AN ANALYSIS OF THE REGULATORY ENVIRONMENT GOVERNING ELECTRONIC EVIDENCE IN SOUTH AFRICA: SUGGESTIONS FOR REFORM

Name: Lee Swales

Contact e-mail: swalesl@ukzn.ac.za or lee@thomsonwilks.co.za

Supervisors: Professor PJ Schwikkard and Professor Caroline Ncube

Thesis Presented for the Degree of

DOCTOR OF PHILOSOPHY

in the Department of Public Law

UNIVERSITY OF CAPE TOWN

December 2018

Table of Contents

Abbreviations

Brown	*S v Brown* 2016 (1) SACR 206 (WCC)
CJA	Criminal Justice Act 2003
CEA	Civil Evidence Act 1995
CPA	Criminal Procedure Act 51 of 1977
CPEA	Civil Proceedings Evidence Act 25 of 1965
CJTL	Canadian Journal of Law and Technology
Delsheray Trust	*Trustees for the time Being of the Delsheray Trust* v *ABSA Bank Limited* [2014] 4 All SA 748 (WCC)
ECT Act	Electronic Communications and Transactions Act 25 of 2002
Ex Parte Rosch	*Ex parte Rosch* [1998] 1 All SA 319 (W)
ICT	Information, communication and technology
LA Consortium	*LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ)
LSSA	Law Society of South Africa
Meyer	*S v Meyer* 2017 JDR 1728 (GJ)
Model Law, 1996	United Nations Commission on International Trade Law Model Law on Electronic Commerce of 1996
Modise	*Director of Public Prosecution v Modise* 2012 (1) SACR 553 (GSJ)
Mthimkulu	*S v Mthimkulu* 1975 (4) SA 759 (A)
Narlis	*Narlis v South African Bank of Athens* 1976 (2) SA 573 (A)
Ndiki	*S v Ndiki* 2008 (2) SACR 252 (Ck)
Ndlovu	*Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W)
NPA	National Prosecuting Authority
PELJ	Potchefstroom Electronic Law Journal
POCA	Prevention of Organised Crime Act 121 of 1998
SACJ	South African Journal of Criminal Justice

SALJ	South African Law Journal
SALRC	South African Law Reform Commission
SAMLJ	South African Mercantile Law Journal
SAPS	South African Police Service
SCA	Supreme Court of Appeal
TSAR	Tydskrif vir die Suid-Afrikaanse Reg
UECA	Uniform Electronic Commerce Act, Canada
UNCITRAL	United Nations Commission on International Trade Law
VAT	Value Added Tax

Acknowledgements

I am eternally grateful for my beautiful and patient wife, Lindy. Without her support this research would not be possible – thank you for everything (and sorry for being so grumpy). You truly are a super-woman, and super-mom.

The University of KwaZulu-Natal provided me with the opportunity to present this research, and I will always be thankful for the support. I had the luxury of a six-month sabbatical to concentrate on getting over the line, and I am extremely fortunate to have had a plethora of colleagues who were always willing to assist with comments and moral support. It is hard to single any one person out, but specific thanks to my mentor, friend, and evidence expert – Adrian Bellengère, who introduced me to my supervisors, and gave me tremendous assistance with this research (as well as assisting with propelling my academic career forward in general).

Finally, thank you to my supervisors – Professor PJ Schwikkard, and Professor Caroline Ncube. I appreciate the assistance, encouragement, and insight. Without your support this research would have never been possible. I thoroughly enjoyed my time at UCT, and the assistance I received was always prompt, professional and comprehensive; I look forward to collaborating again with you both in the future.

Abstract

Technology has developed rapidly over the last three decades. Information is regularly transmitted and stored electronically – *and only electronically*. The use of mobile phones, e-mail, social media, and various electronic messaging services are ubiquitous. However, there are several areas of confusion and inconsistent application in the regulation of electronic evidence in South Africa. As a result, the South African Law Reform Commission ('SALRC') has suggested three different methods for law reform, and recommends the most aggressive of these options in the form of a *Law of Evidence Bill*. In this thesis, I agree with many of the findings made by the SALRC, but I disagree with the option selected for law reform. As suggested by several other stakeholders, rather than a drastic overhaul of the current legal framework, a more cautious amendment of existing legislation would be the more preferable approach.

Electronic evidence is primarily regulated by the Electronic Communications and Transactions Act 25 of 2002 ('ECT Act'), and although it is ageing, it still achieves one of its primary functions, namely facilitating the admissibility and evidential weight of electronic evidence. However, there is room for improvement.

This research addresses six primary questions relating to electronic evidence: Namely, whether the definition of data message requires amendment; whether the ECT Act liberates data messages from the exclusionary hearsay rules; whether a presumption of regularity exists in South Africa; whether section 15 of the ECT Act requires amendment; whether it is appropriate to apply different evidentiary considerations to electronic evidence in civil and criminal proceedings; and finally, this research considers the SALRC's selected option for law reform.

This thesis, which adopts a descriptive form of desktop research, concludes that the ECT Act is sufficient to regulate the admissibility of electronic evidence, but that it requires amendment in certain areas, together with the amendment of related legislation in relation to 1) the definition of data message; 2) the hearsay exceptions; 3) terminology and consistency in relation to electronic evidence in South African legislation; and 4) the discovery of electronic evidence.

UNIVERSITY OF CAPE TOWN

DOCTORAL DEGREES BOARD

APPROVAL BY THE DOCTORAL DEGREES BOARD TO INCLUDE PUBLICATIONS

I confirm that I have been granted permission by the University of Cape Town's Doctoral Degrees Board to include the following publications in my thesis:

Publication
L Swales 'The regulation of electronic signatures: Time for review and amendment' (2015) 132 *SALJ* 257 – 270
L Swales 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One' (2018) 21 *PELJ* 2 – 24
L Swales 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two' (2018) 21 *PELJ* 10 – 18
L Swales 'Electronic instruments – a presumption of reliability, a presumption of regularity, judicial notice, or none of the above?' (2018) 2 SACJ *(upcoming: to be published in the second part of the 2018 edition)*

Signed	Signed by candidate	Date	12/12/2018

1.1 INTRODUCTION AND RESEARCH CONTEXT

Technology is inseparably integrated into our lives,[1] and has become an indispensable part of modern life.[2] As a result, we have witnessed a sea-change in relation to methods of communication[3] – societies' increasing reliance on technology and electronic devices[4] means that basic communication, interaction and transaction methodologies have been indelibly altered.[5] There is no going-back; and although this shift in communication norms is sometimes described with exaggeration,[6] growth will likely continue.[7] It seems certain that future generations will be increasingly technologically reliant and sophisticated.[8] Consequently, the law must adapt.[9]

---

[1] E Casey *Digital Evidence and Computer Crime* 3 ed (2011) xxi.
[2] P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) 437.
[3] T Holt et al *Cybercrime and Digital Forensics* (2015) 1 – 3.
[4] Schwikkard & van der Merwe op cit note 2 at 437 – 438; A Bellengère et al *The Law of Evidence in South Africa* (2013) 73; D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) ch 5; S Papadopoulos & S Snail (eds) *Cyberlaw@SA III* (2012) 315. See also See also D Zeffertt & A Paizes *The South African Law of Evidence* 3 ed (2017) at 455 – 460, 976 – 981.
[5] *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD) para 2; *Heroldt v Wills* 2013 (2) SA 530 (GSJ) para 8; *Trustees for the time being of the Delsheray Trust v ABSA Bank Limited* [2014] 4 All SA 748 (WCC) para 18 where the court noted: 'It is well known that modern technological developments have brought about a revolution in the way that information, including legal information, is captured and disseminated.'
[6] W Jacobs 'The Electronic Communications and Transactions Act: Consumer Protection and Contracts' (2004) 16 *SAMLJ* 556 – 557.
[7] Internet World Stats 2018 *http://www.internetworldstats.com/africa.htm#za*, accessed on 17 April 2016 and 31 July 2018. Roughly 53.7% of South Africa's population had Internet access as at December 2017. In 2008, the South African internet penetration rate was approximately 9%.
[8] *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association* 2014 (2) SA 569 (GSJ) para 19 where, obiter, the court noted: 'information technology and the use of the internet is now commonplace' and para 28 where it is noted that 'email is perhaps the most convenient means of communicating whether for work-related activities or socially'. See also D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 1)' (2010) 3 *TSAR* 558 – 575; D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)' (2010) 4 *TSAR* 720 – 735; J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 257 – 275.
[9] *Heroldt v Wills* supra note 5 at para 8 where it was stated: 'The pace of the march of technological progress has quickened to the extent that the social changes that result therefrom require high levels of skill not only from the courts, which must respond appropriately, but also from the lawyers who prepare cases…' See also *CMC Woodworking Machinery* supra note 5 para 2 where it was stated, in the context of technological change, that 'it is therefore not unreasonable to expect the law to recognise such changes and accommodate it.' See further C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461; J Hofman & J de Jager 'South Africa' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 761.

In a legal context, the transformation of communication methodologies has affected the administration of justice,[10] presented some challenges[11] to various fields of law, and necessitated a plethora of new legislative instruments.[12] In particular, the law of evidence and the law relating to information, communication and technology (ICT) are faced with several unique and novel challenges.[13]

With the exponential increase in internet use (read together with the inevitable change in communication methodologies),[14] one would expect concomitant amendments to the legislative environment regulating the characteristics and admissibility of *electronic evidence*.[15] However, the required change to the legal framework in the ICT environment has, thus far, been conservative[16] and hesitant[17] – presumably to ensure legal certainty, and clarity.

