangement, sorting, comparison, analysis, synthesis, classification, selection, summarising or consolidation.'[64] Regardless of the recognition by CEA of the function of processing, it still required authentication of a printout and an authenticating affidavit for all computer generated evidence.[65] This did not seem to affect the courts' recognition of such types of evidence, because it was held in *S v Fuhri*[66] that a photograph of a car whose

[58] CEA, sec 2(4); the control of computers by IT staff does not demonstrate the evidence adduced is accurate or truthful, for which the see the British Post Office Horizon scandal, discussed in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapter 5, 'The presumption that computers are 'reliable'' generally, and in particular at 5.165-5.170 and 6.55-6.56.
[59] CEA, sec 3.
[60] CEA, sec 4.
[61] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 8.
[62] P M Storm, 'Admitting computer generated records: A presumption of reliability', 18 J. Marshall L. Rev. 115 (1984-1985), 153.
[63] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[64] Section 1 of the Computer Evidence Act 57 of 1983; see S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapter 4 for a more detailed analysis.
[65] CEA, sec 1.
[66] 1994(2) SACR 829 (A).

owner had violated a traffic rule constituted real evidence, whereas in the case of *S v De Villiers*[67] the court found that an electronic printout that contained information in the form of data where the information was created by a human being was a document.[68]

This issue was brought to light and addressed in some detail in *Ex Parte Rosche*.[69] In this case, the telephone company's printout consisted of information about telephone calls automatically generated for all telephone calls made by subscribers. This case focused on one telephone call made from a hotel in Mozambique to a guest house in South Africa.[70] In determining the reliability of the printouts, the court examined the information contained in handwritten records of the calls, which were duplicates of the transcripts of the conversation between the callers generated by the telephone operator who was available on the day in question. The transcripts on the duplicates contained the same information as that on the printouts, although the operator was not available as a witness during the trial.[71] Evidence of the functional workings of the telephone recording equipment, as well as evidence of the reliability of the information contained in the printout, were also provided.[72] Although the court reached the conclusion that the provisions of the CEA had not been met, it accepted the printout as real evidence holding that:

> 'The printout is real evidence in the sense that it came about automatically and not as a result of any input of information by a human being. There is, therefore, no room for dishonesty or human error.'[73]

In reaching this conclusion, the court interpreted the statute liberally and held:

> 'In our view, a reading of the statute makes it plain that the statute does not require that whatever is retrieved from a computer can only be used if the statute's requirements have been met. It is a facilitating Act, not a restricting one.'[74]

The several other functions of a computer other than recording and storing information were also recognized in the case of *S v Mashiyi*[75] where the dictum of Milne J in *S v Harper*[76] was considered in excluding computer printouts that bore information that was retrieved after the process of sorting, calculations and other forms of alteration by the computer.[77] Milne J observed:

> 'Computers do record and store information but they do a great deal else; *inter alia*, they sort and calculate information and make adjustments. … The extended definition of "document" (in ss (5)) is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than their mere storage or recording of information.'[78]

Although the application of this dictum in the case of *S v Mashiyi*[79] has been criticized as being too narrow,[80] it became apparent that a legislative review on the nature of, admissibility, and weight to be accorded to,

[67] 1993 (1) SACR 574 (Nm).
[68] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position'.
[69] [1998] 1 All SA 319 (W).
[70] South African Law Reform Commission Report Review of the law of Evidence, Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[71] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[72] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[73] *Ex parte Rosche* [1998] 1 All SA 319 (W), at 321.
[74] *Ex parte Rosche* [1998] 1 All SA 319 (W), at 321.
[75] 2002 (2) SACR 387 (Tk).
[76] *S v Harper* 1981 (1) SA 88 (D), at 259.
[77] 2002 (2) SACR 387 (Tk).
[78] *S v Harper* 1981 (1) SA 88 (D), at 259.
[79] 2002 (2) SACR 387 (Tk).
[80] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.

electronically generated evidence was necessary.[81] The legislation came in the form of the Electronic Communications and Transactions Act (ECTA).[82]

The application of the ECTA in determining the admissibility and weight of electronic data in South Africa

In 2002, the ECTA was passed into law and laid out requirements for assessing the admissibility and evaluating the weight of data messages.[83] The ECTA is largely based on the United Nations' Model Law on Electronic Commerce (UNCITRAL Model Law).[84] It also introduced important definitions, such as data, data messages, and electronic signatures.[85] The ECTA reiterated the existence of the legal force of a data message by providing that the rules of evidence must not be applied so as to deny the admissibility of a data message in any legal proceedings on the ground that it is a data message or that it is not in its original form.[86] It also set out criteria for the presentation of an original data message before a court,[87] the production of information in the form of data,[88] the retention of data messages,[89] and the admissibility and evidential weight of a data message.[90]

Relevance and admissibility of evidence in South Africa

Relevance is an essential requirement for evidence to be admissible and it is predicated on a standard of practical logic and reason.[91] The general rule of relevance is that all facts that are logically and legally relevant to legal proceedings are admissible and ought to be proved.[92] Therefore once any evidence has passed the hurdle of relevance, it is admissible provided it does not fall within the ambit of an exclusionary rule of evidence.[93] It is pertinent to point out that not all logically relevant evidence is automatically legally relevant.[94] The South African legal system also makes inadmissible any fact which is irrelevant to the fact in issue in legal proceedings:

> 'No evidence as to any fact, matter or thing shall be admissible which is irrelevant or immaterial and which cannot conduce to prove or disprove any point of fact at issue in criminal proceedings.'[95]

The CPEA also contains a similar provision which provides that '[N]o evidence as to any fact, matter or thing which is irrelevant or immaterial and cannot conduce to prove or disprove any point of fact in issue shall be admissible'.[96]

The admissibility of electronic evidence is primarily governed by the ECTA, specifically subsections 15(1) and (4). The sections essentially declare that a data message shall not be rendered inadmissible because it is constituted by a

