An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two

L Swales*

P·E·R

Pioneer in peer-reviewed, open access online law publications

Author

Lee Swales

Affiliation

University of KwaZulu-Natal
South Africa

Email swalesl@ukzn.ac.za

Date of submission

11 July 2017

Date published

19 March 2018

Editor Dr A Gildenhuys

How to cite this article

Swales L "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two"*PER / PELJ* 2018(21) - DOI http://dx.doi.org/10.17159/1727-3781/2018/v21i0a4496

DOI
http://dx.doi.org/10.17159/1727-3781/2018/v21i0a4496

Abstract

The purpose of this two-part article is to examine the regulatory environment governing hearsay electronic evidence in South Africa with a view to suggesting law reform in the light of the most recent proposals put forward by the South African Law Reform Commission.

Part one considered the definition of data messages in the context of hearsay electronic evidence and concluded that amendment is required (as suggested by the South African Law Reform Commission). Further, part one sought to answer two additional queries posed in *Discussion Paper 131 Review of the Law of Evidence* in relation to electronic hearsay, ultimately finding that a data message can constitute hearsay within the meaning of the applicable legislation; further, that South African law must distinguish between data messages produced substantially by a computer or mechanical process and those that rely substantially on the credibility of a person.

Part two of this article will review the statutory exceptions to the hearsay rules applicable to electronic evidence, including the controversial section 15(4) of the *Electronic Communications and Transactions Act* 25 of 2002. Further, part two will analyse the situation in selected foreign jurisdictions where hearsay electronic evidence has had more time to mature and develop (United Kingdom, Canada and United States) with a view to incorporating suggestions that South Africa can implement.

Finally, this article will conclude by providing suggestions for law reform in the context of the recommendations put forward by the South African Law Reform Commission, and will suggest that that there must be law reform in at least the following areas: the definition of data messages; the definition of the term document in the statutes applicable to the hearsay exceptions; a distinction between types of electronic evidence insofar as computer-generated evidence with human intervention, and without human intervention is concerned; and more cohesion and alignment with the statutory hearsay exceptions.

Keywords

Electronic evidence; data messages; *ECT Act*; law of evidence; South African Law Reform Commission; technology and law.

.....

1 Introduction

Given the enormous increase in internet penetration in South Africa[1] and our society's apparent increasing reliance on technology,[2] it is reasonable to infer that the use of data messages[3] as evidence in all forms of legal proceedings will continue to increase.

Part one[4] of this two-part article examined the regulatory framework governing hearsay electronic evidence in South Africa and sought to answer three critical questions posed by the South African Law Reform Commission (SALRC):[5] should the definition of data messages be revised?[6] Should a data message constitute hearsay?[7] And, how should one distinguish between documentary evidence and real evidence in the context of data messages?[8]

Part two will seek to complete this discussion by reviewing the statutory exceptions to the hearsay rules applicable to electronic evidence, including the controversial[9] section 15(4) of the *Electronic Communications and Transactions Act* 25 of 2002 (the *ECT Act*). Further, part two of this article will analyse the situation in selected foreign jurisdictions where electronic evidence has had more time to mature and develop (the United Kingdom, Canada and the United States). Finally, this article will conclude by

---

* Lee Swales. LLB (UKZN) LLM (Wits). Lecturer, School of Law, University of KwaZulu-Natal and Consultant Attorney Thomson Wilks Inc. E-mail: swalesl@ukzn.ac.za. A revised version of this paper was presented at a conference of the South African Association of Intellectual Property Law and Information Technology Law Teachers and Researchers, hosted by Stellenbosch University on 21-22 June 2017. This paper forms part of an ongoing PhD study.

1 Internet World Stats 2017 http://www.internetworldstats.com/africa.htm#za: roughly 54% of South Africa's population had internet access as at June 2017. In 2008 the South African penetration rate was roughly 9%.

2 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 437; Papadopoulos and Snail *Cyberlaw@SA III* 1; Van der Merwe *et al Information and Communications Technology Law* 1

3 Swales 2018 *PELJ* 3-5 for a discussion on data messages.

4 See Swales 2018 *PELJ* – https://doi.org/10.17159/1727-3781/2018/v21i0a2916

5 SALRC *Discussion Paper 131* where issue 3 considers whether the *Electronic Communications and Transactions Act* 25 of 2002 (the *ECT Act*) definition of data message should be revised; issue 6 considers s 15 of the *ECT Act* and the hearsay rules in the context of electronic evidence; and issue 7 considers whether there should be a distinction between different types of electronic evidence. Also see SALRC *Issue Paper 27* 7-49.

6 SALRC *Discussion Paper 131* 52-55; Swales 2018 *PELJ* 3-5.

7 SALRC *Discussion Paper 131* 62-68; Swales 2018 *PELJ* 8-14.

8 SALRC *Discussion Paper 131* 68-70; Swales 2018 *PELJ* 14-23.

9 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 12.

providing suggestions for law reform in the context of the recommendations put forward by the SALRC.[10]

2 Hearsay electronic evidence

The *Law of Evidence Amendment Act*[11] defines hearsay evidence as:

> evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence.

Although not specifically stated, the *Law of Evidence Amendment Act* applies to data messages.[12] Simply, hearsay electronic evidence (in the form of a data message) is that evidence where the creator of the document (or other form of data message) is not at court to directly testify.

As noted in part one of this article, if a data message is classified as real evidence, then it should not be subject to a hearsay analysis, and should be admissible if it is otherwise relevant.[13] There is some debate as to whether real electronic evidence must also be authentic (and relevant) to be admissible, or whether the authenticity of the real electronic evidence is considered when determining the weight of the data message. There is authority for both propositions.[14]

Traditionally, hearsay evidence was excluded on the basis that it may unduly influence a jury,[15] the rationale being that the evidence is not direct, and cannot be directly tested. That is, one is not able to cross-examine a witness about what the witness saw, or knows, or heard, nor is one able to observe the body language and general demeanor of the person in question.

Arguably, however, with a legal system that has long dispensed with a jury, a unitary court (with a trained legal expert as Judge) is unlikely to be unduly influenced by hearsay evidence. Although this is beyond the scope of this

10 SALRC *Discussion Paper 131* 83-106.

11 *Law of Evidence Amendment Act* 45 of 1988.

12 *S v Ndiki* 2007 2 All SA 185 (Ck) para 31*; LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 19; Zeffertt and Paizes *South African Law of Evidence* 432-435; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 441-446; Hofman 2006 *SACJ* 262; Theophilopoulos 2015 *TSAR* 474-475.

13 Swales 2018 *PELJ* 14-23.

14 Swales 2018 *PELJ* 17-19.

15 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 287.

article, it may be necessary to re-consider hearsay and the rationale for its existence entirely.[16]

3 Exceptions to the hearsay rule

If a data message is relevant and authentic – on the basis that it is classified as documentary evidence, and not real evidence – the rules regulating hearsay may still mean the evidence is excluded[17] if the person responsible for the document is not at court.[18] Consequently, in the context of hearsay electronic evidence, there are a number of statutory exceptions where hearsay evidence will be admitted.[19]

3.1 The Law of Evidence Amendment Act

The *Law of Evidence Amendment Act*[20] changed[21] the law of evidence by introducing a statutory definition of hearsay and including several exceptions to the exclusionary hearsay rule. The three exceptions created by section 3(1) are as follows:

- in terms of 3(1)(a) where the party against whom the hearsay evidence is to be adduced agrees to its admission;
- in terms of 3(1)(b) where the person upon whose credibility the probative value of the hearsay evidence depends testifies; and
- in terms of 3(1)(c) where a court is provided with a list of factors, and ultimately has a wide discretion to admit hearsay evidence if the court deems it to be in the interests of justice.