As at October 2018, the regulatory environment governing electronic commerce is dated and showing its age – it requires amendment to accommodate technological development, and in order to ensure consistency and clarity. In this regard, the South African Law Reform Commission (SALRC) suggests three different methodologies for law reform, and ultimately recommends the most aggressive of these three options[18] in the guise of a *Law of Evidence Bill*.[19] Although this research, holistically, agrees with the SALRC and its findings, it disagrees with the selected option for law reform. Rather than a drastic overhaul of the current legal framework, to ensure internationally compliant and conceptually sound

[10] M Beazley *Social Media and the Courts: Service of Process* Fourth Judicial Seminar on Commercial Litigation (2013) *http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/Pre-2015%20Speeches/Beazley/beazley_160513.pdf,* accessed 17 April 2016.
[11] *Heroldt v Wills* supra note 5 at para 9 where the court noted that there is a 'dearth of case law on the question of social media'. See further Van der Merwe et al op cit note 4 at 1 and 14; De Villiers (1) op cit note 8 at 558.
[12] For example, in South Africa: the Electronic Communications and Transactions Act 25 of 2002; the Protection of Personal Information Act 4 of 2013, and the Regulation of Interception of Communications and Provision of Communication Related Information Act 70 of 2002.
[13] Schwikkard & van der Merwe op cit note 2 at 437; D Zeffertt and A Paizes *Essential Evidence* (2010) 268-270; S Papadopoulos & S Snail (eds) *Cyberlaw@SA III* (2012) 315 – 317.
[14] *CMC Woodworking Machinery* supra note 5 at para 2.
[15] As an umbrella term, and for purposes of this research, the terms data message and electronic evidence will be used interchangeably. See, for example, *S v Meyer* 2017 JDR 1728 (GJ) para 298 where the court uses the term *electronic* evidence. See also Hofman & de Jager op cit note 9 at 761 where the authors use the same term, and note that 'data messages do not fit comfortably into the traditional categories of excluded and admitted evidence'. As to terminology (data messages and electronic evidence), see further the discussion in chapter 2 below in paragraph 2.1.
[16] Schwikkard & van der Merwe op cit note 2 at 438.
[17] M Watney 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 *Journal of Information, Law and Technology* 3.
[18] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 86 – 88 for a summary of the three proposed options for law reform.
[19] Attached hereto as Annexure A.

legislation, a more cautious amendment of existing legislation is the preferable approach in the short to medium term.[20]

1.2 NATURE OF ELECTRONIC EVIDENCE

In terms of the Electronic Communications and Transactions Act 25 of 2002 (ECT Act), the correct term to describe electronic evidence is *data messages* and/or *data*.[21] This follows the position of the United Nations Commission on International Trade Law (UNCITRAL), and the Model Law on Electronic Commerce of 1996 (Model Law, 1996).[22] Although there is no one single, definitive definition for electronic evidence, in the latest edition of *Electronic Evidence*,[23] the authors define it as:

> data (comprising the output of analogue devices or data in digital form) that is manipulated, stored or communicated by any manufactured device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence

There are a number of devices and technologies that produce electronic evidence: They are too numerous to exhaustively catalogue.[24] However, most modern legal disputes appear to contain one or more of the following types of electronic evidence: Mobile phone data and/or records;[25] data produced from a software programme;[26] e-mail data and/or e-mail access data;[27] social media and messaging services communication data;[28] data contained on a person's laptop or

[20] The analysis of foreign law in this thesis is deliberately within English speaking countries with a common law heritage – aspects of the law in United Kingdom, Canada, New Zealand and the United States of America will be reviewed herein. The reason for this is to focus on law as similar as possible to South Africa given that the country is in the throes of attempting to introduce legislation relating to electronic evidence when this is arguably not necessary at this time.
[21] See section 1 of the ECT Act.
[22] Article 2 of United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* accessed on 5 April 2016. See also the discussion in Chapter 2 paragraph 2.1 below.
[23] B Schafer & S Mason 'The characteristics of electronic evidence' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 18 – 34.
[24] B Schafer & S Mason 'The characteristics of electronic evidence in digital format' in Mason (ed) *Electronic Evidence* 3 ed (2012) 23 – 69; G Weir & S Mason 'The sources of digital evidence' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 1 – 21. See also the fourth edition of this text: Schafer & Mason op cit note 22 at 18 – 34; G Weir & S Mason 'The sources of electronic evidence' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 1 – 17.
[25] *S v Miller* 2016 (1) SACR 251 (WCC); *S v Panayiotou* [2018] 1 All SA 224 (ECP).
[26] *LA Consortium & Vending CC v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ).
[27] *General Council of the Bar of South Africa v Jiba* 2017 (2) SA 122 (GP); *Mnyandu v Padayachi* 2017 (1) SA 151 (KZP); *S v Meyer* supra note 15.
[28] *RM v RB* 2015 (1) SA 270 (KZP); *Isparta v Richter* 2013 (6) SA 529 (GNP).

personal computer;[29] or data that may be contained on a remote server, a so-called cloud based service – such as *DropBox*, *Amazon Cloud* and *Google Drive*.[30]

Electronic forms of evidence have traditionally been viewed with scepticism. Primarily, because of the perception that evidence in electronic form can be easily manipulated[31] – the key evidentiary concerns relate to authentication and reliability of the evidence.[32]

1.3 ELECTRONIC EVIDENCE IN SOUTH AFRICA

Technology has developed rapidly over the last three decades.[33] Over the last decade in particular, information is regularly transmitted and stored electronically – *and only electronically*. The use of mobile phones, e-mail, social media, and various electronic messaging services are ubiquitous. This current norm will more than likely change and transform as society develops (and with the effluxion of time), but for the short to medium term, electronic forms of evidence will be critical in all types of legal proceedings.

Post the promulgation of the ECT Act, despite some confusion around business records and its interaction with hearsay, as well as some debate as to the precise meaning of s 15 of the ECT Act, more recent case law[34] suggests a maturing approach to electronic evidence. South Africa's judiciary has adapted to the needs of a modern, quickly-developing society with an ageing legislative environment.

The first reported case dealing with electronic evidence in South Africa was *Narlis v South African Bank of Athens* (*Narlis*).[35] Ultimately, bank records in the form of computer

---

[29] *Harvey v Niland* 2016 (2) SA 436 (ECG).
[30] C Theophilopoulos 'Electronic documents, encryption, cloud storage and the privilege against self-incrimination' (2015) 123(3) *SALJ* 596 – 599.
[31] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7 – 13. Although not exhaustive, further challenges include: rapidly evolving technology, fragility of the media, dependency on certain specific hardware and/or software, and fact that data on networked environments is regarded as dynamic. See further Watney op cit note 17 at 1 – 13.
[32] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 20 – 25.
[33] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7. For the basics on computer technology, and the sources of electronic evidence, see Schafer & Mason op cit note 23 at 18 – 34.
[34] *S v Panayiotou* supra note 25; *S v Miller* supra note 25; *S v Brown* 2016 (1) SACR 206 (WCC); *Delsheray Trust* supra note 5; *ABSA Bank Ltd v Le Roux* 2014 1 SA 475 (WCC); *Harvey v Niland* supra note 29; *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA).
[35] 1976 (2) SA 573 (A). See also South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7.

print-outs in *Narlis* could not be admitted to court as evidence. Since then, it appears that electronic evidence in South Africa has been looked at with a sense of caution – however, recent case law[36] suggests this attitude does appear to have changed (or is in the process of changing).

Following *Narlis*, South Africa promulgated overly-technical legislation in the form of the Computer Evidence Act.[37] General consensus was that this legislation failed[38] – it was repealed entirely in August 2002 with the promulgation of the ECT Act.[39] Read together with related legislation,[40] the ECT Act is the primary legislation in South Africa regulating electronic evidence. Although the ECT Act is ageing, it still achieves one of its primary functions in facilitating the admissibility of electronic evidence. However, there is room for improvement in the current legislative environment – particularly in so far as hearsay electronic evidence is concerned. Moreover, there are several other areas of confusion and/or inconsistency that require amendment and further consideration by an expert working-group.[41]

1.4 AN OUTLINE OF KEY RESEARCH QUESTIONS

This research will attempt to answer six primary questions relating to electronic evidence, the answers to which will ideally add to the current discourse. Ultimately, this research will suggest several areas of law reform, but will disagree with the suggested approach put forward by the SALRC. However, this research does support the SALRC's overall position that reform is required, and further supports the suggestion that a working group of information technology and legal experts should be established to review this dynamic environment periodically.

Consequently, the primary aim of this study is to suggest law reform that will develop electronic evidence in South Africa in a manner that is clear, consistent, and where appropriate, compliant with international norms. In order to achieve this, this research is separated into the following questions:

1. What is the current legal position in so far as the admissibility and evidential weight of data messages in South Africa is concerned?

---

[36] See note 34 above.
[37] Act 57 of 1983.
[38] *S v Brown* supra note 34 at para 16. See also Schwikkard & van der Merwe op cit note 2 at 440.
[39] Section 92 of the ECT Act. See further the discussion in chapter 2 para 2.2 below.
[40] Civil Proceedings Evidence Act 25 of 1965; Criminal Procedure Act 51 of 1977; Law of Evidence Amendment Act 45 of 1988. These regulatory instruments will be discussed in chapter 2 para 2.2 below.
[41] See chapter 8 para 8.2 below for a summary of law reform recommendations arising from this research.

1.1 What reform, if any, is required to the definition of data message?

1.2 Does the principle of functional equivalence apply in South Africa?

2. Should electronic evidence constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act? [42]

2.1 In the context of hearsay electronic evidence, to what extent, if any, does the ECT Act 'liberate'[43] data messages from the exclusionary hearsay rule?

2.2 Irrespective of hearsay, how does one consistently determine whether a data message is documentary evidence or real evidence?

3. In the context of data messages, does a presumption of regularity exist in South African law?

3.1 Is the law reform proposed by the SALRC regarding presumptions necessary?

3.2 Is the law reform proposed by the SALRC regarding presumptions desirable?

4. In so far as authentication and weight of electronic evidence are concerned, does section 15 of the ECT Act require amendment? [44]

5. Is it appropriate to apply different evidentiary considerations to electronic evidence in civil and criminal proceedings?

6. Regarding the SALRC's recommendations (the proposed *Law of Evidence Bill*), what are the difficulties with the proposed law reform?

6.1 In the context of law reform, what approach should South Africa adopt?

---

[42] This issue is drawn from the South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2014) Issue 6 at 62 – 67.
[43] D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) at 432.
[44] This issue is drawn from South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2014) Issue 8 at 71 – 74. See also, South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) at 41 – 46.

6.2 What urgent law reform is required in the context of electronic evidence?

1.5 RATIONALE FOR THE STUDY AND RESEARCH METHODOLOGY

The SALRC process of reviewing electronic evidence has spanned several issue and discussion papers from 1982 to date.[45] The current recommendations made by the SALRC are pending before the Department of Justice and Constitutional Development, under the Minister of Justice and Correctional Services.

The current proposals have received feedback from, inter alia, the National Prosecuting Authority (NPA), the Law Society of South Africa (LSSA), the South African Police Service (SAPS), commercial business, academia, private attorney practice, and the Johannesburg Bar Council. In my view, the nature of the review together with the plethora of responses received indicates a national importance – particularly when one considers areas of confusion and inconsistency in electronic evidence.