[81] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[82] South African Law Reform Commission Report Review of the law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues'.
[83] ECTA, 2002.
[84] United Nations Commission on International Trade Law (UNCITRAL) regarding electronic commerce: Model Law on Electronic Commerce with Guide to Enactment, 1996 (as adopted in 1998).
[85] ECTA, sec 1.
[86] ECTA, sec 11.
[87] ECTA, sec 14.
[88] ECTA, sec 17.
[89] ECTA, sec 16.
[90] ECTA, sec 15; Adrian Bellengère and Lee Swales, 'Can Facebook ever be a substitute for the real thing? A review of *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens*', (2012) (5) SA 604 (KZD) 2016 *Stell LR*, 454, 466.
[91] D T Zeffert, A Paizes, and A Skeen, *The South African Law of Evidence* (LexisNexis Butterworths, Durban, 2003), 220.
[92] *S v Gokool* 1965 3 SA 461 (N), at 475.
[93] *R v Schaube Kuffler* 1969 2 SA 40 (RA), at 50.
[94] The term 'legally relevant' can be misleading. What is intended to be conveyed by the term is that even if evidence is logically relevant it may not be admitted because of a legal rule prohibiting its admission, in other words, it is not 'relevant' because of a 'legal' rule'. See also P J Schwikkard and S E Van der Merwe, *Principles of Evidence*; S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 3.65.
[95] Section 210 CPA, 1977; D S De Villiers, 'Old 'documents, 'videotapes' and new 'data messages' a functional approach to the law of evidence (part 1)', 2010 *Tydskrifvir die Suid AfrikaanseReg*, 572.
[96] Section 2 CPEA, 1965.

data message.[97] This proclamation does not automatically make every data message admissible, because data messages may be rejected as inadmissible on other grounds whether or not contained in the ECTA.[98]

The Supreme Court of Appeal in *Firstrand Bank Limited v Venter*[99] highlighted the purpose of Section 15 of the ECTA as follows:

> 'Section 15 of [ECTA]:
>
> 1. facilitates the use of and reliance on a data message;
>
> 2. deals with the assessment of the evidential weight of such a message; and
>
> 3. lays down the minimum requirements for admissibility.'[100]

The purpose of ECTA was also adumbrated in another Supreme Court of Appeal case: *Spring Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash*[101] where it was stated as follows:

> '[The aim of the ECTA] is to promote legal certainty and confidence in respect of electronic communications and transactions, and when interpreting the Act, the courts are enjoined to recognise and accommodate electronic transactions and data messages in the application of any statutory law or the common law.'[102]

The conclusion to be drawn from this is where a data message or an electronic transaction is to be presented as evidence and is of a documentary nature, a combined reading of sections 3, 4 and 15(1) of the ECTA will reveal that any other law regulating the admissibility of evidence may apply.[103]

Admissibility of data messages of a real or documentary nature

Though the ECTA does not define the nature of a data message as either real or documentary, inferences have been drawn in judicial decisions about the forms in which data messages can be presented.[104] The differentiation becomes necessary when it is considered that for a data message in a documentary form, the credibility of such a piece of evidence may rely on a natural person giving evidence.[105] The truth of the contents of a document will require corroboration by the maker of the document or a person with adequate knowledge of the contents of it.[106]

A document as defined by both the CPA and CPEA has been interpreted to include everything that contains written or pictorial proof of something regardless of what material it is made of.[107] This definition has led some scholars to consider that a data message falls conveniently within the realm of what constitutes a document.[108] This opinion seems to be backed up by the apparent functional equivalency created by the ECTA, which states that the criteria in law that information in documentary form should be in writing has been met if the information was created by an electronic device in data form and is retrievable in an intelligible form.[109] This section seems to equate the rules of admissibility and weight of documents to that of data messages by considering them as being similar.[110]

---

[97] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012), 681.
[98] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 681. See also, *Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA).
[99] [2012] JOL 29436 (SCA), paragraph 16.
[100] [2012] JOL 29436 (SCA). See also *S v Brown* 2016 (1) SACR 206 (WCC).
[101] 2015 (2) SA 118 (SCA).
[102] *Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash*, at 682.
[103] *Forest Trading CC v Wilberry (Pty) Ltd t/a Ecowash*, at 682. Section 4(1) of the ECT Act expressly provides that the Act applies 'in respect of any electronic transaction or data message'.
[104] South African Law Reform Commission Report Review of the Law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues', 6.34.
[105] D P Van der Merwe, *Information and Communications Technology Law*, 123.
[106] D S De Villiers, 'Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)', 564.
[107] *Seccombe v Attorney General* 2002 (2) All SA 185 (Ck) 277; *S v Harper* 1981(2) SA 88 (D); G P van Tonder, 'The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective', 18.
[108] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 5.
[109] Section 12 ECTA, 2002.
[110] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 682.

The documentary or real nature of a data message was the subject of consideration in the case of *S v Motata*,[111] where the accused was charged with driving a motor vehicle whilst under the influence of liquor.[112] The accused drove the vehicle into the fence of private property owned by the complainant. The complainant recorded the event on his mobile telephone and took some photographs of the scene of the accident with a camera.[113] Audio records were later shared from the mobile telephone of the complainant and stored on his home computer. At the time the trial proceedings began, the original version of the audio recordings had been deleted from the camera, thus raising the question of its fulfilment of the requirements for admissibility.[114] The court held that the content of the recordings satisfied the requirements for documentary evidence and decided that they were admissible for the purpose of which they were tendered.[115] The decision was affirmed on appeal.[116]

Documentary evidence must be relevant, authentic and original before it can be admitted subject to the concessions in the ECT Act in relation to data messages.[117] This was reflected in the case of *Ndlovu v Minister of Correctional Services* where the court held that, although it was sufficiently convinced that section 15(1) read with sections 15(2) and (3) of the ECTA provided for the admissibility of hearsay evidence and for evidential weight to be ascribed to it,[118] it went on to treat the computer generated evidence as being documentary.[119]

In *Ndlovu's* case, the Minister of Correctional Services presented recorded entries to prove parole violations by Ndlovu to the court in the form of a computer printout from an electronic device in the department.[120] During the course of the trial, the court was tasked with interpreting section 15 of ECTA on the admissibility of data messages as they relate to hearsay rules. The court in its interpretation emphasized a distinction between electronic information, the probative value of which is predicated on a human being, and electronic information, the truth of which is not dependent on an author.[121] The court, upon evaluation of the recorded entries, determined that the computer printouts were in fact documents and it held that as documents, the printout must be relevant, authentic and the original is to be admitted as evidence.[122]

On the other hand, real evidence consists of tangible objects presented to the court for the purpose of proving a fact and is admitted upon proof of its relevance.[123] Unlike documentary evidence, the rules of hearsay evidence do not apply to real evidence.[124] Real evidence does not rely on the testimony of any author, rather any testimony to the real evidence can be on matters of accuracy, reliability, and regularity.[125]