Consequently, even if a court takes a conservative approach and classifies a data message as documentary hearsay evidence, then it will still have the discretion to admit the hearsay data message, if it is of the view that the interests of justice demand its admission into evidence. Therefore, where a court is in doubt as to the classification of a data message, it may classify it as documentary hearsay and still have the ability to receive it into evidence

16 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 287.
17 Hofman and De Jager "South Africa" 770.
18 Hearsay as defined by s 3(4) of the *Law of Evidence Amendment Act* 45 of 1988.
19 Hofman 2006 *SACJ* 265-268; Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 305-323; Zeffertt and Paizes *South African Law of Evidence* 418-441.
20 *Law of Evidence Amendment Act* 45 of 1988.
21 Hofman 2006 *SACJ* 265.

via the broad discretion vested in a court via the *Law of Evidence Amendment Act*.[22]

3.2 The Civil Proceedings Evidence Act

Of the three primary exceptions created by the *Civil Proceedings Evidence Act*[23] *(CPEA)* in the context of data messages, one relates to bankers' books, one relates to business records, and there is a general exception where the author of a data message is not available.[24] The promulgation of the *CPEA* took place when data messages were not fully contemplated or developed but, as noted by Hofman,[25] there is no reason these exceptions should not apply to electronic evidence.

Section 34(1)(a)(i) creates an exception for situations where the author of the data message had personal knowledge of the statements made therein but is not available to testify. Section 34(1)(a)(ii), the wording of which is certainly not a model of clarity, creates a further exception where a document was created by someone who was recording another (which recording is continuous and in the ordinary course of duty), and the person who was being recorded had personal knowledge of the statement.[26]

The details pertaining to these exceptions, largely nullified[27] by the *Law of Evidence Amendment Act* (and are therefore less applicable than they once were), are discussed in ordinary textbooks dealing with the law of evidence.[28] Even though controversial, the creation of the business records exception in section 15 of the *ECT Act*, discussed below, has further nullified the use of the older, more traditional hearsay exceptions.

---

22 *S v Ndiki* 2007 2 All SA 185 (Ck) para 22; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ) para 18.

23 *Civil Proceedings Evidence Act* 25 of 1965 (*CPEA*).

24 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 310-316.

25 Hofman and De Jager "South Africa" 771.

26 Hofman and De Jager "South Africa" 770-771.

27 Hofman and De Jager "South Africa" 771.

28 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 311-316; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 290-301; Zeffertt and Paizes *South African Law of Evidence* 418-429; Bellengere *et al Law of Evidence* 295-305.

3.3 The Criminal Procedure Act

As is the case with the *CPEA* and the *ECT Act*, the *Criminal Procedure Act*[29] *(CPA)* creates an exception for business records in terms of section 221 under the heading admissibility of certain trade or business records.[30]

If the conditions of section 221(1) are satisfied,[31] any statement contained in a document that establishes a fact will be admissible on the mere production thereof.

In terms of the conditions for admissibility the compilation of the document must have taken place in the ordinary course of business, and someone who can be reasonably presumed to have knowledge of the matters dealt with therein must supply it. Finally, the person who supplied the information must be dead, outside the Republic, or unable to testify due to mental or physical ailments.[32]

Moreover, section 222 of the *CPA* incorporates sections 33-38 of the *CPEA* into all forms of criminal proceedings. In the present context, this means that the exception created by section 34 of the *CPEA* (for the admissibility of a data message where the author is not available) is also applicable to criminal proceedings.[33]

Finally, sections 236 and 236A of the *CPA* create an exception for banking records (both local and international banks) where an employee of the bank certifies the accuracy of the record and confirms that the capture thereof took place in the ordinary course of business.[34]

---

29 *Criminal Procedure Act* 51 of 1977 (*CPA*).

30 Hofman and De Jager "South Africa" 773; Hofman 2006 *SACJ* 266; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 290-301; Zeffertt and Paizes *South African Law of Evidence* 418-441.

31 The exception is dealt with in detail in traditional texts dealing with the law of evidence; Hofman 2006 *SACJ* 265.

32 Hofman and De Jager "South Africa" 772-777; Hofman 2006 *SACJ* 266; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 290-301; Zeffertt and Paizes *South African Law of Evidence* 418-441.

33 Hofman and De Jager "South Africa" 772-777; Hofman 2006 *SACJ* 266; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 290-301; Zeffertt and Paizes *South African Law of Evidence* 418-441.

34 Hofman and De Jager "South Africa" 772-777; Hofman 2006 *SACJ* 266; Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed 290-301; Zeffertt and Paizes *South African Law of Evidence* 418-441.

3.4 The Electronic Communications and Transactions Act

Section 15(4)[35] of the *ECT Act* creates a business records exception to the hearsay rule for any data message created in the ordinary course of business. The section, which is controversial,[36] has been criticised because of the difficulties[37] it creates. It reads as follows:

> (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.

Hofman[38] lists six difficulties with the section, and this commentary appears to have received the approval of other academic commentators.[39] These difficulties appear to remain, and although the section has been at issue in several cases, it has often received superficial judicial treatment.[40]

In *LA Consortium*[41] Malan J held that:

> despite the very wide words of s 15(4), any hearsay contained in a data message must pass the criteria set out in s 3 of the Law of Evidence Amendment Act 45 of 1988.

---

35 Duvenhage *Evidential Analysis* 9-34 for a thorough discussion of this exception.

36 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 12.

37 Hofman and De Jager "South Africa" 771-772; Hofman 2006 *SACJ* 267; De Villiers 2010 *TSAR* 734.

38 Hofman 2006 *SACJ* 267-268, where the difficulties, summarised, are: 1. The exception is too wide; 2. The rebuttable presumption the section creates should not apply to all businesses; 3. The certificate required by an officer of the business imposes less responsibility than other similar exceptions; 4. The wording of the section is problematic; 5. The wide exception may force courts to consider excessive volumes of evidence; 6. When applied in criminal matters, the section arguably creates a reverse onus, which may not be constitutional.

39 Theophilopoulos 2015 TSAR 476; De Villiers 2010 *TSAR* 733-734; SALRC *Discussion Paper 131* 71-72; Fourie *Using Social Media as Evidence* 78-79, where the author evaluates the six grounds listed by Hofman, disagreeing specifically with one ground but endorsing the primary "reverse-onus" difficulty.

40 For example, in *S v Van der Linde* 2016 3 All SA 898 (GJ), where the section was referred to, but only briefly; in *Sublime Technologies (Pty) Ltd v Jonker* 2010 2 SA 522 (SCA), where although it appeared central to the dispute it was mentioned only in passing.

41 *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises* 2011 4 SA 577 (GSJ) para 13.

In *Absa Bank Ltd v Le Roux*[42] the court noted 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'.[43]

Also, in the Supreme Court of Appeal, in *Firstrand Bank Limited v Venter*,[44] in the context of section 15(4), the court noted that it:

> lays down the minimum requirements for admissibility…; and
>
> once produced was admissible against [a person] and [serves] as 'rebuttable proof' of the facts contained in the printouts…

Earlier, in what appears to be the first case[45] dealing with section 15(4), in *Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited*,[46] Du Plessis J held:

> In terms of section 15(4) of that Act a printout of a data message can constitute *prima facie* proof if the data message was made by a person in the ordinary course of business and if the printout is certified to be correct by 'an officer in the service of such person'.[47]

Further, in *Ndlovu* the court described section 15(4) as follows:

> Section 15(4) provides for two situations in which a data message may on its mere production be admissible in evidence. The first is 'a data message made by a person in the ordinary course of business', which, juxtaposed with the words that follow, clearly refers to an original data message, and is required to have been made 'in the ordinary course of business'. The second is a copy or printout of or an extract from such data message which is certified to be correct by an officer in the service of such person (being a person who made the data message in the ordinary course of business). Once either of these two situations is present, the data message is on its mere production admissible in evidence and rebuttable proof of the facts contained therein.[48]

In *Trend Finance (Pty) Ltd v Commissioner for SARS*[49] the court pointed out that a party seeking to rely on section 15(4) must show that the document "sought to be admitted is a printout of information existing in electronic

---

42 *Absa Bank Ltd v Le Roux* 2014 1 SA 475 (WCC).
43 *Absa Bank Ltd v Le Roux* 2014 1 SA 475 (WCC) para 19.
44 *Firstrand Bank Limited v Venter* 2012 JOL 29436 (SCA) para 16.
45 Hofman and De Jager "South Africa" 772.
46 *Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited* 2005 ZAGPHC 311 (22 August 2005). Also see Duvenhage *Evidential Analysis* 12-13.
47 *Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited* 2005 ZAGPHC 311 (22 August 2005) 6.
48 *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172-173.
49 *Trend Finance (Pty) Ltd v Commissioner for the South African Revenue Service* 2005 4 All SA 657 (C) 678-679.

form." Consequently, it appears from this case that in order to rely on this statutory exception one must satisfy a court that the printout has a data message format somewhere on a computer or mechanical system.