Moreover, if one has regard to the explosion of internet usage over the past decade,[46] it is reasonable to infer that we are entering a time (or have already entered a time) where the use of electronic communication technologies are critical to a fully functional, modern society.[47] As noted by the KwaZulu-Natal High Court in Durban: *It is not unreasonable to expect the law to recognise* [technological] *changes and accommodate them*.[48]

The research conducted for this thesis is qualitative in the form of descriptive desktop research. There will be an extensive analysis and critical review of the current South African legal position relating to the admissibility and evidentiary weight of electronic evidence. In order to draw definitive conclusions, and offer recommendations on appropriate law reform, it

[45] The SALRC has explored the issue of electronic evidence since its inception in 1982. See, for example, South African Law Commission (Project 6) *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers* (1982) and South African Law Commission Report (Project 6) *Review of the Law Evidence* (1986). See also: South African Law Commission Working Paper 60 (Project 95) *Investigation into the Computer Evidence Act 57 of 1983* (1995); South African Law Commission Issue Paper 14 (Project 108) *Computer-related crime* (1998); South African Law Commission Discussion Paper 99 (Project 108) *Computer-related Crime* (2001); South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010); South African Law Reform Commission Discussion Paper 131 (Project 126) *The Review of the Law of Evidence* (2014).
[46] See note 7 above, Internet World Stats 2018 *http://www.internetworldstats.com/africa.htm#za*, accessed on 31 July 2018.
[47] Hofman & de Jager op cit note 9 at 761.
[48] Steyn J in *CMC Woodworking Machinery* supra note 5 at para 2.

will also be necessary to review South African law reform research, as well as international resolutions, international legislation, and international case law relating to electronic evidence.

1.6 THESIS OUTLINE

This thesis is divided into eight chapters, the first of which is this chapter, *electronic evidence in South Africa – an introduction*, which sets out the work's primary purpose, and relevant research questions. The second chapter explores terminology relating to electronic evidence, and considers whether functional equivalence is applicable in South Africa. The third chapter analyses hearsay electronic evidence, and assesses the application of the hearsay rule in the context of electronic evidence.

The study then proceeds to examine electronic instruments in chapter 4, and considers presumptions, judicial notice and the application thereof in relation to electronic evidence. Next, in chapter 5, the study moves naturally to consider admissibility and weight of electronic evidence holistically.

Chapter 6 considers whether a court should apply different evidentiary considerations to electronic evidence in civil and criminal proceedings, and examines whether all data message evidence should be proved beyond reasonable doubt in a criminal trial. Thereafter, chapter 7 analyses the SALRC's most recent law reform recommendations, and deals with each of the eleven questions posed. Finally, chapter 8 provides a summary of this work's findings and recommendations for law reform.

CHAPTER 2:[1] *TERMINOLOGY, AN OVERVIEW OF THE SOUTH AFRICAN LEGAL POSITION IN RELATION TO DATA MESSAGES, AND FUNCTIONAL EQUIVALENCE*

2.1 INTRODUCTION

Electronic evidence is increasingly relevant in all forms of legal dispute. Accordingly, this chapter starts with an examination of the relevant terminology in the context of electronic evidence. The chapter then proceeds to provide an overview of the regulatory framework governing electronic evidence in South Africa in both civil and criminal proceedings; and concludes with a discussion on functional equivalence (considering whether this principle is applicable in South Africa). The primary objective of this chapter is to set out the basic legal framework applicable to electronic evidence in South Africa.

2.2 DATA MESSAGES

In a South African context, it is prudent to deal with terminology, then to analyse the genesis of the regulatory environment relating to electronic evidence. This will allow a thorough identification of the current areas of confusion and inconsistency, and facilitate clear and consistent law reform suggestions.

Computer or machine related evidence[2] is often referred to as electronic evidence,[3] digital evidence,[4] ESI evidence[5] (electronically stored information), computer evidence,[6] or

[1] A version of this second chapter was published as L Swales 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One' (2018) 21 *PELJ* 2 – 24.
[2] C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 462 – 463 where the admissibility requirements for an electronic document to be presented at a trial are discussed.
[3] J Hofman & J de Jager 'South Africa' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 761 – 796 where the authors review electronic evidence (data messages) in a South African context.
[4] P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) 437.
[5] S Papadopoulos & S Snail (eds) *Cyberlaw@SA III* (2012) 315.
[6] The term used by van Zyl J in *S v Ndiki* 2008 (2) SACR 252 (Ck) para 4. This case is also reported as *S v Ndiki* [2007] 2 All SA 185 (Ck).

ICT[7] evidence – none of these terms exist in South African statutes, rather, the term data message[8] is used.[9] South Africa drew this definition from the UNICTRAL Model Law, 1996.[10]

The first introduction[11] of the term data message[12] to South African law was on 30 August 2002 with the promulgation of the ECT Act.

Interestingly, the promulgation of the proposed Cybercrimes Bill[13] in its current form will lead to the term data message having conflicting definitions – the current definition in the ECT Act reads as follows:

> 'data message' means data generated, sent, received or stored by electronic means and includes-
>
> (a) voice, where the voice is used in an automated transaction; and
>
> (b) a stored record

The Cybercrimes Bill[14] defines the term as:

---

[7] D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 107 – 111.

[8] See the sections containing definitions (section 1) in both the ECT Act and the Cybercrimes Bill B6B – 2017. The term electronic evidence does not exist. The term used is *data message*; see also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 3.2 at 27; D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) at 843 – 847.

[9] Or more broadly, the term *data* is used, and is defined in the ECT Act as 'electronic representation of information of any form'. See also D Zeffertt & A Paizes *Essential Evidence* (2010) 268 – 270; Schwikkard & van der Merwe op cit note 4 at 437 – 438.

[10] United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* accessed on 5 April 2016; South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) ch3; see also United Nations 'Status: UNCITRAL Model Law on Electronic Commerce (1996)' *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html*, accessed on 4 August 2018 where the Secretariat lists member states that comply with the Model Law, 1996. There are 71 States in a total of 150 jurisdictions that have adopted it. South Africa is largely compliant: '…except for the provisions on certification and electronic signatures.'

[11] The ECT Act followed the Computer Evidence Act 57 of 1983, which did not attempt to define electronic evidence – rather, it defined the broad term of *information* as 'any information expressed in or conveyed by letters, figures, characters, symbols, marks, perforations, patterns, pictures, diagrams, sounds or any other visible, audible or perceptible signals.' See also D Zeffertt & A Paizes *The South African Law of Evidence* 3 ed (2017) at 976 – 981.

[12] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 31 – 33; South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) paras 4.23 – 4.40 at 52 – 55.

[13] B6B – 2017.

[14] The first version of the Cybercrimes and Cybersecurity Bill released for public comment (referred to as 'B-2015') used the same definition of data message as was contained in second version of the Bill, B6-2017. The most recent version of the Bill, the B6B – 2017 version was approved by the Justice and Correctional Services committee on 7 November 2018. It will likely be promulgated in 2019. Interestingly, the Bill no longer makes provision for cyber response infrastructure such as a 24/7 point of contact, a Cyber Response Committee, and various government structures supporting cybersecurity. As a result, the proposed law has changed names from the 'Cybercrimes and Cybersecurity Bill' to the 'Cybercrimes Bill'.

> 'data message' means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form

Section 58 of the Cybercrimes Bill[15] does not repeal or amend the definition of data message contained within the ECT Act – this misnomer, although a minor oversight, and of little practical effect, should be corrected as soon as possible.

Moreover, the words '*where any output of the data is in an intelligible form*' are probably not necessary and include a condition to a data message's admissibility that is arguably not necessary, or applicable to traditional evidence.[16] If data is not in intelligible form, it may render the evidence almost meaningless in any event, and it would probably carry very little evidentiary weight if it were to be admissible. However, it may also be the case that the apparently unintelligible data is required to prove some or other relevant issue in dispute – the admission of a data message that is unintelligible may provide context or add a strand of cable to the narrative.[17] One must ask: Is this type of condition to admissibility found with paper or traditional evidence? No. Paper-based evidence need not be intelligible to be admissible. However, if a court is to admit data messages in unintelligible form, the inclusion of theoretically meaningless evidence has the potential to undermine the common law of evidence,[18] and has the potential to increase the time a court will require to dispose of a matter.

Be that as it may, in my view, a concise and simple definition is preferable – with as few limiting features as possible – and adding a further layer or condition to the definition is not necessary or in accordance with international best practice.[19]

The current proposed definition of data message contained in the Cybercrimes Bill (as well as those in the previous Cybercrimes and Cybersecurity Bill) represents a departure from

---

[15] Section 58 (read together with the appropriate Schedule thereto) does not list the definition of data message in ECT Act in the list of repeal or amendment of laws. There are, however, a number of provisions in the ECT Act, for example those relating to cybercrime that will be repealed.

[16] Although no definition for unintelligible data is provided by the SALRC, the ordinary meaning of the word suggests it would refer to data that cannot be read on a screen or used in a software programme. However, unintelligible data (such as a corrupt e-mail message or inaccessible software file) may well, in theory, be useful in proving some other fact at issue. Further, the metadata attached to the data message may also be relevant in proving or disproving some issue in dispute.

[17] A Paizes 'The law of evidence: Seven wishes for the next twenty years' (2014) 3 *SACJ* 281 where reference is made to the Australian cases of *Shepherd v The Queen* (1990) 170 CLR 573 and *Edwards v The Queen* (1993) 178 CLR 193.

[18] The common law of evidence in South Africa can be summarised with reference to *R v Trupedo* 1920 AD 58: all relevant evidence is admissible – the converse will equally apply: namely, all irrelevant evidence is inadmissible; see also South African Law Reform Commission Discussion Paper 113 Project 126 *Review of the Law of Evidence—Hearsay and Relevance* (2008) 14.

[19] See, for example, art 2 of the Model Law, 1996.

what was recommended in the ECT Amendment Bill 2012,[20] where it was suggested that the definition of data message should be amended to:

> 'Data message' means electronic communications including:
>
> (a) voice, where the voice is used in an automated transaction; and
>
> (b) any other form of electronic communications stored as a record

The ECT Amendment Bill, 2012 was withdrawn[21] due to the development and imminent promulgation of comprehensive cybercrime and cybersecurity legislation, namely the Cybercrimes Bill.

Arguably, all three of these South African definitions are overly complicated. By way of example, the United States comparable definition[22] (the concept has a different name – electronic record) is concise – it reads: 'a record created, generated, sent, communicated, received, or stored by electronic means'.

Further, the Model Law, 1996 defines the term as:

> (a) Data message means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy

While the UNICTRAL definition above does appear somewhat dated – verbose even – South Africa has an opportunity to produce a modern, streamlined definition when the Cybercrimes Bill is promulgated as an Act of Parliament. Holistically, any definition should be neutral, concise, and comply with functional equivalence where possible. My suggestion, which is consistent with the most recent SALRC recommendation,[23] is: 'data message' means data generated, sent, received or stored by electronic means.

[20] GN R888 in GG 35821of 26 October 2012.
[21] Advised by the Parliamentary Monitoring Group in August 2015 that the Amendment Bill was withdrawn.
[22] In terms of section 2 of the Uniform Electronic Transactions Act, 1999.
[23] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 52 – 55.