The South African legal system recognizes graphics, audio and video, and other electronic information as real evidence.[126] There are, however, contrasting opinions on whether or not a data message ought to be considered as

---

[111] Johannesburg District Court case number 63/968/07 (unreported).
[112] Johannesburg District Court case number 63/968/07 (unreported).
[113] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position'.
[114] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings', 9.
[115] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings', 10.
[116] *Motata v S* (A345/2010) [2010] ZAGP JHC; this decision coincides with the discussion in S Mason, 'Electronic evidence and the meaning of 'original'', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, Issue 79, Autumn, 2009, 26 – 28 [the articled is cited by Ramasubramanian J, Supreme Court of India in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal*, (2020 SCC OnLine SC 571)], the article is available as Open Access at https://journals.sas.ac.uk/amicus/article/view/1206 .
[117] *S v Meyer* [2017] ZAGPJHC, at 299, *Ndlovu v Minister of Correctional Services and Another* [2006] 4 All SA 165 (W); *S v Baleka (1)* 1986 4 All SA 428 (T).
[118] *Ndlovu v Minister of Correctional Services and Another*, at 172.
[119] *Ndlovu v Minister of Correctional Services and Another*; see also *S v Ramgobin* 1986 4 SA 117 (N) where the court treated videotapes as documents.
[120] *Ndlovu v Minister of Correctional Services and Another* [2006] 4 All SA 165 (W).
[121] *Ndlovu v Minister of Correctional Services and Another* at 173; see S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapter 4 'Software code as the witness', for a more detailed discussion.
[122] *Ndlovu v Minister of Correctional Services and Another*, at 173.
[123] P-J Schwikkard and S E Van der Merwe, *Principles of Evidence.*
[124] D P van der Merwe, *Information and Communications Technology Law*, 123.
[125] D P van der Merwe, *Information and Communications Technology* Law, 123.
[126] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 9. However, there has been some difference in provincial division cases in South Africa. More recently, see *S v Brown* 2016 (1) SACR 206 (WCC), at 20.

real evidence based on the reason that data messages in the form of graphics, audio and video are volatile and subject to alterations. However, information on paper in a documentary form is also subject to being altered.[127] Also, the admissibility and evidential value of data messages depend on interpretation to establish their relevance.[128]

It is pertinent to note that it is also possible to produce a data message with little or no human intervention. This brings into question the extent to which such a data message can be termed as documentary evidence.[129] Also, a printed copy of a data message may not contain detailed information and metadata that would otherwise have been retained in the native digital version.[130]

These contrasting opinions have also been a subject of consideration in the case of *S v Ndiki*[131] where the court reiterated that a data message the admissibility of which relied on the functionality of the electronic device and all its accompaniments is classified as real evidence.[132] In *Ndiki*,[133] the state tendered some computer printouts in proof of charges of fraud against the accused.[134] The court held that some of the computer printouts were documents because their veracity depended upon the credibility of a signatory.[135] The court further held the other computer printouts to be real evidence because they did not require any such corroboration, because they were made with little human intervention.[136] The court, in interpreting section 15 of ECTA was of the view that the section classifies information in the form of data as real evidence as envisaged by the common law.[137]

A data message can be altered, preserved and shared with relative ease.[138] Because of the flexible nature of a data message, it becomes increasingly difficult to determine the accuracy and authenticity of the evidence. While the ECTA provides that courts should not deny the admissibility of a data message merely for the reason of it not being in its original form, it does not provide a definition of 'original' or 'copy' of a data message.[139] The ECTA, however, provides for a form of functional equivalence, which means that information contained on paper should be treated the same way as information contained in the form of an electronic data message,[140] and the requirements of section 14 of the ECTA regarding 'originality' will be need to be satisfied. That is, if the data message is capable of being produced, either in electronic or paper form; that the reliability of information contained in a data form is evaluated by examining its consistency, and the reason for which it has been produced.

The ECTA also did not address the effect of transferring data messages through storage devices particularly as it relates to the best evidence rule. Because data in electronic form can be in the form of many layers of copies, it raises the question of whether such evidence qualifies as having met the requirements of the best evidence rule.[141]

---

[127] J Hofman, 'Electronic Evidence in criminal cases', (2006), South African Journal of Criminal Justice, 257 to 275

[128] J Hofman, 'Electronic Evidence in criminal cases'.

[129] J Hofman 'South Africa' in S Mason, editor, *Electronic Evidence*, 690; D S De Villiers, 'Old 'documents', 'videotapes' and new 'data messages – a functional approach to the law of evidence (part 1)', 560.

[130] *Trend Finance (Pty) Ltd v Commissioner of SARS* (2005) 4 All SA 657 (C); see S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapters 1, 6 and 9 for a detailed discussion. The reality of the resources in South African courts means that often, almost always, data messages will be presented in the form of paper. This is the reality of the South African system that might vary slightly in other common law jurisdictions.

[131] *S v Ndiki and Others* [2007] 2 All SA 185 (Ck).

[132] *S v Ndiki and Others*, at 35.

[133] *S v Ndiki and Others*.

[134] *S v Ndiki and Others*, at 35.

[135] *S v Ndiki and Others*.

[136] *S v Ndiki and Others*, at 37.

[137] *S v Ndiki and Others*.

[138] South African Law Reform Commission Report Review of the Law of Evidence, 'Electronic evidence in criminal and civil proceedings: admissibility and related issues', 2.6; S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapters 1 and 9.

[139] Section 11 ECTA, 2002.

[140] W Jacobs, 'The Electronic Communications and Transactions Act: Consumer Protection and Internet Contracts', (2004) SA Merc LJ, 556, 557.

[141] N Wilson, A Sheldon, H Dries, Burkhard Schafer and S Mason, 'Proof: technical collection examination of electronic evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 9.30 to 9.48. See also South African Law Reform Commission Report 'Review of the Law of Evidence, Electronic evidence in criminal and civil proceedings: admissibility and related issues', 6.29.