Moreover, in *Director of Public Prosecution v Modise*[50] the court catergorised section 15(4)[51] as follows:

> [It is] designed to … allow evidence in the form of the facts and opinions contained in a document which complies with [section 15(4)] to be admitted in evidence at a trial notwithstanding that the person who listed the facts and formed the opinions in the document is not called as a witness.[52]

In an application to review the court above, in *Modise*, Lamont J seemed to indicate that notwithstanding some of the academic concerns pointed out above (which concerns were not dealt with – nor was any prior case law reviewed in reaching a decision), section 15(4) is an intentional step by South Africa's legislature to subjugate the hearsay rule:[53]

> [Section 15(4) is] specifically designed to enable [persons] to avoid the need to lead the evidence of a witness by way of producing him and then leading viva voce evidence. The facts and matters in a document are the evidence. The evidence is admissible if the provisions of this section are complied with. Nothing more is required. The section enables [persons] to easily produce evidence which will generally be of a formal and uncontested nature and to place same in documentary form before a court without the need to call the witness… [A person] does not have to send its experts to a variety of courts countrywide to give evidence which generally is uncontested with the concomitant waste of money and time. In addition the expert becomes free to perform other work. These sections allow limited resources to be properly and adequately used.[54]

This wide exception appears to go further than previous statutory exceptions,[55] and appears to favour evidence in the form of a data message if in a business context. This is probably contrary to the principle of functional equivalence. Moreover, as suggested by others,[56] if a person in a business context is able to comply with the statutory provisions of section 15(4), which simply require certification from an employee that the printout

50 *Director of Public Prosecution v Modise* 2012 1 SACR 553 (GSJ).

51 Duvenhage *Evidential Analysis* 34-38.

52 *Director of Public Prosecution v Modise* 2012 1 SACR 553 (GSJ) 557.

53 Duvenhage *Evidential Analysis* 34-38, where the author notes that s 15(4) of the *ECT Act* is an intentional departure from the *Model Law*, 1996; but concludes that the "radical" provision ought to be repealed in its entirety.

54 *Director of Public Prosecution v Modise* 2012 1 SACR 553 (GSJ) 557.

55 De Villiers 2010 *TSAR* 733-734; Hofman 2006 *SACJ* 267-268; Theophilopoulos 2015 *TSAR* 476.

56 Hofman 2006 *SACJ* 268; De Villiers 2010 *TSAR* 731; Fourie *Using Social Media as Evidence* 79; Theophilopoulos 2015 *TSAR* 476.

of a data message is correct, then those facts are rebuttably presumed true. Arguably, this creates a reverse onus that may be constitutionally suspect[57] in criminal cases, even though it is a presumption which can be challenged. Further, in a civil context, the fact that someone operates a business does not necessarily mean the data message is accurate, reliable or honest, even if certified.[58]

However, as pointed out above in *Modise*, there is merit in the argument that the section is an intentional departure from the *Model Law*, 1996. Further, the cases analysed above indicate clearly that our courts will accept documentary hearsay when the conditions of section 15(4) of the *ECT Act* are satisfied.

As suggested by the SA Law Reform Commission, the interplay between the statutory hearsay exceptions and section 15(4) of the *ECT Act* is "complex", creates "unnecessary confusion" and requires "greater alignment."[59]

4 Selected international positions on hearsay electronic evidence

What follows below in 4.1 to 4.4 is a consideration of the situation in several foreign jurisdictions where electronic evidence has had a longer time to develop and mature. The purpose of the examination of England, Canada and the United States is to facilitate suggestions for law reform. Ideally South Africa should seek to learn from other jurisdictions and/or avoid mistakes that may have already been made in the context of hearsay electronic evidence. This analysis is not intended to serve as a comprehensive comparative study of international law, but as a basis for gleaning information regarding possible interpretations in relation to hearsay electronic evidence.

4.1 England and Wales

The English law of evidence (on which the South African law of evidence is based) has been referred to as being founded on exclusionary rules, which contain two fundamental guiding principles – the best evidence rule and the

57 Hofman 2006 *SACJ* 267. De Villiers 2010 *TSAR* 733-734; Hofman 2006 *SACJ* 267-268; Theophilopoulos 2015 *TSAR* 476.

58 De Villiers 2010 *TSAR* 733-734; Hofman 2006 *SACJ* 267-268; Theophilopoulos 2015 *TSAR* 476.

59 SALRC *Discussion Paper 131* 31-32, 70.

hearsay rule.[60] Much as in South Africa, evidence will be admissible if relevant to an issue in dispute, subject to a number of exceptions.[61] Moreover, and again much as in South Africa, one of the core concerns insofar as computer evidence is concerned has been in relation to the hearsay rule.[62]

In England,[63] the position is the same as in South Africa – that is, if the production of data occurs without human intervention, it is real evidence (no hearsay enquiry).[64] Conversely, if the data is a record of human assertions, then it is hearsay.[65]

The key, as in many jurisdictions around the world, is to determine whether the credibility of the data relies on a person or a computer (via an automated process), and this distinction often leads to "confusion" and has acted as a "brake" on the introduction of new technology.[66]

However, even if the data is documentary in nature and therefore subject to the exclusionary hearsay rules, there are several statutory exceptions, including those found in the *Criminal Justice Ac*t 2003 and the *Civil Evidence Act* 1995.[67]

In the fourth and most recent edition of Electronic Evidence,[68] the authors of the chapter on hearsay appear critical of the "complex" rules one must consider. With this complexity in mind, it is beyond the scope of this paper to analyse the regulatory framework of hearsay evidence in England other than to note that an approach whereby data messages are classified as real evidence (if they rely on the credibility of a computer) is possible and appears to be preferred.[69]

For example, in *R (on the application of O) v Coventry Justices*,[70] automated transactions (involving a credit card and a pornography website) were

60 Leroux 2004 *IRLCT* 202.
61 Mason, Freedman and Patel "England and Wales" 347.
62 Mason, Freedman and Patel "England and Wales" 363.
63 For a comprehensive view of the English position, see Tapper *Cross and Tapper on Evidence*; also see Gallavin and Mason "Hearsay" 72-88.
64 Hofman and De Jager "South Africa" 770.
65 Hofman and De Jager "South Africa" 770.
66 Reed "Admissibility and Authentication of Computer Evidence" 3-5.
67 The exceptions are similar to those found in South Africa, including a business records exception. For a detailed analysis of the exceptions, see Tapper *Cross and Tapper on Evidence* 586-626.
68 Tapper *Cross and Tapper on Evidence* 60-61; Gallavin and Mason "Hearsay" 72-88.
69 Reed "Admissibility and Authentication of Computer Evidence" 2-6.
70 *R (on the application of O) v Coventry Justices* [2004] All ER (D) 78.

regarded admissible real evidence on the basis that they were purely mechanically produced.

Earlier, in *R v Spiby*,[71] where an automated process (a computer) monitored telephone calls, this evidence was real evidence because there was no human intervention in the production of the data. Accordingly, it was not hearsay evidence.[72]

Moreover, in *McDonald v R*,[73] in a criminal appeal largely dealing with character evidence, the court found that a printout from a mobile phone service provider (Vodafone) was real evidence (rather than documentary hearsay).

In *R v Spiby*[74] the court expressed the following opinion when justifying why certain electronic evidence should be regarded as real evidence:

> Where information is recorded by mechanical means without the intervention of a human mind the record made by the machine is admissible in evidence provided, of course, it is accepted that the machine is reliable.

In my view, the key point to take from the English position is that electronic evidence can be classified as either real evidence (not subject to the hearsay rules), or it can be classified as documentary evidence (subject to the hearsay rules). The classification of the evidence will depend on its nature. Simply, it appears from the cases reviewed above that if the data is subject to human intervention in its production, then it will be classified as hearsay documentary evidence. Conversely, if the data is not subject to any human intervention, then the evidence will be real evidence.

4.2 Canada

The Canadian law of evidence is predominantly based on English common law (except in Quebec),[75] and as is the case in England and South Africa,

71 *R v Spiby* [1990] 91 Cr App R 186.