2.3 OVERVIEW OF THE REGULATORY FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN SOUTH AFRICA: CIVIL PROCEEDINGS

The South African law of evidence is not codified in one single statute[24] – the Constitution,[25] a variety of statutes,[26] the common law,[27] and applicable case law must be considered to form a view on whether potential evidence is admissible, and if admissible, the weight it should be accorded.

In general, South Africa takes an exclusionary[28] approach to evidence in civil and criminal proceedings – this position mimics the English common law.[29] Evidence will only be considered admissible if it is relevant to a fact at issue,[30] and even if relevant, the evidence will only be admissible if it is not excluded by a common law or statutory rule precluding the admissibility of a certain type[31] of evidence, or precluding the admissibility of evidence obtained in a certain manner.[32]

Typically, the admission of evidence to civil or criminal court occurs in one of three ways: as oral evidence from a witness,[33] documentary evidence in the form of a document,[34]

---

[24] A Bellengère et al *The Law of Evidence in South Africa* (2013) at 4; P Schwikkard & S van der Merwe *Principles of Evidence* 3 ed (2009) 24 – 31.
[25] Schwikkard & van der Merwe op cit note 4 at 27.
[26] Civil Proceedings Evidence Act 25 of 1965; Criminal Procedure Act 51 of 1977; Law of Evidence Amendment Act 45 of 1988; Electronic Communications and Transactions Act 25 of 2002; and where applicable, The Constitution of the Republic of South Africa, 1996.
[27] Schwikkard & van der Merwe op cit note 4 at 26 – 27.
[28] Schwikkard & van der Merwe op cit note 4 at 438; Papadopoulos & Snail op cit note 5 at 317; van der Merwe et al op cit note 7 at 107; Hofman & de Jager op cit note 3 at 761; M Watney 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 *Journal of Information, Law and Technology* 3.
[29] *S v Ndiki* supra note 6 para 21 where the common law position with regard to evidence is stated as follows: 'evidence tending to prove or disprove an allegation which is in issue is admissible unless a specific ground for exclusion operates'. See also *R v Trupedo* 1920 AD 58 at 62; Hofman & de Jager op cit note 3 at 761; Papadopoulos & Snail op cit note 5 at 316.
[30] *R v Trupedo* supra note 29 at 62; *Ndiki* supra note 6 para 21.
[31] For example, hearsay evidence, as a default position, is not admissible unless an exception applies. For more on hearsay evidence in general, see: Schwikkard & van der Merwe op cit note 4 at 287-304; Zeffertt & Paizes op cit note 8 at 385 – 441; Bellengère et al op cit note 24 at 234 – 245; Zeffertt & Paizes *The South African Law of Evidence* 3 ed (2017) at 399 – 470.
[32] Evidence obtained in an unconstitutional manner is generally inadmissible, but subject to the overriding factor of the administration of justice balanced against the right of an accused to have a fair trial – consequently, even evidence obtained in an unconstitutional manner may (in certain instances) be admissible. For example, see *Harvey v Niland* 2016 (2) SA 436 (ECG) where evidence that was unlawfully obtained by hacking into a person's private social media account (and in violation of the right to privacy) was found to be admissible. For more on unconstitutionally obtained evidence see Schwikkard & van der Merwe op cit note 4 at 198 – 283; Zeffertt & Paizes op cit note 8 at 721 – 736; Bellengère et al op cit note 24 at 292 – 305.
[33] Schwikkard & van der Merwe op cit note 4 at 388 – 420.
[34] Schwikkard & van der Merwe op cit note 4 at 431-436; Zeffertt & Paizes op cit note 8 at 827 – 843; Watney op cit note 28 at 5 – 11.

or real evidence in the form of a tangible thing.[35] There is no *sui generis* category[36] for electronic evidence and many courts have reached differing conclusions[37] on how best to classify and treat electronic evidence.

The classification must depend on the type of electronic evidence, and its nature[38] – once this is established, the admissibility requirements for that type of evidence must be assessed (in light of any concessions provided for in related legislation such as the ECT Act). As noted by Bozalek J in *S v Brown*:[39]

> … the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document.

Electronic evidence has been treated with caution[40] and conservatively[41] – a prominent South African resource on evidence even remarked, in 1997, that in leaving paper, there will be no 'guarantees of authenticity and reliability.'[42] Skepticism of the medium notwithstanding, the default position is that subject to express guidance in applicable legislation such as the ECT

---

[35] Zeffertt & Paizes op cit note 8 at 849 – 862; Schwikkard & van der Merwe op cit note 4 at 421 – 430.

[36] Watney op cit note 28 at 11 where the author does not support the creation of a sui generis category for electronic evidence; see also P Fourie *Using Social Media as Evidence in South African Courts* (LLM thesis, North-West University, 2016) 12; G van Tonder *The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective* (LLM thesis, University of the Western Cape, 2013) 59.

[37] *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ) para 12 where a full bench of the South Gauteng High Court in Johannesburg stated: 'The data messages relied upon in this case are not only real evidence but include hearsay'; *Ndiki* supra note 6 para 20 & para 33 where the court concluded that a data message can be either real or documentary evidence, depending on its purpose and nature; but then commented further, obiter, that to avoid a difficult distinction between what would constitute hearsay evidence and what real evidence, computer generated evidence should always be treated as hearsay. This obiter statement is not supported and should be avoided to ensure South Africa remains consistent with its common law, and with international best practice – see a sample of the international legal position discussed below in chapter 3 at para 3.6. See also *S v Brown* 2016 (1) SACR 206 (WCC) para 20 where the court noted: 'Given the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device, I consider that they are more appropriately dealt with as documentary evidence rather than "real evidence". I associate myself, furthermore, with the approach followed in [*Ndiki* supra note 6 para 20] where Van Zyl J expressed the view that the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one is dealing with and what the requirements for its admissibility are.'

[38] *Ndiki* supra note 6 para 20; *Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W) 18; *Brown* supra note 37 para 20; *S v Meyer* 2017 JDR 1728 (GJ) para 299 – 304. See also van der Merwe et al op cit note 7 at 124 – 130; Schwikkard & van der Merwe op cit note 4 at 445 – 446.

[39] *Brown* supra note 37 para 18.

[40] *S v BM* 2014 (2) SACR 23 (SCA) para 33 where the court noted: 'Whilst the best evidence rule seems everywhere to be in retreat, that does not mean that a court must accept as accurate secondary evidence of a document or other form of writing, such as a text message. The fact, that it has been thought necessary to make elaborate provision in a statute for the admissibility in evidence of such messages, demonstrates the need for caution in this regard.' Hofman & de Jager op cit note 3 para 18.04 at 762; Schwikkard & van der Merwe op cit note 4 at 438.

[41] Schwikkard & van der Merwe op cit note 4 at 438.

[42] Hofman & de Jager op cit note 3 para 18.04 at 762; J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 267 – 268.

Act, the normal South African legal position in relation to the admissibility of evidence also applies to data messages.[43]

2.3.1 The Civil Proceedings Evidence Act

The first computer arrived in South Africa in the 1950's,[44] and one can trace the statutory evolution of electronic evidence in South Africa to the civil decision of *Narlis v South African Bank of Athens (Narlis).*[45]

Prior to *Narlis*, the primary legislative instrument regulating electronic evidence was the Civil Proceedings Evidence Act 25 of 1965 (CPEA). On 30 June 1967 the CPEA was promulgated with the goal of codifying evidentiary issues pertaining to civil matters – it did not provide expressly for electronic evidence, and an amended version of the legislation is still in effect. In its current form in 2018 it still does not expressly provide for electronic evidence – it does, however, provide for the admission[46] of evidence relating to civil matters, particularly documentary evidence (whether the evidence is electronic or otherwise).

In *Narlis*, the key issue was the existence of a principal debt[47] owed by a surety and co-principal debtor to the South African Bank of Athens. The decisive evidence took the form of computerised bank statements, submitted to court by a bank manager. The lower court had ruled that the computerised evidence was admissible and decided in favour of the bank. However, the Appellate Division, as it was then called, found that s 34 of the CPEA provided no basis for any discretionary admissibility of computerised statements.[48] As a result, because a 'person' had not made the 'statement', the evidence was inadmissible, and the appellant successful. The court famously noted:[49] 'a computer, perhaps fortunately, is not a person'[50] and

[43] van der Merwe at al op cit note 7 at 130; Hofman & de Jager op cit note 3 para 18.12 at 766.
[44] Y Lulat *United States Relations with South Africa: A Critical Overview from the Colonial Period to the Present* (2008) 73 where date is stated as 1952; Hofman & de Jager op cit note 3 at 761 where the date is stated 1959 and Mybroadband 2015 *https://mybroadband.co.za/news/hardware/132408-south-africas-first-computers.html*, accessed on 25 July 2018 where the date is also stated as 1959. The actual date is of little consequence to this research, but it appears it was at least in the 1950's.
[45] *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A); van der Merwe at al op cit note 7 at 111; Watney op cit note 28 at 3 – 6.
[46] *Trend Finance (Pty) Ltd v Commissioner for the South African Revenue Service* [2005] 4 All SA 657 (C) para 36 – 42.
[47] *Narlis* supra note 45 at 154.
[48] *Narlis* supra note 45 at 157.
[49] *Narlis* supra note 45 at 156.
[50] This dictum was repeated in *Ex parte Rosch* [1998] 1 All SA 319 (W) at 328 where the court again noted that: 'The computer is not a person.'

further remarked that the matter (electronic evidence) might well engage the attention of the legislature in South Africa.[51] And engage the legislature it did.

In so far as the CPEA is concerned, although dated, the primary sections still applicable to electronic evidence are contained in Part I, particularly section 2 thereof, and Part VI, s 33 – 35.[52] Section 2 of the CPEA restates the common law regarding evidence, but its wording is negative, rather than positive.[53] Section 33 defines a document[54] as 'any book, map, plan, drawing or photograph'. This section and the entire Part VI also applies to criminal proceedings, as per s 222 of the Criminal Procedure Act 51 of 1977 (CPA).[55] Confusingly, s 221[56] of the CPA defines a document as 'any device by means of which information is recorded or stored'. On the face of it, the definition of document in the CPEA is not wide enough as it currently stands to include a data message. Moreover, and strangely, it appears that the definition of document in the CPEA for civil proceedings is more restrictive (and narrow) than the definition contained in the CPA for criminal proceedings – this is not a sensible position.

For the sake of completeness, there should be an amendment to the term 'document' in both the CPEA and the CPA. Although, in practice, given the emergence of the ECT Act, and wide interpretation[57] on the meaning and extent of the word 'document' this amendment would have very little practical effect – barring, of course, that it would ensure the CPEA and CPA are conceptually sound and up-to-date.