The court in *Trend Finance (Pty) Ltd v Commissioner of SARS*[142] addressed the issue that where an electronic copy of a document exists, the question was whether a printout of that information can be regarded as the 'best evidence' that the adducer could reasonably be expected to obtain. The answer in most cases should be 'no', because a printed copy would lack the embedded information normally retained in the electronic copy that purported to evidence when, and by whom, the document was originally created, whether it was revised or edited, to whom it may have been sent and when it was received.[143]

The application of hearsay rules to electronic data in South Africa

Evidence that requires further verification by a person other than the one giving such evidence is hearsay evidence.[144] According to Mason and Seng, hearsay are statements other than one made by a person while giving oral evidence.[145] Such evidence is generally inadmissible and will remain so unless the person upon which the credibility of such evidence testifies, or if the evidence falls within the exceptions to the rules of hearsay evidence.[146] It is important to point out that the reason for the rule against hearsay is predicated on the basis that it is risky to rely on unfounded information as a means of determining the truth.[147]

In South Africa, the primary rule regulating hearsay evidence is the EAA,[148] which defines hearsay evidence as information whether in written or oral form, which the probity depends on an individual other than the person presenting such information to the court.[149] Section 3 of the EAA reads as follows:

> '3(1) Subject to the provisions of any other law hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless
>
> (a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings;
>
> (b) the person upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings; or
>
> (c) the court having regard to
>
> (i) the nature of the proceedings;
>
> (ii) the nature of the evidence;
>
> (iii) the purpose for which the evidence is tendered;
>
> (iv) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;
>
> (v) any prejudice to a party which the admission of such evidence might entail; and
>
> (vi) any other factor which should in the opinion of the court be taken into account,
>
> is of the opinion that such evidence should be admitted in the interest of justice.'[150]

---

[142] *Trend Finance (Pty) Ltd v Commissioner of SARS* (2005) 4 All SA 657 (C).
[143] *Trend Finance (Pty) Ltd v Commissioner of SARS*, at 49.
[144] D T Zeffert, A Paizes, and A Skeen, *The South African Law of Evidence* (LexisNexis Butterworths, Durban, 2003), 366-368.
[145] S Mason and D Seng 'Hearsay' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 3.2 (citing Sir Rupert Cross' definition of hearsay rule of evidence).
[146] P-J Schwikkard and S E Van der Merwe, *Principles of Evidence*.
[147] D Seng and S Mason, 'Hearsay' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 3.5.
[148] Section 3 of the Law of Evidence Amendment Act 45 of 1988; see also Lee Swales, An analysis of the regulatory environment governing electronic evidence in South Africa: suggestions for reform (2019 PhD, University of Cape Town), https://open.uct.ac.za/handle/11427/30335. There is an entire chapter on this topic, and Dr Swales makes very similar points under this section.
[149] Section 3 of the Law of Evidence Amendment Act; see also *Cresto Machines (Edms) Bpk v Die Afdeling Speuroffisier SA Polisie, Noord Transvaal* 1972 1 SA 376 (A) on admitting admission of original evidence; *Giesecke and Devrient South Africa (Pty) Ltd v Minister of Safety and Security* 2012 2 SA 137 (SCA).
[150] Section 3 of the Law of Evidence Amendment Act.

The EAA was introduced to provide rules regulating the admissibility of, and weight to be attached to, hearsay evidence.[151] Whether or not section 3 of the EAA applies to computer generated evidence has been a contentious subject in the South African legal system.[152] Even with the legal recognition afforded to, as well as the assured admissibility of, data message by the ECTA,[153] some scholars are of the opinion that section 3 of the EAA should also apply to information generated on an electronic device in the form of data message.[154] This position is predicated on the argument that although it is possible for the creation of a data message to require little or no direct human influence, all computer printouts occur with some form of human intervention because computer programmes are written by a human, thereby making them documents.[155]

The need for drawing a difference between the real and documentary nature of data messages is because if a data message is adjudged to be real evidence, then section 3 of the EAA will obviously not apply to it. This is because a data message is evidence, and the probative value is not predicated on the credibility of another person. In other words, real evidence cannot be hearsay because its value does not depend on a person's credibility, which means it is admissible, if relevant, and cannot be excluded by the rule against hearsay.[156] If a person creates a data message, the data message constitutes procedural hearsay. For the purpose of relying on procedural hearsay, the value of statements contained in a data message depends on the credibility of the creator. It is pertinent to note here that a data message can contain elements of hearsay and metadata and the data message will only be hearsay to the extent that it is not metadata. If the person who creates the data message testifies himself/herself, the evidence is technically no longer considered hearsay and it will be admitted under the provisions of section 3(1)(b) of the EAA. However, even if the individual is not called as a witness, the court still has the discretion to admit the hearsay information upon being convinced that it is in the interest of justice to do so.[157] In *S v Brown*[158] the court opined that on the basis that a data message is very volatile and can easily be altered and manipulated, they should be treated more as evidence of a documentary nature rather than real evidence.[159]

Other scholars have offered counter arguments to this position, primarily on the grounds that it does not take into account the difference between the form and content of evidence, which is the basis upon which a court excludes a document as hearsay.[160] According to this view, it is a criterion that for evidence to be a document, it must contain information that qualifies it as such.[161] The position is that where a data message is tendered as evidence to establish the fact that information was sent, received or stored, it cannot be excluded merely because it constitutes hearsay.[162]

In *MTN Service Provider (Pty) Limited v LA Consortium & Vending CC t/a LA Enterprises*, the plaintiff tendered computer generated evidence to prove the delivery of the network services which the defendants did not pay for.[163] The defendants objected to the admissibility of the computer generated evidence because it amounted to hearsay.[164] The court held the data messages generated from the computer system were hearsay, because they depended on the credibility of the person inputting the data. In this case, the department head oversaw ensuring

[151] D P Van der Merwe, *Information and Communications Technology Law*, 109 to 110; C H W Schmidt and H Bewysreg Rademeyer, *Law of Evidence* (2000, LexisNexis Durban), 370 to 373.
[152] C W H Schmidt and H Bewysreg Rademeyer, *Law of Evidence*, 372.
[153] Section 11 and 15 of the ECTA, 2002.
[154] D P Van der Merwe, *Information and Communications Technology Law*, 25.
[155] D Collier, 'Evidently not so simple: Producing computer printouts in court', (2005) (1) JBL 6.
[156] P J Schwikkard and S E Van der Merwe, *Principles of Evidence*, 276 to 283.
[157] P F Fourie, 'Using social media evidence in South African Courts', Dissertation submitted in fulfilment of the requirements for the degree *Magister Legum* in Formal Law at the Potchefstroom Campus of the North West University, 2016, 41; *Metedad v National Employer's General Insurance Co Ltd* 1992 1 SA 494 (W).
[158] 2016 (1) SACR 206 (WCC), at 214 h.
[159] 2016 (1) SACR 206 (WCC), at 214 h.
[160] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 684.
[161] P F Fourie, 'Using social media evidence in South African Courts', 12 paragraph 2.1.1.
[162] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 8.
[163] 2011 (4) SA 562 (W), 566 to 567.
[164] 2011 (4) SA 562 (W), 566 to 567.