72 *Castle v Cross* [1985] 1 All ER 87, where a printout (from a computer or device) of what is displayed or recorded on a mechanical measuring device is real evidence.

73 *McDonald v R* [2011] EWCA Crim 2933 para 42.

74 *R v Spiby* [1990] 91 Cr App R 186, which quotes the article Smith 1983 *Crim L R* 390.

75 Boyd *Canadian Law* 87-105; also see CIA 2017 https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html.

electronic evidence is subject to the same evidentiary regime as traditional evidence.[76]

The electronic evidence must be material and relevant to the issues and must not be subject to any other exclusionary rule.[77] The primary legislative instruments regulating electronic evidence are the *Canada Evidence Act*, 1985 and the *Uniform Electronic Evidence Act*, 1999. Canada has departed from the *Model Law,* 1996 (and other jurisdictions)[78] by using the term electronic record instead of data message or computer evidence.

In *R v Mondor*[79] the Ontario Court of Justice, referring to academic authors,[80] confirms that electronic evidence can take the form of real evidence or documentary evidence. This is much like the position in South Africa and England. The court found that:

> Where the electronically stored data is recorded electronically by an automated process, then the evidence is real evidence. Where, however, the electronically stored information is created by humans, then the evidence is not real evidence, and is not admissible for its truth absent some other rule of admissibility.

As with many other jurisdictions, Canada also has a business records hearsay exception, and the court in *Mondor* was tasked with determining whether hearsay electronic evidence (documentary evidence that is subject to human intervention) would be admissible in terms of the Canadian hearsay exception.[81]

Using logic similar to that in the South African decisions in *Ndlovu* and *Ndiki* (discussed above), the Canadian court in *Mondor* found that:

> [The Canada Evidence Act] does not allow for the admission of hearsay evidence contained within an electronic document just because it is in electronic form. The applicant must first establish that the hearsay is admissible either under section 30 or some other mechanism.

---

76 Groulx, Rothman and Zawidzki 2011 https://www.dentons.com/~/media/FMC%20Import/publications/pdf/a/Admissibility%20Understanding%20Types%20and%20Sources%20of%20Electronic%20Evidence.ashx 22.

77 For a comprehensive overview and discussion of the Canadian law of evidence, see Paciocco and Stuesser *Law of Evidence*.

78 Seng and Chakravarthi 2003 https://www.agc.gov.sg/DATA/0/Docs/PublicationFiles/Sep_03_ComputerOutput.pdf 14.

79 *R v Mondor* 2014 ONCJ 135 para 17.

80 Underwood and Penner *Electronic Evidence* 186.

81 Sections 30 and 31 of the *Canada Evidence Act*, 1985

Ultimately, after analysing previous cases dealing with hearsay electronic evidence[82] the court found the evidence to be "inadmissible for the truth of their contents."[83]

In *Saturley v CIBC World Markets Inc*[84] the Nova Scotia Supreme Court set out the position as follows (mimicking what in my view is the correct positon in South Africa):

> Electronic information may be considered either real or documentary evidence. If it is real evidence, it simply needs to be authenticated and the trier of fact will then draw their own inferences from it. Examples of real evidence include photographs and physical objects.[85]
>
> If electronic information is determined to be real evidence, the evidentiary rules relating to documents, such as the best evidence and hearsay rules, will not be applicable.[86]

The court goes further to note that the real issue lies in deciding "when electronic information should be treated as real evidence, rather than documentary".[87] Ultimately, electronic evidence will be real evidence when its production is "without human intervention."[88]

The position in Canada - that data produced without human intervention is real evidence - has received judicial support, including in the matter of *R v McCulloch*,[89] where telephone records were admitted as real evidence because of the automated nature of the data.

Moreover, in *R v Hall*[90] the court found that automated billing records were real evidence (although in this case they also fell under the hearsay business records exception). In this matter the Canadian court referred with approval to the English case of *R v Spiby*[91] (discussed above), where the English court found that an automated process monitoring phone calls was real evidence (not subject to hearsay rules).

---

82 *R v Mondor* 2014 ONCJ 135 paras 34-39, where previous Canadian cases dealing with hearsay electronic evidence are discussed.
83 *R v Mondor* 2014 ONCJ 135 para 43.
84 *Saturley v CIBC World Markets Inc* 2012 NSSC 226.
85 *Saturley v CIBC World Markets Inc* 2012 NSSC 226 para 11.
86 *Saturley v CIBC World Markets Inc* 2012 NSSC 226 para 13.
87 *Saturley v CIBC World Markets Inc* 2012 NSSC 226 para 14.
88 *Saturley v CIBC World Markets Inc* 2012 NSSC 226 para 21.
89 *R v McCulloch* [1992] BCJ 2282 para 18.
90 *R v Hall* [1998] BCJ 2515.
91 *R v Spiby* [1990] 91 Cr App R 186.

4.3 The United States of America

It is almost impossible to concisely summarise the legal position on any legal issue in the United States, primarily because it is subject to a federal system. Each state has its own independent judiciary and applies its own procedural and evidentiary rules.[92]

Be that as it may, the legal system of the United States is similar to that of South Africa and those jurisdictions discussed above in that it is a predominantly common law system based on English common law (at a federal level).[93] Moreover, and as a general position, the United States adopts a similar stance in relation to hearsay electronic evidence. The United States adopts a business records hearsay exception,[94] and distinguishes between computer-generated records (with no human intervention – real evidence), and computer-stored records (with human intervention – documentary hearsay).[95]

In terms of the *Federal Rules of Evidence*, hearsay is not admissible as evidence,[96] but this is subject to several exceptions.[97] The basis for considering the admissibility of electronic evidence in the United States is similar to that in South Africa – the evidence must be relevant, authentic, must not be hearsay, must be the best evidence available, and its probative value must outweigh any prejudicial effect.[98]

In my view, the distinction between real and documentary evidence created in South Africa, England and Canada is largely the same as that observed in the United States, in that if the data relies on a human mind (or a human statement) it is subject to hearsay rules. If the data relies on, or its

---

92 Schwerha, Bagby and Esler "United States of America" 798.

93 Friedman and Hayden *American Law* 35-55; also see CIA 2017 https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html.

94 Schwerha, Bagby and Esler "United States of America" 797-835.

95 Seng and Chakravarthi 2003 https://www.agc.gov.sg/DATA/0/Docs/Publication Files/Sep_03_ComputerOutput.pdf.

96 *Federal Rules of Evidence*, 1975 802. See also, *Federal Rules of Evidence* art VIII – Hearsay, and ss 801-807.

97 *Federal Rules of Evidence* 803. See also, *Federal Rules of Evidence* art VIII – Hearsay, and ss 801-807.

98 Kemp 2012 *NC JOLT* 20-21; Frieden and Murray 2011 *Rich J L & Tech* 2-6; Thomson 2012 https://www.americanbar.org/content/dam/aba/events/science_technology/mobiledevices_new_challenges_admissibility_of_electronic_device.authcheckdam.pdf; Pendleton 2013 http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/; Miskel 2015 http://www.emilymiskel.com/blog/admissibility-of-digital-evidence-in-a-family-case/.

production is solely automated or mechanical, then it is not subject to the hearsay rules.[99]

For example, in *U-Haul Intern Inc. v Lumbermens*,[100] the United States Court of Appeals for the Ninth Circuit dealt with computer-generated summaries of payments made on insurance claims, and found that, in the context of the business records hearsay exception: "Rule 803(6) provides that records of regularly conducted business activity meeting … criteria constitute an exception to the prohibition against hearsay evidence."[101]

In *Telewizja Polska USA Inc. v Echostar Satellite Corp*[102] the court found that images and text (that purported to show what a website looked like at a point in time) were not statements for purposes of the federal hearsay rules (akin to real evidence in South Africa).

Moreover, in *United States v Rollins*[103] the court found that computer-generated evidence (without human intervention) was admissible without requiring admissibility in terms of hearsay rules.

Furthermore, in *Lorraine v Markel American Insurance Company*[104] the court delivered a comprehensive 101-page opinion outlining the admissibility of electronically stored information. One submission from a practitioner in the United States suggests that the court set the admissibility bar unnecessarily high,[105] but the lengthy opinion canvasses all relevant United States' law (insofar as electronic evidence is concerned) and may well be a point of departure if US electronic evidence is at issue.