2.3.2 The Computer Evidence Act

Following the decision in *Narlis*, the Clearing Bankers Association approached the South African Law Commission (as it was then called)[58] to investigate the need for legislative reform.

---

[51] Supra note 45 at 157.
[52] Zeffertt & Paizes op cit 8 at 721-736; Schwikkard & van der Merwe op cit note 4 at 439-440.
[53] Section 2 is entitled 'evidence as to irrelevant matters' and reads: 'No evidence as to any fact, matter or thing which is irrelevant or immaterial and cannot conduce to prove or disprove any point or fact in issue shall be admissible'. South Africa's common law of evidence revolves around relevance – see *Ndiki* supra note 6 at para 21 where court sets out South Africa's common law in one of the early (and seminal) electronic evidence cases.
[54] Watney op cit note 28 at 5.
[55] *Shaik v S* [2007] 2 All SA 9 (SCA) para 180.
[56] This section deals with the admissibility of business records and will be discussed in detail in chapter 3 below in the context of hearsay electronic evidence.
[57] *Makate v Vodacom* (Pty) Ltd 2014 (1) SA 191 (GSJ) where the South Gauteng High Court in Johannesburg found that a data message is a document for purposes of Rule 35 of the Uniform Rules of Court.
[58] The South African Law Commission changed its name to the South African Law *Reform* Commission in 2002. see South African Law Reform Commission 2013 *http://salawreform.justice.gov.za/anr/2012-2013-anr-salrc.pdf* at 7, accessed on 5 April 2017.

The Commission was of the view that legislative reform was required and suggested the promulgation of a separate statute.[59]

As a result, the Computer Evidence Act 57 of 1983[60] commenced operation on 1 October 1983 and was South Africa's first attempt at legislating rules and norms for computer and/or electronic based evidence.

The Computer Evidence Act only applied to civil proceedings.[61] While it was in effect, it was roundly criticised by a variety of academics,[62] and even courts,[63] for being overly technical.[64] The understandably cautious approach was based on the general belief that alterations (or manipulation) of electronic data is far harder to detect than an alteration made to a paper-based document.[65]

The promulgation of the Computer Evidence Act notwithstanding, the SALRC continued investigating evidence, and in particular electronic evidence through the 1980's[66] and into the 2000's.[67] As was predicted in *Narlis*, computer evidence did indeed engage the attention of lawmakers in South Africa.

---

[59] South African Law Commission (Project 6) *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computer, Review of the Law of Evidence* (1982).

[60] For a perspective on the now repealed Computer Evidence Act, see S Mapoma *A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM thesis, University of South Africa, 1997) 3 – 32.

[61] Bellengère et al op cit note 24 at 74; Zeffertt & Paizes op cit note 8 at 843; South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 19 – 20.

[62] Schwikkard & van der Merwe op cit note 4 at 440; van der Merwe et al op cit note 7 at 112, South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 19; Hofman & de Jager op cit note 3 at 763.

[63] *Ndlovu* supra note 38 at 171 where the court noted that the Computer Evidence Act had two major shortcomings: first, that is was 'cumbersome' to comply with its provisions, and secondly, that it only applied to civil proceedings. See also *Brown* supra note 37 para 16 where it was stated that the Computer Evidence Act 'was generally considered to have failed to achieve its purpose'.

[64] Hofman & de Jager op cit note 3 at 762 – 763.

[65] Theophilopoulos op cit note 2 at 467 – 468.

[66] South African Law Commission (Project 6) *Review of the Law of Evidence* (1986).

[67] South African Law Commission Discussion Paper 99 (Project 108) *Computer related crime* (2001); South African Law Commission (Project 126) *Report on the Preliminary Investigation into the Review of the Rules of Evidence* (2002); South African Law Reform Commission (Project 113) *The Use Of Electronic Equipment In Court Proceedings Postponement Of Criminal Cases Via Audiovisual Link* (2003); South African Law Reform Commission Discussion Paper 113 (Project 126) *Review of the Law of Evidence Hearsay and Relevance* (2008).

A limited number of reported decisions dealt with the Computer Evidence Act,[68] but in *Ex Parte Rosch*, the court tried to bypass the cumbersome[69] nature of the admissibility provisions by interpreting the statute to be a facilitating Act not a restricting one.[70]

This type of interpretation, although twenty years old, is consistent with what may be described as the ideal philosophy in electronic evidence – a facilitating approach, attempting functional equivalence,[71] while ensuring that one type of evidence is not preferred over the other.

2.3.3 The Electronic Communications and Transactions Act[72]

The ECT Act repealed[73] the Computer Evidence Act entirely when it came into effect on 30 August 2002 following global trends,[74] judicial calls,[75] and law reform recommendations.[76]

The ECT Act is the primary legislative instrument regulating electronic evidence and, although not expressly stated, applies to both civil and criminal proceedings[77] – addressing one of the primary flaws of the now defunct Computer Evidence Act. It seeks to comprehensively regulate all aspects of electronic commerce, and but for two areas,[78] follows the UNCITRAL Model Law, 1996. [79]

---

[68] See *Ex parte Rosch* [1998] 1 All SA 319 (W); *Ndiki* supra note 6 para 2; *Ndlovu* supra note 38 at 171.
[69] Supra note 68 at 327 – 328; see also South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 20.
[70] *Ex parte Rosch* supra note 68 at 327.
[71] See the discussion on functional equivalence at para 2.4 below.
[72] Section 15 of the ECT Act, and admissibility of data message evidence in general is discussed in detail in chapter 5 below.
[73] Section 92 of the ECT Act.
[74] Based on the Model Law, 1996.
[75] *S v Mashiyi* 2002 (2) SACR 387 (Tk) 393 where Miller J noted: 'all that I can do is add my voice to the call that this lacuna in our law be filled and for new legislation relating specifically to computer evidence in criminal cases.'
[76] See note 66 and 67 above.
[77] Section 4 of the ECT Act states that it applies in respect of any electronic transaction or data message. See also the general discussion on the ECT Act in South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 16 – 17, and 29 – 49 where the SALRC also conclude that the ECT Act applies to both civil and criminal proceedings; see further Theophilopoulos op cit note 2 at 461.
[78] According to the Secretariat of the United Nations, electronic signatures and certification are two areas that the ECT Act does not follow the Model Law, 1996. See United Nations 'Status: UNCITRAL Model Law on Electronic Commerce (1996)' *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html*, accessed on 5 April 2018.
[79] *Jafta v Ezemvelo KZN Wildlife* (2009) 30 ILJ 131 (LC) para 62 – 99 where the Model Law, 1996 is discussed in detail with one of the delineations being: the ECT Act is primarily based thereon.

One of the primary purposes of the legislation (and the Model Law, 1996), is to facilitate functional equivalence[80] by, inter alia, providing an electronic equivalent[81] for paper-based documents while recognising the inherent distinctions between written and electronic evidence. Moreover, in terms of section 2(e) of the ECT Act, one of the specific reasons for the promulgation of the Act is to promote legal certainty.[82]

The ECT Act[83] is the only South African legislation that specifically regulates electronic evidence[84] and can be described as facilitating[85] e-commerce, and more specifically in this context, facilitating the admission and evidentiary weight of electronic evidence. Section 3 (interpretation) expressly makes this intention clear: it must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions.

The Supreme Court of Appeal[86] has had limited opportunity to deal with the ECT Act,[87] but has noted:

> One of the [ECT] Act's aims 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. [88]

Further, in *Firstrand Bank Limited v Venter*,[89] the Supreme Court of Appeal confirmed that section 15 of the ECT Act:

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

---

[80] See para 2.4 below for a detailed discussion on functional equivalence.
[81] Papadopoulos & Snail op cit note 5 at 318.
[82] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 29 – 30.
[83] For further background on the ECT Act see South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) ch 6.
[84] Papadopoulos & Snail op cit note 5 at 317; Schwikkard & van der Merwe op cit note 4 at 441-446.
[85] As envisioned by the court in *Ex Parte Rosch* supra note 68, in the technological environment, legislation ought to be facilitating – notwithstanding our common law heritage; see also Papadopoulos & Snail op cit note 5 at 318.
[86] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA) where the court dealt with electronic signatures.
[87] See also *Sublime Technologies (Pty) Ltd v Jonker* 2010 (2) SA 522 (SCA) at para 13 – 14 where the primary issue dealt with an undertaking to pay costs as a result of a Practice Directive in the North Gauteng High Court, but where the definition of data message was mentioned. In my view, the decision of the court a quo in this matter is clearly incorrect, namely that 'evidence of bank records will be inadmissible unless the prescribed notice has been given' (notice in terms of the CPEA). Section 15(4) of the ECT facilitates the admission of this type of evidence without the need for notice if the section is complied with. The underlying decision of the court a quo does not appear to be reported and is not material to this contribution.
[88] *Spring Forest Trading* supra note 85 para 16.
[89] [2012] JOL 29436 (SCA).

3. lays down the minimum requirements for admissibility.

In addition, in *S v Brown*,[90] the Western Cape High Court noted:

> Clearly, the overall scheme of the [ECT Act] is to facilitate the admissibility of data messaging as electronic evidence.

The primary provisions of the ECT Act relevant to electronic evidence are found in Part 1 of Chapter III (facilitating electronic transactions), particularly sections 11 (legal recognition of data messages), 12 (writing), 14 (original) and 15 (admissibility and evidential weight of data messages), together with Part II which deals with the communication of data messages.[91]

Principally, the ECT Act provides that data messages are legally binding and will have full legal force and effect – moreover, that a data message will be considered *in writing*, can be considered an *original*, and in certain instances a data message will qualify as an ordinary *signature*. In summary, the ECT Act attempts to provide a regulatory framework that facilitates data messages (electronic communications) being treated the same, in law, as traditional forms of communication.