the accurate recording of the orders into the computer.[165] On appeal,[166] Malan J in addressing the application of section 3(1) of the EAA to data messages found that data messages can be classified as real evidence if 'the probative value…depends on the reliability and accuracy' of a computer system.'[167]

The application of section 3 of the EAA is also dependent on the interpretation of section 15 of the ECTA. This issue came under consideration in the case of *Ndlovu v Minister of Correctional Services*,[168] where Gautschi AJ opined as follows:

> 'Where the probative value of the information in a data message depends upon the credibility of a person other than the person giving evidence, there is no reason to suppose that Section 15 seeks to override the normal rules applying to hearsay evidence. On the other hand, where the probative value of the evidence depends upon the "credibility" of the computer Section 3 of the Law of Evidence Amendment Act 45 of 1988 will not apply, and there is every reason *to suppose* that Section 15(1), read with Sections 15(2) and (3), intend for such "hearsay" to be admitted, and due evidential weight to be given thereto according to an assessment having regard to certain factors.'[169]

Also, in *S v Ndiki*[170] Van Zyl J stated thus:

> 'As I shall attempt to show when I deal with the provisions of the Law of Evidence Amendment Act 45 of 1988, computer evidence which falls within the definition of hearsay evidence in s 3 thereof may become admissible in terms of the provisions of that Act. Evidence that depends solely on the reliability and accuracy of the computer itself and its operating systems or programs, constitutes real evidence. What s 15 of the Act does, is to treat a data message in the same way as real evidence at common law. It is admissible as evidence in terms of ss (2) and the court's discretion simply relates to an assessment of the evidential weight to be given thereto (ss (3)). The ECT Act 25 of 2002 is therefore inclusionary as opposed to exclusionary.'[171]

The issue, however, remains unsettled and therefore clarification is needed as to whether data messages constitute hearsay within the contemplation of section 3 of the EAA and if so, whether the EAA applies to data messages made with little or no human effort.[172] Theophilopoulos sums the issue up as follows:

> 'The Principal, and at present, the unanswered question is whether Section 15 of the Act may be interpreted as a justifiable exception to the hearsay rule. May a hearsay message be admitted without being tested against the limitations set out in Section 3 of the Law of Evidence Amendment Act? … First, it is unlikely that such an interpretation would be adopted by a future court as it conflicts with Section 35(3) (1) of the Constitution – the right to challenge evidence. Secondly, it may also be contrary to the supreme court of appeal's interpretation of the doctrine of functional equivalence. A logical consequence of the court's reasoning, as the author understands it, is that if a message is obliged to meet common law threshold admissibility rules of originality and authenticity then surely a hearsay message must also be obliged to meet constitutionally tested limitations set out in Section 3 of the Law of Evidence Amendment Act. After all, a common law rule does not carry the same weight as a constitutionally tested statutory right… Thirdly, the *Ndiki* case had previously reinforced this strict functional equivalence reasoning by stating that the meaning of hearsay should be extended to include "evidence that depends on the accuracy of the computer."'[173]

---

[165] 2011 (4) SA 562 (W), 566 to 567.
[166] *MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a La Enterprises and Others* (2011 (4) SA 577 (GSJ)).
[167] *MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a La Enterprises and Others* (2011 (4) SA 577 (GSJ)), [16].
[168] [2006] 4 All SA 165 (W).
[169] *Ndlovu v Minister of Correctional Services and Another* [2006] 4 All SA 165(W), at 173.
[170] (2008) (2) SACR 252 (Ck).
[171] *S v Ndiki and others* (2008) (2) SACR 252 (Ck), at 7.
[172] *Ndlovu v Minister of Correctional Services and Another* [2006] 4 All SA 165 (W), at 173.
[173] C Theophilopoulos, 'The admissibility of data, data messages, and electronic documents at trial', (2015) *Tydskrifvir die Suid AfrikaanseReg*, 474 to 475. See also S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 3.65 and chapter 4 'Software code as the witness'.

Ascription of evidential value to data messages

Evidential weight is an important part of the criteria for the determination of legal disputes. The court in judicial proceedings has a duty to evaluate the probative value of an exhibit once it has been admitted into evidence and to determine the weight to be attached to it.[174] The appropriate period for the evaluation of the evidential weight to be ascribed to evidence is at the conclusion of the trial. It is at this time that the court will then take into consideration the reliability of the evidence and credibility of the individuals upon which the probative value of the evidence is predicated as well as the plausibility of the litigant's case.[175] The evidential weight of a data message is provided for by the ECTA, which not only provides for the legal recognition of a data message but also states that information in the form of a data message must be given due evidential weight once such information has been admitted into evidence.[176] Subsections 15(2), (3) and (4) of the ECTA outline the factors to be taken into account in evaluating the evidential weight of data messages for the purpose of attaching the appropriate weight thereto:

> '15(2) Information in the form of a data message must be given due evidential weight.
>
> (3) In assessing the evidential weight of a data message, regard must be had to
>
> (a) the reliability of the manner in which the data message was generated, stored or communicated;
>
> (b) the reliability of the manner in which the integrity of the data message was maintained;
>
> (c) the manner in which its originator was identified; and
>
> (d) any other relevant factor.
>
> (4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.'