In summary, the court comprehensively reviewed the applicable statutory regime for the admissibility of electronic evidence (at a federal level), and found that if evidence is generated by a computer, it cannot be subject to hearsay as it is not produced by a person.[106] In the context of hearsay electronic evidence, the court found that:[107]

> When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the 'report'

99 Joseph 1999 http://www.jha.com/us/articles/viewarticle.php?8.
100 *U-Haul Intern Inc. v Lumbermens* 576 F 3d 1040 (9th Cir 2009).
101 *U-Haul Intern Inc. v Lumbermens* 576 F 3d 1040 (9th Cir 2009) 1043.
102 *Telewizja Polska USA Inc v Echostar Satellite Corp* 2004 WL 2367740.
103 *United States v Rollins* 2004 WL 26780.
104 *Lorraine v Markel American Insurance Company* 241 FRD 534.
105 Esler 2007 *DEESLR* 80-82.
106 Similar logic was used in the South African cases of *Ex parte Rosch* 1998 1 All SA 319 (W) and *Narlis v South African Bank of Athens* 1976 2 SA 573 (A).
107 Kemp 2012 *NC JOLT* 16-30.

> generated when a fax is sent showing the number to which the fax was sent and the time it was received, there is no 'person' involved in the creation of the record, and no 'assertion' being made. For that reason, the record is not a statement and cannot be hearsay.

In a similar vein, in *United States v Lizarraga-Tirado*[108] the Ninth Circuit Court of Appeals found that machine-generated evidence (without any substantial human intervention) is not hearsay. In this case the court found that a "pin" from Google Earth (satellite image software) was not an assertion by a person and was therefore not hearsay. The court stated as follows: "we join other circuits that have held that machine statements aren't hearsay".[109]

Consequently, the key issue in the United States in relation to computer generated evidence and hearsay is to determine whether the evidence is subject to input, assertions or conclusions by a person. If so, it is hearsay. If not, and the evidence is automatically generated, then subject to the other evidential conditions being satisfied (relevance, authenticity, best evidence and the probative value outweighing prejudicial effect), the evidence will be admissible. Of course, as in South Africa and other jurisdictions, even if the evidence is hearsay in nature, then it may still be admissible under one of the statutory exceptions (contained in the *Federal Rules of Evidence* or in an applicable State statute).

4.4 Comment

Many jurisdictions appear to favour electronic evidence being admissible without hearsay considerations if it is produced by a machine or a computer without human intervention.

Granted, there will always be a person involved in the genesis of machine- or computer-based evidence – whether to design, implement, maintain or repair - but this type of evidence is categorised by a system that does not rely on regular human input, and does not make any human assertions or observations. It can operate on an automated basis. For example, phone records or GPS data from Google Earth – there is a limited amount of human

---

108 *United States v Lizarraga-Tirado* 2015 WL 3772772 (9th Cir 2015).

109 *United States v Lizarraga-Tirado* 2015 WL 3772772 (9th Cir 2015) 7-8. The appeal court quotes the following cases in support of this conclusion: *United States v Lamons* 532 F 3d 1251, 1263 (11th Cir 2008); *United States v Moon* 512 F 3d 359, 362 (7th Cir 2008); *United States v Washington* 498 F 3d 225, 230 (4th Cir 2007); *United States v Hamilton* 413 F 3d 1138, 1142 (10th Cir 2005); *United States v Khorozian* 333 F 3d 498, 506 (3d Cir 2003).

involvement in their generation, and the credibility of the data as evidence derives predominantly from the system's being automated.

Consequently, in my view an accurate formulation of a rule applicable to such computer records would be the following: a data message will be real evidence (and not subject to hearsay considerations) where its credibility relies substantially (or predominantly) on a computer (or mechanical process).[110]

Similarly, if a litigant relies on the truth of a statement with human intervention or input, or a human observation or summary is contained therein, then that evidence will be regarded as hearsay and inadmissible, unless it falls into one of the hearsay admissibility exceptions, such as business records.

5 Suggestions for reform

In comments to the Law Reform Commission's Discussion Paper 131,[111] the view from the legal profession and academia is mixed. What follows below is a synopsis of the findings of the SALRC, including published comments from the legal profession and academia, in relation to the issues dealt with in this contribution (relevant to hearsay electronic evidence), together with a discussion thereon, and suggestions for law reform.

5.1 The definition of "data message"

The third issue covered in the SALRC's Discussion Paper 131 deals with the definition of data messages. The Paper asks if the definition of "data message" in the *ECT Act* should be revised.[112]

Ultimately, the SALRC concludes by noting that the current definition of data message (contained in the *ECT Act*) is problematic in that it strays from the Model Law by including the words "voice, where the voice is used in an automated transaction."

Moreover, some have cautioned against moving away from internationally accepted terminology,[113] and both the National Prosecuting Authority[114] and Legal Aid South Africa have expressed the view that the current definition

110 See, for example: *S v Ndiki* 2007 2 All SA 185 (Ck); *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W).
111 SALRC *Discussion Paper 131*.
112 SALRC *Discussion Paper 131* 27-32.
113 SALRC *Discussion Paper 131* 53.
114 SALRC *Discussion Paper 131* 53.

of data message can be "confusing."[115] As discussed in part one of this article, my view is that the definition should be amended.[116]

5.2 *Admissibility of data messages as evidence in legal proceedings in the context of hearsay*

In the light of the principle of functional equivalence,[117] it cannot be that section 15 of the *ECT Act* automatically prescribes that all data messages are admissible. As a result, South African courts have consistently found that the *ECT Act* does not override the normal rules applicable to hearsay.[118]

The *obiter dictum* in *Ndiki* (that all data messages should be treated as documentary hearsay),[119] which position is supported by the Law Society of South Africa,[120] should be avoided. As seen above, it would conflict with the internationally accepted position, and arguably it would not be conceptually correct.[121] Moreover the fact that drawing the distinction between real evidence and documentary evidence in the context of data messages can be difficult should not result in sacrificing conceptual clarity. If a court is unsure whether evidence is real or documentary, it can err on the side of caution and classify the evidence as documentary hearsay. This would mean subjecting the data message to a hearsay enquiry, where in terms of the *Law of Evidence Amendment Act* the court would in any event have the discretion to admit the evidence - if the interests of justice demand that that be done.

---

115 SALRC *Discussion Paper 131* 53-54.

116 Swales 2018 *PELJ* 3-5.

117 Swales 2081 *PELJ* 9.

118 *S v Brown* 2015 ZAWCHC 128 (17 August 2015) para 18; *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W) 172-173, *S v Ndiki* 2007 2 All SA 185 (Ck) para 31, *La Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a La Enterprises* 2011 4 SA 577 (GSJ) para 13; Theophilopoulos 2015 *TSAR* 474-475; Watney 2009 *JILT* 8-9; Hofman and De Jager "South Africa" 776-777.

119 *S v Ndiki* 2007 2 All SA 185 (Ck) para 33. The court relies on the opinion of Bilchitz "Law of Evidence" 796 to form the view that all data messages should be treated as hearsay. Although the argument of Bilchitz is noted (that all computer-based evidence relies on some human intervention or input), it is in my view semantics and outdated in 2018. As with the position in several foreign jurisdictions, including England, Canada and the United States of America, if a data messages relies substantially on a computer for its "credibility", then that evidence must be treated as real in nature. A court will always have the discretion to give the evidence very low weight if there are doubts about its accuracy and/or reliability.

120 SALRC *Discussion Paper 131* 63.

121 Hofman and De Jager "South Africa" 777 and particularly fn 3 thereof; Theophilopoulos 2015 *TSAR* 474.

Where the evidence is clearly automated and depends upon the credibility of a computer (or as Theophilopoulos puts it: an information system automatically generated data message which does not require the input of a human mind) then it must be treated as real evidence and cannot be subject to a hearsay enquiry.[122]

As with other issues in the SALRC paper, there is no common ground among the comments received,[123] and there is support for data messages to be admissible if relevant and authentic (regardless of hearsay),[124] as well as support from both the South African Police Services and the Law Society of South Africa for the position that all data messages constitute hearsay.[125]

The SALRC supports the view that hearsay evidence in a data message should be treated the same as a paper-based document (in line with the principle of functional equivalence).[126] Ultimately, however, the SALRC proposes a *Law of Evidence Amendment Bill*[127] to clarify the distinction between various types of electronic evidence (real or documentary), and to clarify the interaction between the statutory exceptions to the hearsay rule.