For example, in *Jafta v Ezemvelo KZN Wildlife*[92] the Labour Court found that the ECT Act is consistent with global law.[93] Further, that given s 11, which provides that a data message will have legal force and effect, even though SMS and e-mail often contain colloquial or relaxed language: 'treating them [data messages] as having no legal effect would be a mistake.'[94]

Sihlali v South African Broadcasting Corporation Ltd[95] is instructive as it confirmed the fact that a data message (whether informal, SMS, e-mail, or howsoever transmitted) will carry all legal implications that would otherwise be the case with traditional and more formal communication.[96] Further, in *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a*

---

[90] Supra note 37 para 19.
[91] See van der Merwe et al op cit note 7 at 112-130 for an overview of the ECT Act in the context of evidentiary issues. See also Papadopoulos & Snail op cit note 5 at 317-330; Schwikkard & van der Merwe op cit note 4 at 441 – 446; Theophilopoulos op cit note 2 at 464 – 465.
[92] [2008] ZALC 84.
[93] *Jafta v Ezemvelo KZN Wildlife* supra note 92 para 62 – 99.
[94] *Jafta v Ezemvelo KZN Wildlife* supra note 92 para 78. Although, see the recent reported arbitration of *Gaxa and Kaiser Chiefs Football Club* (2017) 38 ILJ 1221 (ARB), where a statement on social media platform Twitter by Kaizer Chiefs Football Club indicating that it had renewed the contract of Gaxa was not binding in the circumstances. However, Gaxa's decision was primarily based on contractual principles (reasonable reliance) and is not material to this research.
[95] (2010) 31 ILJ 1477 (LC).
[96] In this matter, a legal advisor for the South African Broadcasting Corporation (SABC) sent an SMS message to the CEO indicating that he 'quit with immediate effect' – the primary issue was whether an SMS sent by the

Ecowash,[97] the Supreme Court of Appeal found that e-mail communication will be regarded as reduced to writing and signed by the parties – if 'the data in an email is intended by the user to serve as a signature and is logically connected with other data in the email.'[98] Invariably, in my view, when a user types her name at the end of an e-mail, that action will be with the intention to serve as a signature and there will be data logically connected therewith – consequently, as a default position, in almost all cases, a person's name at the end of an e-mail will qualify as an electronic signature in terms of section 13 read with section 1 of the ECT Act.[99]

In so far as electronic evidence is concerned, the critical provision in the ECT Act is s 15 which prohibits the exclusion of evidence on the mere grounds that it is generated by a computer and not by a natural person;[100] and prohibits the exclusion of evidence on the grounds that it is not original – if the evidence is the best evidence reasonably available.[101]

Section 15 seeks to facilitate[102] the admissibility of data messages, and follows an inclusionary rather than an exclusionary approach.[103] That said, s 15 does not seek to override the normal principles applicable to hearsay[104] – data messages must be treated the same as any other evidence and the admissibility thereof must follow the ordinary rules applicable[105] to the South African law of evidence (except where concessions are made in the ECT Act: for example, with the concept of original, and with the 'business-records' exception).

2.3.4 The Law of Evidence Amendment Act

The Law of Evidence Amendment Act 45 of 1988 was assented to on 15 April 1988 and became effective on 3 October 1988 – it is still in force in 2018, and applies to both civil and criminal proceedings. It is exceptionally short and deals with only two matters of evidence:

---

applicant (Sihlali) to the SABC constituted a valid resignation. It was held that a communication by SMS, in terms of the ECT Act, is a communication in writing, and the SMS was binding.

[97] Supra note 86.

[98] *Spring Forest Trading* supra note 86 para 17 – 19 and paras 27 – 29.

[99] An electronic signature should not be confused with an advanced electronic signature. For more on the distinction between the two, see S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17 *PELJ* 2805 – 2820; L Swales 'The regulation of electronic signatures: Time for review and amendment' (2015) 132 *SALJ* 257 – 270; Y Mupangavanhu 'Electronic signatures and nonvariation clauses in the modern digital world: The case of South Africa' (2016) 133 *SALJ* 853 – 873.

[100] Section 15(1)(a); *Ndlovu* supra note 38 at 172; *Meyer* supra note 38 at para 299 – 301.

[101] Section 15(1)(b); *Ndlovu* supra note 38 at 172; *Meyer* supra note 38 at para 297; *Brown* supra note 37 para 17.

[102] *Ndlovu* supra note 38 at 173; *LA Consortium* supra note 37 at para 17.

[103] *Brown* supra note 37 para 17.

[104] *LA Consortium* supra note 37 para 13; *Ndlovu* supra note 38 at 18-19, *Ndiki* supra note 6 at 31; *Meyer* supra note 38 para 298 – 301. See also Schwikkard & van der Merwe op cit note 4 at 445 – 446.

[105] Hofman & de Jager op cit note 3 at 766 – 767.

Judicial notice and hearsay.[106] In so far as hearsay is concerned, the Act regulates the admissibility of any hearsay evidence and provides judicial officers with a general discretion to admit hearsay as admissible if it proves to be in the interests of justice.[107]

The Act does not expressly refer to electronic evidence and its application has been the subject of judicial, policy and academic debate[108] – although it now appears settled, even though not expressly stated, the Law of Evidence Amendment Act *does* apply to data messages.[109]

In *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd*[110] (*LA Consortium*) it was held that: '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.'[111]

Earlier, in *Ndlovu v Minister of Correctional Services (Ndlovu),*[112] it was held that s 3 of the Law of Evidence Amendment Act provides a court with a broad discretion to admit hearsay evidence if it is of the opinion that the hearsay evidence should be admitted in the interests of justice after having regard to certain factors.[113] Ultimately, a trained and experienced judicial officer is left with large swathes of discretion when deciding whether to admit hearsay evidence.

As noted by the court in *Ndlovu*, s 3 of the Law of Evidence Amendment[114] provides a court with a wide discretion to admit hearsay evidence. A court must assess the relevance of the evidence – which means they must use a blend of 'reason and common sense' in deciding whether the evidence should be admissible.[115] This test is flexible, and much will depend on the facts of the case, and the nature of proceedings; it should be noted that courts are more reluctant to accept hearsay in criminal matters.[116]

---

[106] Van der Merwe et al op cit note 7 at 113 – 114.
[107] Section 3 (1)(c) of the Law of Evidence Amendment Act.
[108] Hofman & de Jager op cit note 3 at 770 – 771.
[109] *LA Consortium* supra note 37 para 13-14; *Ndiki* supra note 6 para 7; *Ndlovu* supra note 38 at 165 – 166.
[110] *Brown* supra note 37.
[111] *Brown* supra note 37 para 13.
[112] *Ndlovu* supra note 38 at 165 – 166.
[113] The factors a court must have regard to are: (i) the nature of the proceedings; (ii) the nature of the evidence; (iii) the purpose for which the evidence is tendered; (iv) the probative value of the evidence; (v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends; (vi) any prejudice to a party which the admission of such evidence might entail; and (vii) any other factor.
[114] See chapter 3 below where this section of the Law of Evidence Amendment Act is reproduced in full in paragraph 3.3, and hearsay electronic evidence discussed in detail.
[115] Zeffertt & Paizes op cit note 8 at 247.
[116] Ibid at 417.

Specifically, s 3 (1) (c) (vii) provides that a court must consider whether 'such evidence should be admitted in the interests of justice.' This is a value judgment that will be made on a case-by-case basis assessing the overall relevance of the evidence. A court will ultimately be considering whether the evidence is relevant to an issue at trial, and whether the benefit of accepting the evidence will outweigh its potentially prejudicial effect.

In my view, this position is satisfactory – South Africa no longer has to guard against jury members being influenced or poisoned by hearsay evidence, and a judicial officer (who is trained and experienced) is best placed to make a case-by-case determination on whether the hearsay evidence should be admissible in the interests of justice.

Even if all electronic evidence were to be categorised as hearsay[117] (which view is not supported), then conceivably, it could still be admissible under the exceptions contained in this section. Ultimately, a judicial officer will always have the discretion to admit hearsay electronic evidence if he or she feels it to be in the interests of justice – and rightly so in my view.

However, the discretion to admit hearsay electronic evidence notwithstanding, it is conceptually incorrect to insist that all electronic evidence is hearsay – this is akin to saying all documents produced by a type-writer are hearsay, and does not properly consider South Africa's common law relating to real evidence.[118] The technology is merely a tool to deliver the information; if the information contains hearsay, it must be subject to the hearsay rules. However, if the information produced electronically does not contain hearsay, its admissibility should be determined by reference to how one would typically determine admissibility – for example, in the case of information created electronically, but reduced to paper for production in court, one would need to determine whether the contents of the document were relevant (and otherwise admissible), to confirm authenticity of the document, and to produce it.[119]

---

[117] *Ndiki* op cit note 6 para 33 where the court quotes Bilchitz's contribution to the *Annual Survey of South Africa Law* in 1998 and comments, obiter, that all computer based evidence should be treated as hearsay. The court was of the view that such a classification would do away with a necessity to distinguish whether the evidence is real or documentary in nature. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 63 – 64. See also Zeffertt & Paizes op cit note 8 at *The South African Law of Evidence* 3 ed (2017) at 455 – 460.

[118] See paragraph 3.3 – 3.5 below for a more detailed discussion of these issues.

[119] *S v Meyer* 2017 JDR 1728 (GJ) para 299.

2.4 OVERVIEW OF THE REGULATORY FRAMEWORK GOVERNING ELECTRONIC EVIDENCE IN SOUTH AFRICA: CRIMINAL PROCEEDINGS

The major distinguishing factor between criminal and civil matters relates to the onus of proof[120] – that aside, the regulatory framework and applicable common law governing electronic evidence is similar.

In addition to the common law and Constitution, the Law of Evidence Amendment Act and the ECT Act apply to both civil and criminal matters – the primary distinction from a legislative perspective is that in criminal matters the CPA will find application, as opposed to the CPEA in civil matters. However, holistically, the legislation and considerations are similar regardless of whether the matter is civil or criminal in nature.

2.4.1 The Criminal Procedure Act

Chapter 24 (s 208 – 253) of the CPA deals with evidence. Section 210, titled *irrelevant evidence inadmissible*, confirms South Africa's common law position: the basic rationale being that only relevant evidence will be admissible.

The principal sections in the CPA relevant to electronic evidence are s 221, 222 and 236, read together with s 246 and 247.[121] Primarily, these sections create an exception to the hearsay rule in the form of business records (that have been duly authenticated), as well as making the CPEA applicable to criminal proceedings (in so far as documentary evidence is concerned).[122]

In so far as electronic evidence is concerned, section 221(5) of the CPA defines a document as 'any device by means of which information is recorded or stored'. This was one of the central issues in *S v Harper*,[123] where the court found that a computer could not be a document for purposes of the CPA, but that a print-out by a computer could be a document –

[120] Although trite, it is worth repetition: in criminal matters, the State must prove guilt *beyond reasonable doubt*. In civil matters, a litigant must prove their case on a *balance of probabilities*. See further the discussion in chapter 6 below which poses the following question: Are there different evidentiary considerations applicable to data message evidence in civil and criminal proceedings?
[121] Watney op cit note 28 at 2 – 7. *S v De Villiers* 1993 (1) SACR 574 (Nm) 367 – 368; *S v Harper* 1981 (1) SA 88 (D) para 46 – 52.
[122] For a full discussion on the impact of the CPA on the law of evidence, and traditional forms of hearsay, see the ordinary academic sources dealing with hearsay evidence: Schwikkard & van der Merwe op cit note 4 at 440 – 441; Bellengère et al op cit note 24 at 301 – 305; Zeffertt & Paizes op cit note 8 at 399 – 470.
[123] *Harper* Supra note 121 para 46 – 52.

and that the word document should be interpreted 'in its ordinary grammatical sense'.[124] Consequently, there are different definitions for the word document in civil and criminal proceedings, and it is an area that concerns the SALRC, and one that should be rectified with statutory amendments.[125]

2.4.2 Cybercrimes Bill (Previously known as the Cybercrimes and Cybersecurity Bill)

According to a discussion document[126] released by the Department of Justice in January 2017:

> The laws dealing with electronic evidence are, in general, sufficient for the purposes of criminal proceedings. However, certain improvements can be made to cater for new technologies.