Rules regulating the evaluation of probative value to determine the weight to attach to evidence are often matters of fact and vary from case to case.[177] Unlike the rules regulating the admissibility of evidence, which is often unyielding, those regulating the probative value are usually the result of the evaluation by the court of the nature and circumstance of the evidence before it.[178]

Upon admission, evidence needs to be factual and verifiable before it can be relied upon by the court and the primary onus of proof is on the person who tenders it to prove its authenticity.[179] This is also the same in the case of data messages. The ECTA also provides for the establishment of the authenticity of data messages.[180] It is for this purpose that information from data must be accompanied by the surrounding facts of its existence, the chain of dissemination, creation, storage, manipulation.[181] One of the methods of establishing authenticity, found in the ECTA, is the introduction of an advanced electronic signature[182] which may be used to prove and verify the creation and storage of a data message.[183]

Depending on what purpose evidence is tendered, there can be several methods of verifying the authenticity of evidence in electronic form. However, a general requirement is adducing evidence as to authorship and possession,

---

[174] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 691.
[175] P F Fourie, 'Using social media evidence in South African Courts', 75; *S v Van Aswegen* 2001 2 SACR 97 (SCA).
[176] Sections 11 and 15 ECTA, 2002.
[177] D Van der Merwe, *Information and Communications Technology Law*, 109-110.
[178] *S v Ndiki and others* (2008) (2) SACR 252 (Ck).
[179] DT Zeffert, A Paizes, and A Skeen, *The South African Law of Evidence* (2003), 94; P J Schwikkard and S E Van der Merwe, *Principles of Evidence* (3rd ed Juta & Co Wetton, 2009), 437.
[180] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 8.
[181] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 8; see S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapters 6 and 9 for detailed discussions.
[182] Section 1 of ECTA defines an advanced electronic signature as an electronic signature which results from a process which has been accredited by an Authority as provided for in section 37 ECTA, 2002.
[183] D Van der Merwe, *Information and Communications Technology Law*, 115 and 123.

especially when the evidence is created by a human.[184] In *Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa*, Human J outlined the requirements to establish authorship and possession of private documents as follows:

> 'The law in relation to the proof of private documents is that the document must be identified by a witness who is either (i) writer or signatory thereof, or (ii) the attesting witness, or (iii) the person in whose lawful custody the document is, or (iv) the person who found it in possession of the opposite party, or (v) handwriting expert…'[185]

In the case of data messages, however, it is not always the case that a printout of the data message will contain all the properties of the data message and its surrounding circumstances.[186] This is because details of the creation of the data are usually recorded in the form of embedded information retained in the electronic copy. This information is often referred to as metadata.[187]

Metadata can be used to ascertain the purported author and origin of an electronic message and the existence of any attachments thereto.[188] The information which is contained in the metadata is not often visible on a printout of the data message.[189] Metadata includes information such as the purported date of creation of the document, the date sent and received usually stored as written records, audio, video, databases, temporary files, deleted records, and other electronic data generated on the storage memory device by the electronic software.[190] The use of digital evidence professionals to assist the court in understanding embedded data messages as well as other technical electronic matters that can help with the evaluation of weight to be attached to electronic evidence has been advocated.[191]

As a general rule in the South African legal system, the truth of the information contained in a piece of evidence cannot be established unless the best version of the evidence is produced.[192] The effect on a data message is that secondary evidence will generally not be accepted to prove its contents unless such evidence is shown to be the only means or the best available means of proving the content of the data message.[193] The need for the application of the best evidence rule is evident in electronic evidence because of the transient nature of data messages, which makes them easy to tamper with.[194]

It is suggested that the proper application of the best evidence rule to data messages should not be limited to the authentication of electronic devices or the presumption of the workability of originating devices.[195] Unique identifiers such as hash functions and magic numbers[196] have the potential to provide for the integrity and continuity

---

[184] *Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa* 1971 (3) SA 937 (T).
[185] *Howard & Decker Witkoppen Agencies and Fourways* Estates 1971 (3) SA 937 (T), at 940.
[186] *Trend Finance (Pty) Ltd v Commissioner of SARS* (2005) 4 All SA 657 (C).
[187] *Trend Finance (Pty) Ltd v Commissioner of SARS*; for a detailed explanation of metadata, see S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 1.67-1.78; 2.8; 2.56; for metadata in the context of authentication, see 6.81; 6.92.
[188] Per Tamberlin J in *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2006] FCA [11]. See also Rilwan F. Mahmoud, 'The Potential of WhatsApp as a Medium of Substituted Service in the Nigerian Judicial System', (2019) Malaysia Current Law Journal, Legal Network Series, A (cx iii), 1.
[189] Per Tamberlin J in *Jarra Creek Central Packing Shed Pty Ltd v Amcor Limited* [2006] FCA 11.
[190] L Duranti and A Stanfield 'Authenticating Electronic Evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 6.7.
[191] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 692; M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 10. See also Rilwan F. Mahmoud, H. O. Abdulazeez, and O. T. Wuraola, 'An Assessment of the Legal Recognition and implementation of Electronic Evidence in the Tanzanian and Nigerian Legal Systems', (2019) The Public and International Law Journal, University of Abuja, 1(1).
[192] *Standard Merchant Bank v Creaser* 1982 (4) SA 671 (W) 674; G P van Tonder, 'The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective', 18.
[193] P-J Schwikkard and S E Van der Merwe, *Principles of Evidence*, 405; *Welz v Hall* 1996 4 SA 1073 (C).
[194] D T Zeffert, A Paizes and A Skeen, *The South African Law of Evidence*, 358.
[195] South African Law Reform Commission, 'Report on the Review of Law of Evidence' (Paper 131, Project 126, 2017) 101. The application of best evidence rule to electronic evidence is suggested to be certified upon the proof of integrity of the device in which the data message is stored.
[196] https://en.wikipedia.org/wiki/Magic_number_(programming) .

of data messages. Non-fungible tokens[197] for instance, can create a certified true copy of a data message such picture or a text message.

The limitations of ECTA in regulating electronic evidence

The ECTA brought the much-needed legal recognition of data messages, however, it remains a challenging law with regards to the admissibility and weight of electronic information, and its application has not been consistent.[198] The court in *Jafta v Ezemvelo KZN Wildlife*,[199] held that though the information contained in email may contain informal language, evaluating such information as having no legal effect would be a mistake.[200]

One major point of contention that the ECTA has failed to resolve is the definition of a document with respect to data messages. The implication of this is section 34 of the CPEA, section 221 of the CPA and section 3 of the EAA, among others, which applied to traditional paper documents and still apply to electronic information. These provisions must be read together with the provisions of ECTA for the purpose of admissibility and weight to be ascribed thereto.[201] The problem with this is that the application of these sections to data messages might create absurdities because these provisions were not originally designed with electronic information in mind.[202] Section 34 of the CPEA, for instance, provides for a statement made by a person in a document to be admissible. However, this is of little help because a computer is not regarded as a person.