If the proposed amendment bill is supported, this will mean that the issue of whether a data message can constitute hearsay in the context of the *Law of Evidence Amendment Act* is absolutely resolved (with the answer being: *data messages can contain hearsay*). However, the rejection of the amendment bill (or if its promulgation takes place in a limited or partial form) will mean that technically there is still some doubt as to whether or not a data message can constitute hearsay (even though the cases discussed above appear to have all but removed any doubt).

Consequently, if there is no amendment bill as suggested in Annexure A to the SALRC Discussion Paper 131, for the sake of clarity and best practice, there must be an amendment to the *Law of Evidence Amendment Act* with reference to data messages. Moreover, in the absence of drastic law reform, the *Civil Proceedings Evidence Act* and the *Criminal Procedure Act* should similarly be amended to take account of (and specifically refer to where

122 Theophilopoulos 2015 *TSAR* 474.
123 SALRC *Discussion Paper 131* 62-64.
124 SALRC *Discussion Paper 131* 63.
125 SALRC *Discussion Paper 131* 63.
126 SALRC *Discussion Paper 131* 67.
127 SALRC *Discussion Paper 131* 67, 89-95.

necessary) data messages, and to ensure that there is consistency in the definition of a document.[128]

Finally, in the context of limited law reform, the *ECT Act* also requires amendment in order to align it with the statutory exceptions to the hearsay rule.

5.3 Distinguishing between various types of electronic evidence

The determination as to whether a data message is real evidence or documentary evidence will dictate the admissibility requirements applicable;[129] and importantly for the present purposes will determine whether a hearsay enquiry is necessary. (By its nature, real evidence is what it purports to be and it cannot be subject to the exclusionary hearsay rules.)

The SALRC supports a distinction between automated data messages and data messages made by a person.[130] In an article written after the publication of the SALRC report, even though not done so expressly, Theophilopoulos appears to agree by stating:

> a distinction should be made between 'an information system automatically generated data message which does not require the input of a human mind' – a real data message; and 'an information system produced and stored data message based on the input of a human mind' – a hearsay data message.[131]

Moreover, recent cases in the form of *Ndlovu, Ndiki* and *LA Consortium*, amongst others, all endorse this approach. As seen above, this approach is also consistent with foreign law.[132]

Some academics[133] draw this distinction with reference to copyright cases[134] by referring to "computer-assisted" and "computer-generated" data.[135] The choice of the terms the legislature, SALRC or the SCA (as the case may be) decide to use to resolve this debate is probably secondary.

---

128 See Annexure C of SALRC *Discussion Paper 131,* where there are extracts from legislation that will require amendment if the proposed amendment bill is not enacted.

129 SALRC *Discussion Paper 131* 34-37.

130 SALRC *Discussion Paper 131* 70.

131 Theophilopoulos 2015 *TSAR* 474; Hofman 2006 *SACJ* 257, 269.

132 Theophilopoulos 2015 *TSAR* 474; SALRC *Discussion Paper 131* 70, where the SALRC confirm that the international position supports this distinction.

133 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 445.

134 *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd* 2006 4 SA 458 (SCA).

135 *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd* 2006 4 SA 458 (SCA) para 31.

The key principle is the endorsement of a distinction between types of electronically produced machine or computer evidence.

In the proposed evidence amendment bill (Annexure A to the SALRC Discussion Paper 131), section 5 reads as follows:

> 5. Evidence produced by processes, machines and other devices
>
> 5.1 Subject to the provisions of this Act and any other law, evidence that is produced wholly or partly by a machine, device, or technical process –
>
> (i) is admissible in all legal proceedings; and
>
> (ii) may be produced as an electronic document.
>
> 5.2 A statement which has been generated wholly by a machine, device or technical process does not constitute hearsay evidence.
>
> 5.3 Subject to the provisions of this Act or unless the Court orders otherwise, the admissibility of evidence produced in terms of this section should be established by the oral testimony of a witness or witnesses.

An electronic document (in section 5(1)(ii)) is defined as follows:

> 'Electronic document' means data that are recorded or stored on any medium in or by a computer system or other similar device, and includes a display, printout or other output of that data…

There is no definition of the term data message, nor is there a definition of data in this proposed amendment. The likelihood is that there will be a reliance on the definitions in the *ECT Act* and/or the *Cybercrimes and Cybersecurity Bill* (when it becomes law). Moreover, the definition of hearsay is the same as that contained in the *Law of Evidence Amendment Act*.

In the context of the proposed section 5 of the amendment bill, the key question, in my view, is: When will a data message be wholly generated by a machine, device or technical process? [136]

As discussed in part one of this article,[137] the core concern raised by some is that all computer-generated evidence has human involvement at some stage, and a court might take a literal approach and exclude evidence on the basis that there has been some human involvement in the maintenance or storing of the data.

---

136 In terms of the proposed s 5(2), a statement generated wholly by a machine will not be hearsay.

137 Swales 2018 *PELJ* 8-23.

Consequently, I would suggest replacing the word "wholly" with "substantially". As with the *Law of Evidence Amendment Act*, this may at first create room for some legal gymnastics, but a court will be seized with determining whether the data or output is substantially automated, or relies substantially on the credibility of a machine (such as phone records or GPS data). This minor amendment would also satisfy conceptual criticisms[138] that at some stage a human being is always involved in machine-generated evidence (or that in reality all computer based evidence relies on the credibly of a human being – the person who designs, implements, controls, maintains, *etcetera*).

The other question, which may be semantics, is: In terms of section 5(2) of the proposed bill, under what circumstances will a print-out from a computer or technical device be regarded as a statement? It may be that the SALRC intended to include any output from a computer (all forms of electronic evidence) and refer to it as a statement. However, the word statement could be misconstrued (or a situation could develop where an output may not be a statement). Consequently, I would suggest that the word statement be replaced with "any output", or "data" to avoid any confusion.

Consequently, it appears that in order to foster clarity and certainty, law reform is required. The most effective (and cleanest) approach appears to be the promulgation of legislation along the lines set out in Annexure A to the SALRC Discussion Paper 131. That said, this approach would also be the most drastic and require the most change in our current legal framework.

Conversely, if there is no support for the amendment bill, or if it does not deal with the distinction between real and documentary electronic evidence, then as suggested by the South African Police Services[139] the *ECT Act* should be amended (section 15 thereof). The amendment should make a clear distinction between mechanically produced evidence without any substantial human intervention (real evidence), and mechanically produced evidence with substantial human intervention (documentary hearsay). Put differently,[140] and using copyright terminology, a distinction should be drawn between "computer-assisted" and "computer-generated" output.

138 Bilchitz "Law of Evidence" 796; Zeffertt and Paizes *South African Law of Evidence* 432-433; SALRC *Discussion Paper 131* 68-69.

139 SALRC *Discussion Paper 131* 69.

140 Schwikkard and Van der Merwe *Principles of Evidence* 4th ed 445, referring to *Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd* 2006 4 SA 458 (SCA) para 31.

5.4 Statutory exceptions to the hearsay rule

"Confusing" and "complicated" – two common descriptions of the statutory exceptions to the hearsay rule.[141] Why is this the case? Potentially, a legal practitioner must consider multiple sources of law,[142] and a variety of (at times) conflicting and conceptually grey cases when determining whether a hearsay exception applies. This is less than ideal and leads to misunderstanding and inconsistent application.

In addition, the business-records exception created by section 15(4) of the *ECT Act* has received severe academic criticism.[143] Moreover, in comments received by the SALRC, the South African Police Services and Legal Aid submit that in the context of criminal proceedings the section unjustly shifts the onus of proof and may well be unconstitutional.[144] Conversely, the National Prosecution Authority and the Law Society of South Africa feel it should remain unchanged, but perhaps be given a restrictive interpretation.

Be that as it may, if the amendment bill proposed by the SALRC is promulgated in its current form it will seek to repeal section 3 of the *Law of Evidence Amendment Act*; section 15(4) of the *ECT Act*; section 27-38 of the *CPEA,* and sections 221, 222 and 236 of the *CPA*.