This perception that the current position in so far as electronic evidence is adequate is further borne out by the marked difference in the evidentiary provisions of the first two versions of the Bill released for public comment. In the first iteration, the B-2015 version, then called the *Cybercrimes and Cybersecurity Bill*, Chapter 8 evidence[127] contained three comprehensive sections dealing with evidence: s 61 (admissibility of affidavits); s 62 (admissibility of evidence obtained as result of direction requesting foreign assistance and co-operation); and s 63 (admissibility of evidence).

Conversely, the next version of the Bill, called the *Cybercrimes and Cybersecurity Bill* B6-2017 contained only one section under the heading, Chapter 8 evidence – s 51 (proof of certain facts by affidavit). This is the current position in s 53 of the most recent draft of the Cybercrimes Bill B6B – 2017 – that is, only one section under the heading *evidence* (the Bill changed names from the *Cybercrimes and Cybersecurity Bill* to the *Cybercrimes Bill* in the third version). The B6B – 2017 version of Bill was approved by Parliament's Justice and Correctional Services committee on 7 November 2018, and further approved by the National

---

[124] Ibid.
[125] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 83.
[126] Department of Justice and Constitutional Development 'Memorandum on the objects of the Cybercrimes and Cybersecurity Bill 2017' available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.pdf*, accessed on 12 April 2018.
[127] The erstwhile provisions were predominantly applicable to criminal proceedings. See the B-2015 version of the Bill, particularly Chapter 8. Department of Justice and Constitutional Development 2015 *http://www.justice.gov.za/legislation/invitations/CyberCrimesBill2015.pdf*, accessed on 25 July 2017.

Assembly on 27 November 2018:[128] It appears likely the bill will be promulgated in its current form.

The section's current wording means it will only be applicable if civil or criminal proceedings are instituted in terms Chapter 5 or 6 of the Prevention of Organised Crime Act 121 of 1998 ('POCA'). The explanatory memorandum[129] released by the Department of Justice and Constitutional Development states as follows: '[This clause] aims to regulate the proof of certain facts by affidavit... if relevant to criminal proceedings.' However, the section itself contains a limiting feature, and reads as follows:

> *Proof of certain facts by affidavit*
>
> 53. (1) Whenever any fact established by any examination or process requiring any skill in—
>
> (a) the interpretation of data;
>
> (b) the design or functioning of data, a computer program, a computer data storage medium or a computer system;
>
> (c) computer science;
>
> (d) electronic communications networks and technology;
>
> (e) software engineering; or
>
> (f) computer programming,
>
> is or may become relevant to an issue at criminal proceedings or civil proceedings as contemplated in Chapter 5 or 6 of the Prevention of Organised Crime Act, 1998, a document purporting to be an affidavit made by a person who, in that affidavit, states that he or she—
>
> (i) is in the service of a body in the Republic or a foreign State designated by the Cabinet member responsible for the administration of justice by notice in the Gazette;
>
> (ii) possesses relevant qualifications, expertise and experience which make him or

[128] Parliament of the Republic of South Africa 'Several Bills get the nod from parliament this afternoon' *https://www.parliament.gov.za/press-releases/several-bills-get-nod-parliament-afternoon*, accessed on 29 November 2018.

[129] Department of Justice and Constitutional Development 'Memorandum on the objects of the Cybercrimes and Cybersecurity Bill 2017' available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.pdf*, accessed on 12 August 2018.

her competent to make the affidavit; and

(iii) has established such fact by means of an examination or process,

is, upon its mere production at such proceedings, prima facie proof of such fact.

As it stands, the section will only be applicable if criminal action is instituted in terms of Chapter 5 of POCA to recover the proceeds of unlawful activities, and where civil action is instituted in terms of Chapter 6 of POCA for the civil recovery of property.

The only inference one can draw is that the legislature appears satisfied[130] that the current position regarding electronic evidence in civil and criminal trials is adequately regulated by the ECT Act, the common law and where applicable either the CPA or the CPEA. In my view, and the view the SALRC,[131] electronic evidence is not adequately regulated in so far as hearsay electronic evidence is concerned – the legal position, which involves multiple sources of law, can be applied inconsistently, and creates confusion.

2.5 FUNCTIONAL EQUIVALENCE

In order to contextualise the surrounding e-commerce environment, it is important to be cognisant of the fact that in any debate or discussion involving electronic evidence, or electronic commerce in general, South Africa should be striving to reach a position that conforms to one of the fundamental guiding principles relating to laws dealing with technology and electronic commerce – functional equivalence.[132]

The United Nations[133] state that a functional equivalent approach is:

[130] By way of private discussion with two of the participants on the committee responsible for this legislation, I am informed that in the committee's view, the evidentiary issues are adequately regulated by existing legislation, and there is no need to codify established principles. I agree with this position, subject to minor amendment being necessary in certain areas as discussed below in chapter 7 and summarised in chapter 8.

[131] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 83 – 86 and ch5 in general for a summary of the SALRC's recommendations for reform.

[132] T Pistorius ' "Nobody Knows you're a Dog": The Attribution of Data Messages' (2002) 14 *SA Merc LJ* 737–738; see also United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* para 15-18, accessed on 25 July 2017. See further, M Kulehile *An analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and the SADC region* (PhD thesis, University of Cape Town, 2017) ch3.

[133] United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* para 16, accessed on 25 July 2017.

> based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.

At its core, a functional equivalent approach seeks to provide or facilitate an electronic equivalent for written, signed and original documents.[134] Put differently, and according to a senior legal officer within the UNCITRAL organisation, functional equivalence is:

> the basic underlying principle of the Model Law. It involves an examination of the function fulfilled by traditional form requirements ('writing', 'signature', 'original', 'dispatch', and 'receipt') and a determination as to how the same function could be transposed, reproduced, or imitated in a dematerialized environment. [135]

The ECT Act facilitates this modern approach in South Africa[136] by recognising data messages as the functional equivalent of paper.[137] This approach has been endorsed by South Africa's judiciary.[138]

It is worth noting that, in addition to UNICTRAL, there is express support for the principle of functional equivalence in many other common law jurisdictions; for example, in New Zealand,[139] in *R v Hayes*[140] the court stated that:

> Applying the principles of functional equivalence and technological neutrality, the approach to sentencing for computer based crime should start by reference to the penalties that would have been imposed had the crime been committed through paper based means.

In *R v D*[141] the court stated (referring to *Hayes* above as authority):[142]

> It is enough to apply settled case law, in the context of a clear policy choice that has been made in this country to deal with electronic data in the same way as its paper-based equivalents. The policy is premised on principles of functional equivalence and technological neutrality.

---

[134] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 57; Hofman op cit note 42 at 260.
[135] J Faria 'E-commerce and International Legal Harmonization: Time to Go Beyond Functional Equivalence?' (2004) 16 *SA Merc LJ* 531.
[136] Theophilopoulos op cit note 2 at 465.
[137] Mupangavanhu op cit note 99 at 859.
[138] *S v Miller* 2016 (1) SACR 251 (WCC) para 52; *LA Consortium* op cit note 37 at para 12 – 13*; Ndlovu* op cit note 38 at 165; *Meyer* op cit note 38 at para 299. See also the court's analysis in one of the seminal cases involving electronic evidence *Ndiki* op cit note 6 at para 53 where although the term is not specifically used, the analysis performed by the court uses similar logic. See also the South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 62 – 63.
[139] New Zealand uses a common law legal system, which is predominantly based on English common law, much like the legal system in South Africa.
[140] (2006) 23 CRNZ 547 (CA). However, see the criticism of the court's use of the term in D Harvey *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (2017) 58 – 59.
[141] CA287/2010 [2011] NZCA 69 para 64.
[142] See also *Jonathan Dixon v R* [2015] NZSC 147 [20 October 2015] at para 40 – 41 where the basis of the Supreme Court of New Zealand's entire analysis was the concept of functional equivalence.

The Law Commission for England and Wales, in its 2001 paper on Electronic Commerce,[143] referred with approval to the concept of functional equivalence.[144] In summary, the advice by the Commission concluded that English law (as it was in 2001) provided for e-mails, website trading, and other forms of electronic commerce and consequently could be said to already embrace technology and the principle of functional equivalence.

The Law Reform Commission of Ireland's Consultation Paper on Documentary and Electronic Evidence refers to the principle on a number of occasions.[145] After an exhaustive review of international law on electronic evidence, the Irish Commission suggested incorporating the approach espoused in the Model Law, 1996.[146]

In Canada, a predominantly common-law based country[147] with a federal system[148] the promulgation of the Uniform Electronic Commerce Act (UECA) implemented the principles contained in the UNCITRAL Model Law – including functional equivalence.[149] Much like South Africa, the basis of UECA is the Model Law, 1996.[150]

For example, in section 7, if information must be in writing, electronic forms of communication will satisfy this if the information is 'accessible for future use so as to be usable for subsequent reference'.[151] Canada's Supreme Court, in *Dell Computer Corporation v Union des consommateurs*,[152] applied a functional equivalence test to determine whether electronic clauses are reasonably accessible for the parties. The court ultimately found that access to the arbitration clause should be no more difficult than access to its equivalent on paper and in so doing applied and endorsed functional equivalence.

---

[143] Law Commission for England and Wales *Electronic Commerce: Formal Requirements in Commercial Transactions* 2001 *http://www.lawcom.gov.uk/wp-content/uploads/2015/09/electronic_commerce_advice.pdf*, accessed on 25 July 2017.
[144] Ibid para 2.15.
[145] Ireland Law Reform Commission Consultation Paper *Documentary and Electronic Evidence* LRC CP 57 - 2009 *http://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf*, accessed on 25 August 2017.
[146]Ireland Law Reform Commission Consultation Paper *Documentary and Electronic Evidence* LRC CP 57 - 2009 *http://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf* at para 1.34, accessed on 25 August 2017.
[147] Except in Quebec, where it is a civil law system based on the French civil code.
[148] J Gregory 'The UETA and the UECA – Canadian Reflections' (2001) *Idaho Law Review* 441 – 476.
[149] M Smith 'Facilitating electronic commerce through the development of laws to recognize electronic documents and transactions' 2000 *http://publications.gc.ca/Collection-R/LoPBdP/BP/prb0012-e.htm*, accessed on 25 August 2017.
[150] Gregory op cit note 148 at 445.
[151] Section 7 of the UECA.
[152] [2007] 2 S.C.R. 801.