The definition of a document, which includes any device by which information is recorded or stored, is wide enough to include a computer itself.[203] A document as defined by both the CPA and CPEA has been interpreted to include everything that contains written or pictorial proof of something regardless of what material it is made of.[204] This definition has led to some scholars considering that data messages fall conveniently within the realm of what constitutes documents.[205] This view seems to be substantiated by the apparent functional equivalency created by the ECTA, which states that the criteria that information contained in a document must be in writing will have been fulfilled where such information was created in data form on an electronic device and is retrievable in a visibly intelligible form.[206] This section seems to equate the rules of admissibility and weight of documents to those of a data message by considering them as being similar.[207]

There is, therefore, a need for clarification of the definition and nature of what constitutes documents in relation to electronic information by way of an amendment or the enactment of an electronic information evidence act. Another matter to be considered is the lack of clarification of the difference between an original and a copy of electronic evidence in the ECTA.[208]

It is pertinent at this juncture to examine the need to reconsider the meaning of 'original' within the purview of electronic evidence. Mason has emphasised in several works the need to do away with the classification of 'original'

---

[197] https://en.wikipedia.org/wiki/Non-fungible_token ; for a case from China regarding intellectual property infringement and the authenticity of electronic evidence in relation to SHA256 hash value and the value of blockchain related evidence, see *Hangzhou Huatai Yimei Culture Media Co., Ltd. v. Shenzhen Daotong Technology Development Co., Ltd.* (2018) Zhe 0192 Civil Case, First Court No. 81**,** Hangzhou Internet Court of the People's Republic of China, translated by Dr Jiong He, 16 *Digital Evidence and Electronic Signature Law Review* (2019) 61, https://journals.sas.ac.uk/deeslr/issue/view/533 .

[198] D S De Villiers, 'Old 'documents', 'videotapes' and new 'data messages – a functional approach to the law of evidence (part 1)', 720.

[199] (2008) ZALC 84.

[200] D S De Villiers, 'Old 'documents', 'videotapes' and new 'data messages – a functional approach to the law of evidence (part 1)', 720.

[201] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).

[202] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 9.

[203] *S v Harper* 1981 (2) SA 638 (D).

[204] *Seccombe v Attorney-General* 2002 (2) All SA 185 (Ck) 277; *S v Harper* 1981 (2) SA 88 (D).

[205] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 5.

[206] Sec 12 ECTA, 2002.

[207] J Hofman, 'South Africa' in S Mason, editor, *Electronic Evidence*, 682.

[208] South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010), 6.13.

within the preview of electronic evidence.[209] He puts it succinctly in his paper, 'Electronic evidence and the meaning of 'original'' as follows:

> 'The digital object, made up of a series of zeros and the number one, can be, and frequently is manipulated and altered. The new manipulated digital images can also be divided back into its constituent parts… In the same way, consider a digital object that has been manipulated and added to, and the process is then reversed. The original object that was used remains (unless it was never saved independently, and the changes made to the images were saved in the original file), but another object, with the identical image (or near identical, depending on the system software and application software) now exists… both images are identical, apart from some additional meta data that might, or might not be conclusive… However, it is apparent that the images, if viewed together are identical – will be identical, and the viewer will not be able to determine which is the original and which image was manipulated.'[210]

It is suggested, in line with Mason's opinion, that the ease of duplicability of the output of electronic evidence renders the use of the term 'original' otiose. Consequently, the concept of 'first in time evidence' which is the 'data that is subject to copying' as defined by Mason and others should be adopted.[211] This paper merely considers the practicality of applying elements of documentary evidence to electronic information. It is also suggested that the procedural cultures in common law jurisdictions on the requirement of originality in relation to electronic evidence affects how this is treated. For instance, the legal culture in Nigeria insists on the strict adherence to the production of original evidence with a few statutory exceptions, while other jurisdictions, such as England and Wales and South Africa appear to be more liberal in the application of the best evidence rule.

While the ECTA provides that courts should not deny the admissibility of data messages merely for the reason of not being in its original form, it does not provide the definition of 'original' or 'copy' of a data message.[212] Section 14 of the ECTA states that the requirement of 'originality' will be satisfied if the data message can be produced in either electronic or paper form, and the evaluation of the integrity of the content of a data message is a necessary requirement, as well as the purpose for which it is being tendered into evidence.[213]

Another point of contention is the scope of section 15(4) of the ECTA which appears rather broad and uncertain.[214] The section makes a data message in any form, be it a copy, printout or an extract, made by any person in the ordinary course of business, admissible as rebuttable proof upon certification by an officer in the service of the maker of the data message.[215] In *Absa Bank Ltd v Le Roux*, the court was of the opinion that:

> 'Section 15(4) has a twofold effect. It creates a statutory exception to the hearsay rule and it gives rise to a rebuttable presumption in favour of the correctness of electronic data falling within the definition of the term 'data message'.'[216]

Though the ECTA provisions regarding admissibility and weight are based on the UNCITRAL Model Law, section 15(4) is an apparent departure from the Model Law[217] and the provision runs the risk of opening a floodgate of data

---

[209] N Wilson, A Sheldon, H Dries, Burkhard Schafer and S Mason, 'Proof: technical collection examination of electronic evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 9.30 to 9.33; S Mason, 'Electronic evidence and the meaning of 'original'', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*; see also, L Duranti and A Stanfield 'Authenticating Electronic Evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 6.3-6.4.

[210] S. Mason 'Electronic evidence and the meaning of 'original'', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, 28.

[211] N Wilson, A Sheldon, H Dries, Burkhard Schafer and S Mason, 'Proof: technical collection examination of electronic evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 9.30-9.33. See also South African Law Reform Commission Report 'Review of the Law of Evidence, Electronic evidence in criminal and civil proceedings: admissibility and related issues', 6.29.

[212] Sec 11 ECTA, 2002.

[213] Sec 14 ECTA, 2002.

[214] D T Zeffert, A Paizes and A Skeen, *The South African Law of Evidence*, 393-395.

[215] Sec 15(4) ECTA, 2002.

[216] 2014 (1) SA 475 (WCC) 19.