It will replace these with a singular piece of legislation which facilitates a more coherent, less fragmented approach.[145] The primary sections relevant in the current context will be section 3 (the general hearsay provision – similar to section 3 of the *Law of Evidence Amendment Act*), and section 4 (the business records exception). The SALRC have not tried to reinvent the wheel, and the legislation is familiar and internationally consistent. The primary purpose of the law reform would be to promote certainty and remove the current confusion (which appears to be caused by the fragmentation of the relevant legislation in use at the moment).

Chapter 5 of the most recent SALRC report[146] proposes three options for law reform in the context of electronic evidence. These are: (option 1) the retention of the status quo with the minor statutory reform of the existing

---

141 SALRC *Discussion Paper 131* 31.

142 The *Law of Evidence Amendment Act*, the *Civil Proceedings Evidence Act*, the *Criminal Procedure Act* and the *Electronic Communications and Transactions Act*.

143 See the discussion in para 3.4 above.

144 SALRC *Discussion Paper 131* 76.

145 SALRC *Discussion Paper 131* 87-88, where the SALRC states that the proposed bill is reflective of practice in several commonwealth countries and consistent with the *Model Law*, 1996.

146 SALRC *Discussion Paper 131* 83-88.

legislation; (option 2) the retention of the existing regulatory framework with the introduction of additional legislation to supplement it; and (option 3) the reform of the current regulatory framework with the repeal of existing laws and the introduction of a single piece of legislation. The SALRC provisionally recommends option 3, with the introduction of new legislation (Annexure A to the SALRC Discussion Paper 131). This option would amount to a comprehensive overhaul of the current legal framework.

Given the analysis above, in my view the approach recommended by the SALRC should be endorsed. In addition to resolving the more serious issues relating to admissibility and the weight of electronic evidence, it would also clarify the current inconsistency in some definitions in civil and criminal proceedings.

6 Conclusion

While electronic evidence is certainly susceptible[147] to manipulation and evolving technology, its use is now commonplace and ubiquitous. A plethora of expertise is readily available to detect and comment on manipulation where that may be at issue, and the law must adapt.[148] South Africa cannot sustain a legal position where the exclusion of evidence is justified because it is new and/or uncertain. The traditional principles of evidence need not be re-written, but in certain instances some adaption is required.

South African courts and academics have been almost entirely *ad idem* in their determination that electronic evidence can constitute hearsay within the meaning of the *Law of Evidence Amendment Act*. Notwithstanding the imminent promulgation of the *Cybercrimes and Cybersecurity Bill*, the evidentiary position will remain unchanged by that legislation.[149]

The categorisation of a data message as either real evidence or documentary evidence will play a pivotal role in determining the admissibility requirements the evidence must face. With this in mind, most recent South African cases dealing with the admissibility of electronic evidence appear to accept that a distinction must be drawn between evidence generated by a

147 SALRC *Issue Paper 27* 7-13, where apparent difficulties with electronic evidence are discussed in detail.

148 *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 5 SA 604 (KZD) para 2, where it is stated in the context of technological change that "it is therefore not unreasonable to expect the law to recognise such changes and accommodate it"; *Heroldt v Wills* 2013 2 SA 530 (GSJ) para 8; Hofman and De Jager "South Africa" 761; Theophilopoulos 2015 *TSAR* 461.

149 Based on the *Cybercrimes and Cybersecurity Bill* B6-2017.

computer without substantial human involvement (real evidence and no hearsay enquiry) and evidence where there is human involvement or assertions (documentary hearsay and subject to the exclusionary hearsay rules). However, the distinction is not always clearly articulated and/or justified, and the statutory exception created in section 15(4) of the *ECT Act* remains contentious for many academics.

That notwithstanding, it appears to be settled foreign law that electronic evidence that relies on a computer or automated system (such as phone records) should be introduced into evidence without the need for a hearsay enquiry (of course, subject to any other exclusionary rule of evidence applicable in that jurisdiction, such as relevance, authenticity or the best evidence rule).

The current position in South Africa, with a multitude of sources of law, differing definitions, some conflicting case law, some questionable *obiter* statements and, importantly, no real clarity on the distinction between different types of electronic evidence, would benefit greatly from law reform, whether minor reform to existing statutes or a more aggressive overhaul of the legislative framework as proposed by Annexure A to the SALRC's Discussion Paper 131.

Finally, and based on the analysis contained in this two-part article, there must be law reform in at least the following areas: the definition of data messages; the definition of the term document in the statutes applicable to the hearsay exceptions; a distinction between types of electronic evidence insofar as computer-generated evidence with human intervention and without human intervention is concerned; and more cohesion and alignment with the statutory hearsay exceptions.

Bibliography

Literature

Bellengere *et al Law of Evidence*
Bellengere A *et al The Law of Evidence in South Africa* (Oxford University Press Cape Town 2013)

Bilchitz "Law of Evidence"
Bilchitz D "Law of Evidence" in Lewis C *et al* (eds) *Annual Survey of South African Law* (Juta Johannesburg 1998) 735-821

Boyd *Canadian Law*
Boyd N *Canadian Law: An Introduction* 5th ed (Nelson Education Toronto 2011)

De Villiers 2010 *TSAR*
De Villiers DS "Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)" 2010 *TSAR* 720-734

Duvenhage *Evidential Analysis*
Duvenhage A *An Evidential Analysis of Section 15(4) of the Electronic Communications and Transactions Act 25 of 2002* (LLM-dissertation University of Pretoria 2016)

Esler 2007 *DEESLR*
Esler BW " Lorraine v Markel: Unnecessarily Raising the Standard for Admissibility of Electronic Evidence" 2007 *DEESLR* 80-82

Fourie *Using Social Media as Evidence*
Fourie PF *Using Social Media as Evidence in South African Courts* (LLM-dissertation North-West University 2016)

Frieden and Murray 2011 *Rich J L & Tech*
Frieden JD and Murray LM "The Admissibility of Electronic Evidence under the Federal Rules of Evidence" 2011 *Rich J L & Tech* 1-39

Friedman and Hayden *American Law*
Friedman LM and Hayden GM *American Law: An Introduction* (Oxford University Press New York 2017)

Gallavin and Mason "Hearsay"
Gallavin C and Mason S "Hearsay" in Mason S and Seng D (eds) *Electronic Evidence* 4th ed (Institute of Advanced Legal Studies London 2017) 70-87

Hofman 2006 *SACJ*
Hofman J "Electronic Evidence in Criminal Cases" 2006 *SACJ* 257-275

Hofman and De Jager "South Africa"
Hofman J and De Jager J "South Africa" in Mason S (ed) *Electronic Evidence* 3rd ed (LexisNexis Butterworths London 2012) 761-797

Kemp 2012 *NC JOLT*
Kemp LJ "Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations)" 2012 *NC JOLT* 16-30

Leroux 2004 *IRLCT*
Leroux O "Legal Admissibility of Electronic Evidence" 2004 *IRLCT* 193-220

Mason, Freedman and Patel "England and Wales"
Mason S, Freedman C and Patel S "England and Wales" in Mason S (ed) *Electronic Evidence* 3rd ed (LexisNexis Butterworths London 2012) 327-474

Paciocco and Stuesser *Law of Evidence*
Paciocco D and Stuesser L *The Law of Evidence* 7th ed (Irwin Law Toronto 2015)

Papadopoulos and Snail *Cyberlaw@SA III*
Papadopoulos S and Snail S (eds) *Cyberlaw@SA III: The Law of the Internet in South Africa* 3rd ed (Van Schaik Pretoria 2012)

Reed "Admissibility and Authentication of Computer Evidence"
Reed C "The Admissibility and Authentication of Computer Evidence – A Confusion of Issues" in 5th Annual *British and Irish Legal Education Technology Association Conference* (1990) 1-9

SALRC *Discussion Paper 131*
South African Law Reform Commission *Discussion Paper 131, Project 126 - Review of the Law of Evidence* (SALRC Pretoria 2014)

SALRC *Issue Paper 27*
South African Law Reform Commission *Issue Paper 27, Project 126 – Review of the Law of Evidence: Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (SALRC Pretoria 2010)

Schwerha, Bagby and Esler "United States of America"
Schwerha JJ, Bagby JW and Esler BW "United States of America" in Mason S (ed) *Electronic Evidence* 3rd ed (LexisNexis Butterworths London 2012) 797-835