[217] South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010), 6.40.

messages that now enjoy a presumption of genuineness on the mere production of the data.[218] The law, therefore, needs to be reviewed with specific consideration given to the nature of electronic information.[219]

Conclusion

While the CEA ushered a new era of evidentiary rules of electronic evidence, it is arguable that did not achieve its intended purpose because the attempt to simplify and streamline the rules regulating the admissibility of, and weight to be attached to, electronic evidence was an overcautious approach, leading to an unfairly high standard of authenticity and reliability.[220] It is concluded that the vacuum left by the repeal of CEA has not been filled by the ECTA, despite its many achievements and there is still the need for a review of the rules regulating the admissibility and weight to be accorded to electronically generated evidence.[221] This was reflected in the South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010).[222] Swales also emphasised the limitations of ECTA in filling the vacuum left by the CEA.[223]

It is, therefore, necessary for a review of the laws regulating the evidentiary procedure in South Africa. The South African Law Reform Commission (SALRC) in its discussion paper 131: 'The Review of Law of Evidence', has addressed some of these issues and made several essential recommendations on some of the issues relating to admissibility and weight of electronic evidence.[224] Some of the recommendations include the differentiation between information created in the form of data solely by a person, and data created without the aid of human intervention.[225] It also suggested reforms in the bill to make practice directions on the evaluation of both types of information.[226] The SALRC also recommends that the rules of evidence should do away with the conventional 'presumption of regularity' when dealing with mechanical devices.[227] Rather, it suggests that a limited presumption should be applied especially in civil proceedings which place an evidential burden on the other party who did not object on notice.[228] It also recommends the enactment of a subsidiary practice direction on obtaining and producing information from electronic devices so as to help legal practitioners streamline the process of tendering evidence in data form and to help judicial officers with the more technical aspects of producing electronic evidence in court to avoid unnecessary confusion.[229]

---

[218] D W Collier 'Electronic Evidence and Related Matters' in P J Schwikkard and S E van der Merwel, *Principles of Evidence*, 416-7.

[219] These considerations, which include the 'first in time' rule and a review of the application of the best evidence rules to electronic evidence have been discussed extensively in L Duranti and A Stanfield 'Authenticating Electronic Evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures* 6.32 and N Wilson, A Sheldon, H Dries, Burkhard Schafer and S Mason, 'Proof: technical collection examination of electronic evidence' in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures* 9.32.

[220] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position', 9.

[221] M Watney, 'Admissibility of Electronic Evidence in Criminal Proceedings' and S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 3.68.

[222] South African Law Reform Commission Report Review (Issue Paper 27, Project 126, 2010) 4.2-4.6 and 6.

[223] Lee Swales, An analysis of the regulatory environment governing electronic evidence in South Africa: suggestions for reform. See also Lee Swales, 'Electronic instruments – a presumption of reliability, a presumption of regularity, judicial notice, or none of the above?', South African Journal of Criminal Justice, Vol. 31, No. 2, December 2018, 189-211; *Trustees for the time Being of the Delsheray Trust and Others v ABSA Bank Limited* (A504/13) [2014] ZAWCHC 152; [2014] 4 All SA 748 (WCC) (9 October 2014).

[224] South African Law Reform Commission, 'Discussion Paper: The Review of Law of Evidence' (Paper 131, Project 126, 2015).

[225] This is discussed in detail in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapters 3 and 4. The SALRC's recommendations were also restated in Lee Swales, 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One', PER/PELJ (2018) 24 and Lee Swales, 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two', PER/PELJ (2018) 26.

[226] South African Law Reform Commission Discussion Paper 131 (Project 126, 2015) Annexure A (Law of Evidence Bill 2014). A revised version of the Bill was also included in the South African Law Reform Commission report of Project 126 in 2017.

[227] The presumption of reliability and the unfairness scandal it has caused in England & Wales is discussed in depth in S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, chapter 5.

[228] South African Law Reform Commission Discussion Paper 131 (Project 126, 2015), 5.20.

[229] South African Law Reform Commission Discussion Paper 131 (Project 126, 2015), 5.17. See also S Mason and D Seng, editors, *Electronic Evidence and Electronic Signatures*, 5.35; on this specific point, the reader's attention is drawn to the following important papers: Paul Marshall, James Christie, Peter Bernard Ladkin, Bev Littlewood, Stephen Mason, Martin Newby, Jonathan

The conventional rules of hearsay, real and documentary evidence cannot pragmatically be applied to all forms of electronically stored information. To apply documentary rules to all forms of electronic information will be creating a functional equivalency of paper evidence/documents to electronic evidence.[230] The potential risk of classifying data as either exclusively real evidence or documentary evidence is that there might be attributes of either classification that do not fit the evidence being evaluated such as the application of hearsay to a data message.[231] It is suggested that such restrictive classifications such the requirement that data in electronic form should be original creates some absurdities, as Mason points out.[232] It is also suggested that the SALRC's recommendations do not adequately address the lacunae. Consequently, it is recommended that there are clearer definitions of what constitutes electronic information, which can be considered a statement in electronic form that is contained in documents and electronic data that are created wholly by electronic algorithms and software. It is also recommended that the rules regulating each of these types of information on authentication, best evidence, relevance, admission, presumption, and weight ascription are defined individually to avoid inconsistencies in the classification of evidence.[233]

mahmoudesq@yahoo.com

ORCID: https://orcid.org/0000-0002-1162-149X

Rilwan Mahmoud LLB, LLM (University of Ilorin), PhD (University of KwaZulu-Natal) is a Postdoctoral Fellow of the College of Law and Management Studies, University of KwaZulu-Natal, South Africa. He is also a Lecturer in the Department of Public Law, University of Ilorin, Nigeria and the Head of Practice of the Prometheus Law Associate, Nigeria.

Rogers, Harold Thimbleby, Martyn Thomas CBE, 'Recommendations for the probity of computer evidence', 18 *Digital Evidence and Electronic Signature Law Review* (2021) 18-26; Michael Jackson, 'An approach to the judicial evaluation of evidence from computers and computer systems' 18 *Digital Evidence and Electronic Signature Law Review* (2021) 50-55, both available as Open Access at Volume 18 : 2021 | Digital Evidence and Electronic Signature Law Review (sas.ac.uk) .

[230] The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 SEDONA C ONF . J. 1 (2018), https://thesedonaconference.org/sites/default/files/publications/The%20Sedona%20Principles%20Third%20Edition.19TSCJ1.pdf .

[231] D S De Villiers, 'Old 'documents', 'videotapes' and new 'data messages – a functional approach to the law of evidence (part 1)', 564.

[232] S. Mason 'Electronic evidence and the meaning of 'original'', *Amicus Curiae The Journal of the Society for Advanced Legal Studies*, 28.

[233] I wish to share my unreserved gratitude to Stephen Mason, Dr. Allison Stanfield and the peer reviewer for the thorough assessment of this paper.