Schwikkard and Van der Merwe *Principles of Evidence* 3rd ed
Schwikkard PJ and Van der Merwe SE *Principles of Evidence* 3rd ed (Juta Cape Town 2009)

Schwikkard and Van der Merwe *Principles of Evidence* 4th ed
Schwikkard PJ and Van der Merwe SE *Principles of Evidence* 4th ed (Juta Cape Town 2016)

Smith 1983 *Crim L R*
Smith JC "The Admissibility of Statements by Computer" 1983 *Crim L R* 389-391

Swales 2018 *PELJ*
Swales L "An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One" 2018 *PELJ* https://doi.org/10.17159/1727-3781/2018/v21i0a2916

Tapper *Cross and Tapper on Evidence*
Tapper C *Cross and Tapper on Evidence* 12th ed (Oxford University Press London 2010)

Theophilopoulos 2015 *TSAR*
Theophilopoulos C "The Admissibility of Data, Data Messages, and Electronic Documents at Trial" 2015 *TSAR* 461-481

Underwood and Penner *Electronic Evidence*
Underwood GJ and Penner J *Electronic Evidence in Canada* (Carswell Toronto 2010)

Van der Merwe *et al Information and Communications Technology Law*
Van der Merwe D *et al Information and Communications Technology Law* 2nd ed (LexisNexis Durban 2016)

Watney 2009 *JILT*
Watney M "Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position" 2009 *JILT* 1-13

Zeffertt and Paizes *South African Law of Evidence*
Zeffertt DT and Paizes AP *The South African Law of Evidence* 2nd ed (LexisNexis Durban 2009)

Case law

England

Castle v Cross [1985] 1 All ER 87

McDonald v R [2011] EWCA Crim 2933

R (on the application of O) v Coventry Justices [2004] All ER (D) 78

R v Spiby [1990] 91 Cr App R 186

Canada

R v Hall [1998] BCJ 2515

R v McCulloch [1992] BCJ 2282

R v Mondor 2014 ONCJ 135

Saturley v CIBC World Markets Inc 2012 NSSC 226

South Africa

Absa Bank Ltd v Le Roux 2014 1 SA 475 (WCC)

CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens 2012 5 SA 604 (KZD)

Director of Public Prosecution v Modise 2012 1 SACR 553 (GSJ)

Ex parte Rosch 1998 1 All SA 319 (W)

Firstrand Bank Limited v Venter 2012 JOL 29436 (SCA)

Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited 2005 ZAGPHC 311 (22 August 2005)

Haupt t/a Softcopy v Brewers Marketing Intelligence (Pty) Ltd 2006 4 SA 458 (SCA)

Heroldt v Wills 2013 2 SA 530 (GSJ)

La Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd In re: MTN Service Provider (Pty) Ltd v La Consortium & Vending CC t/a La Enterprises 2011 4 SA 577 (GSJ)

Narlis v South African Bank of Athens 1976 2 SA 573 (A)

Ndlovu v Minister of Correctional Services 2006 4 All SA 165 (W)

S v Brown 2015 ZAWCHC 128 (17 August 2015)

S v Ndiki 2007 2 All SA 185 (Ck)

S v Van der Linde 2016 3 All SA 898 (GJ)

Sublime Technologies (Pty) Ltd v Jonker 2010 2 SA 522 (SCA)

Trend Finance (Pty) Ltd v Commissioner for the South African Revenue Service 2005 4 All SA 657 (C)

United States of America

Lorraine v Markel American Insurance Company 241 FRD 534

Telewizja Polska USA Inc v Echostar Satellite Corp 2004 WL 2367740

U-Haul Intern Inc. v Lumbermens 576 F 3d 1040 (9th Cir 2009)

United States v Hamilton 413 F 3d 1138, 1142 (10th Cir 2005)

United States v Khorozian 333 F 3d 498, 506 (3d Cir 2003)

United States v Lamons 532 F 3d 1251, 1263 (11th Cir 2008)

United States v Lizarraga-Tirado 2015 WL 3772772 (9th Cir 2015)

United States v Moon 512 F 3d 359, 362 (7th Cir 2008)

United States v Rollins 2004 WL 26780

United States v Washington 498 F 3d 225, 230 (4th Cir 2007)

Legislation

England

Civil Evidence Act, 1995

Criminal Justice Act, 2003

Canada

Canada Evidence Act, 1985

Uniform Electronic Evidence Act, 1999

South Africa

Civil Proceedings Evidence Act 25 of 1965

Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill B6-2017

Electronic Communications and Transactions Act 25 of 2002

Law of Evidence Amendment Act 45 of 1988

United States of America

Federal Rules of Evidence, 1975

International instruments

United Nations Commission on International Trade Law Model Law on Electronic Commerce (1996)

Internet sources

CIA 2017 https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html
Central Intelligence Agency 2017 *World Fact Book*: *Field Listing Legal System* https://www.cia.gov/library/publications/the-world-factbook/fields/2100.html accessed 8 June 2017

Groulx, Rothman and Zawidzki 2011 https://www.dentons.com/~/media/FMC%20Import/publications/pdf/a/Admissibility%20Understanding%20Types%20and%20Sources%20of%20Electronic%20Evidence.ashx
Groulx K, Rothman C and Zawidzki M 2011 *Admissibility: Understanding Types and Sources of Electronic Evidence* https://www.dentons.com/~/media/FMC%20Import/publications/pdf/a/Admissibility%20Understanding%20Types%20and%20Sources%20of%20Electronic%20Evidence.ashx accessed 1 February 2017

Joseph 1999 http://www.jha.com/us/articles/viewarticle.php?8
Joseph GP 1999 *A Simplified Approach to Computer-Generated Evidence and Animations* http://www.jha.com/us/articles/viewarticle.php?8 accessed 8 June 2017

Internet World Stats 2017 http://www.internetworldstats.com/africa.htm#za
Internet World Stats 2017 *Usage and Population Statistics: South Africa* http://www.internetworldstats.com/africa.htm#za accessed 1 February 2018

Miskel 2015 http://www.emilymiskel.com/blog/admissibility-of-digital-evidence-in-a-family-case/
Miskel E 2015 *Admissibility of Digital Evidence in a Family Case* http://www.emilymiskel.com/blog/admissibility-of-digital-evidence-in-a-family-case/ accessed 8 June 2017

Pendleton 2013 http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/
Pendleton A 2013 *Admissibility of Electronic Evidence: A New Evidentiary Frontier* http://mnbenchbar.com/2013/10/admissibility-of-electronic-evidence/ accessed 8 June 2017

Seng and Chakravarthi 2003 https://www.agc.gov.sg/DATA/0/Docs/PublicationFiles/Sep_03_ComputerOutput.pdf
Seng D and Chakravarthi S 2003 *Technology Law Development Group, Singapore Academy of Law - Computer Output as Evidence: Consultation Paper* https://www.agc.gov.sg/DATA/0/Docs/PublicationFiles/Sep_03_ComputerOutput.pdf 14 accessed 2 March 2017

Thomson 2012 https://www.americanbar.org/content/dam/aba/events/science_technology/mobiledevices_new_challenges_admissibility_of_electronic_device.authcheckdam.pdf
Thomson LL 2012 *Mobile Devices: New Challenges for Admissibility of Electronic Evidence* https://www.americanbar.org/content/dam/aba/events/science_technology/mobiledevices_new_challenges_admissibility_of_electronic_device.authcheckdam.pdf accessed 2 March 2017

List of Abbreviations

CIA	Central Intelligence Agency
CPA	Criminal Procedure Act 51 of 1977
CPEA	Civil Proceedings Evidence Act 25 of 1965
Crim L R	Criminal Law Review
DEESLR	Digital Evidence and Electronic Signature Law Review
ECT Act	Electronic Communications and Transactions Act 25 of 2002
IRLCT	International Review of Law, Computers and Technology
JILT	Journal of Information, Law and Technology
Model Law, 1996	United Nations Commission on International Trade Law Model Law on Electronic Commerce, 1996

NC JOLT	North Carolina Journal of Law and Technology
PELJ	Potchefstroom Electronic Law Journal
Rich J L & Tech	Richmond Journal for Law and Technology
SACJ	South African Journal of Criminal Justice
SALRC	South African Law Reform Commission
TSAR	Tydskrif vir die Suid-Afrikaanse Reg