Consequently, as a matter of international best practice, functional equivalence must be incorporated in any law or decision relating to technology and electronic commerce.

2.6 CONCLUSION

As a starting point, South Africa ought to ensure consistency and clarity with the key definition of *data message*. If promulgated as it stands, the current B6B – 2017 version of the Cybercrimes Bill will leave South Africa with two definitions for data message. This anomaly ought to be rectified, and in addition, the newer version of the definition ought to be more concise and neutral (to withstand short to medium term technological development).

The principle of functional equivalence – the lodestar for e-commerce law-making – is applicable in a South African context, and has been approved judicially in a number of reported decisions, both locally and abroad. Any suggested amendments to South Africa's legislative environment must take account of this – and not seek to prefer one form of evidence over another.

3.1 INTRODUCTION

Hearsay evidence is defined in s 3(4) of the Law of Evidence Amendment Act[2] as 'evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving evidence'. In the context of electronic evidence, in addition to the Law of Evidence Amendment Act, one must also potentially consider the ECT Act, the CPA, and the CPEA.[3] This position leads to 'inefficiencies and potential confusions.'[4]

As a result, this chapter will consider whether the Law of Evidence Amendment Act applies to electronic evidence,[5] and in any event, whether the ECT Act frees electronic evidence from the exclusionary hearsay rule.[6] The chapter will then analyse how one consistently determines whether a data message is real evidence, or documentary evidence.[7] The chapter will conclude with a review of selected foreign jurisdictions in so far as the hearsay rule in the context of electronic evidence is concerned – and seek to articulate an ideal position when considering hearsay electronic evidence.

3.2 OVERVIEW AND CONTEXT

Any potential evidence that a party to civil or criminal proceedings wishes to have admitted in court will typically be classified under one or more of three headings: as an object (real

[1] A version of this chapter 3 was published as a two-part article: L Swales 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One' (2018) 21 *PELJ* 2 – 24 and L Swales 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two' (2018) 21 *PELJ* 1 – 25.
[2] Act 45 of 1988. See also P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) ch 13; D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) ch 13.
[3] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 62 – 69. See also D Zeffertt & A Paizes *The South African Law of Evidence* 3 ed (2017) ch 13.
[4] Ibid at 65.
[5] These issues are based on the questions posed in South African Law Reform Commission Discussion Paper 131 *Review of the Law of Evidence* (2014).
[6] Zeffertt & Paizes op cit note 2 at 432.
[7] Zeffertt & Paizes op cit note 2 at 431 – 436; J Hofman & J de Jager 'South Africa' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 761; C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 464 (in particular note 9) and 474 (in particular note 31); P Fourie *Using Social Media as Evidence in South African Courts* (LLM thesis, North-West University, 2016) 8 – 14.

evidence),[8] as a document (documentary evidence),[9] or evidence from a witness (oral evidence).[10]

South African courts are not yet equipped to deal with a variety of computer systems and computer programs that produce electronic evidence – therefore, for practical reasons, a data message is normally presented to court as a print-out when tendering the information as evidence.[11] Consequently, many South African cases have grappled with the issue of how to treat (classify) a printout of the data message – as documentary evidence, or as real evidence?[12]

Increasingly, parties to criminal and civil proceedings rely on some form of data messages as evidence, and the rules relating to hearsay are often at issue (unless the person upon whose credibility the probative value of the data message depends testifies). It is not always practical or reasonable to have every person testify, and the precise classification of a data message, together with its statutory exceptions, become increasingly important.

3.3 DEVELOPMENT OF THE LEGAL POSITION RELATING TO HEARSAY ELECTRONIC EVIDENCE

The promulgation of the Law of Evidence Amendment Act 45 of 1988 took place in October 1988 – it rendered the common law definition of hearsay[13] obsolete.[14] The relevant portion of the Act is contained within s 3 (hearsay evidence) and 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

[8] Schwikkard & van der Merwe op cit note 2 at 421 – 430; A Bellengère et al *The Law of Evidence in South Africa* (2013) 59 – 63; Zeffertt & Paizes op cit note 1 at 849 – 862.
[9] Schwikkard & van der Merwe op cit note 2 at 431 – 436; Bellengère et al op cit note 8 at 59 – 63; Zeffertt & Paizes op cit note 1 at 827 – 843.
[10] Schwikkard & van der Merwe op cit note 2 at 387 – 420. See chapter 2 para 2.3 – 2.4 for an overview of electronic evidence in South Africa.
[11] For example, see *S v Ndiki* 2008 (2) SACR 252 (Ck); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ); *S v Meyer* 2017 JDR 1728 (GJ) para 296 – 300. This observation also accords with my own personal experience in practice.
[12] *Ndiki* supra note 11; *LA Consortium* supra note 11; *Ex parte Rosch* [1998] 1 All SA 319 (W)*; Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W); *S v Brown* 2016 (1) SACR 206 (WCC).
[13] For a useful discussion of hearsay in general, see Schwikkard & van der Merwe op cit note 2 at 287 – 304; Zeffertt & Paizes op cit note 2 at 385-443.
[14] *Ndiki* supra note 11 at para 31; Schwikkard & van der Merwe op cit note 2 at 269; Zeffertt & Paizes op cit note 2 at 389 – 416.

(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 probative value of the evidence;
(v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;
(vi) any prejudice to a party which the admission of such evidence might entail; and
(vii) 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 interests of justice.

The definition of hearsay above in s 3(4)[15] above applies to both civil and criminal matters.[16] Interestingly, as noted by Schwikkard and Van der Merwe[17] (referring also to Zeffertt, Paizes and Skeen)[18] there may be some debate in so far as the interpretation of the word *depends* in the definition above is concerned. The nuance or issue of interpretation is this: when applying the above definition (to any form of evidence, electronic included), does the word *depends* mean that the probative value of the evidence depends entirely on another person? Or only partially? Or is it somewhere in between the two? In my view, the answer lies somewhere in the middle of the two.[19] As suggested by Zeffertt and Paizes,[20] the preferred interpretation must be that the probative value of the evidence must depend substantially, primarily, or even sufficiently upon the credibility of any person other than the person giving evidence. [21]

In any evidentiary dispute involving hearsay, the statutory definition above will be the point of departure[22] when determining whether a data message constitutes hearsay. Of course, in order to draw any definitive conclusion on whether a data message is admissible, the statutory definition above requires the reading in and context of: applicable case law, the ECT Act, and other relevant legislation.

[15] See the definition above in chapter 3 para 3.1.
[16] Hofman & de Jager op cit note 7 at 770 – 771.
[17] P Schwikkard & S van der Merwe *Principles of Evidence* 3 ed (2009) at 275 and particularly the discussion at para 13.4; Schwikkard & van der Merwe op cit note 2 at 293 – 294.
[18] D Zeffertt, A Paizes & A Skeen *The South African Law of Evidence* (2003) 364 – 402; see Zeffertt & Paizes op cit note 2 at 389 – 391.
[19] A view endorsed in Zeffertt & Paizes op cit note 2 at 390 – 391 where the authors state: 'a case may be made for reading the words as meaning depends substantially or primarily upon'.
[20] Zeffertt & Paizes op cit note 2 at 390 – 391; Schwikkard & van der Merwe op cit note 2 at 293 – 294. See also Zeffertt & Paizes op cit note 3 ch 13.
[21] Zeffertt & Paizes op cit note 2 at 390, in particular, see notes 24 – 28 thereof where an analysis of hearsay related cases decided before the Law of Evidence Amendment Act, going back as far as 1837 inform the view expressed.
[22] *S v Ndiki* supra note 11 para 31.

3.4 *CAN ELECTRONIC EVIDENCE CONSTITUTE HEARSAY?*

It would seem at first blush that if electronic evidence were to be exempt from the rules regulating hearsay, the net effect of this approach would be to favour electronic evidence over other forms of evidence. This could lead to forum or format shopping[23] and would undoubtedly abolish any form of functional equivalence.[24] Ideally, any form of electronic evidence must be treated as the functional equivalent of traditional evidence as far as possible.

It cannot be that hearsay electronic evidence faces fewer hurdles on its admission to court (than traditional hearsay evidence), and similarly, South Africa cannot sustain a position where it is more cumbersome (with more requirements to meet) to admit electronic forms of hearsay evidence.

Prior to the promulgation of the ECT Act, some early decisions[25] favoured an approach which suggested that electronic evidence could not constitute hearsay as it was produced by a machine, and therefore, its probative value did not depend on a person. This approach was based on the rationale of the first reported South African decision dealing with hearsay electronic evidence – *Narlis*,[26] where the key finding was: 'a computer, perhaps fortunately, is not a person' (and therefore evidence produced by a computer cannot depend on the probative value of a person). This decision provided the grounding for computer-based evidence to be inadmissible under the then applicable statutory provisions.

In *S v Harper*,[27] the court considered whether a computer could be classified as a document in terms of the CPA. It ultimately found a computer could not be a document (for purposes of the CPA), and held that:

> Computers do record and store information but they do a great deal else; inter alia, they sort and collate information and make adjustments… 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 the mere storage or recording of information.[28]

However, the court did note that a print-out by a computer could be a document for purposes of the CPA, and held that:

---

[23] Hofman & de Jager op cit note 7 at 766 – 767.
[24] J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 257.
[25] A Mapoma *A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM thesis, University of South Africa, 1997) 20 – 26.
[26] 1976 (2) SA 573 (A).
[27] 1981 (1) SA 88 (D).
[28] Ibid at 259.

> 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 print-outs themselves are admissible.[29]

As noted by the court in *Ndiki*,[30] the *Harper* judgment has been misunderstood to some extent. The ratio above, as the law was then, was authority for the proposition that evidence on a computer (on computer storage) would not be covered by the exception in the CPA. However, if the information was reduced to a print-out, the evidence (as long as it met the statutory requirements in the CPA) could be regarded as a document, and therefore admissible.

Moreover, in *Ex Parte Rosch*,[31] the court found that the Law of Evidence Amendment Act was not applicable to computer printouts because, on a similar basis to the rationale in *Narlis*, the court found that a computer was not a person – it held that:

> The provisions of the Law of Evidence Amendment Act 45 of 1988 regarding hearsay evidence were also not applicable as the computer was not a 'person' as contemplated in section 3(4) of that Act.[32]

Further, in *S v Mashiyi,*[33] another case based on the rationale of the *Narlis*, the court found it was unable in terms of the prevailing law, to admit as evidence the disputed documents, which contained information that had been processed and generated by a computer.[34] It reached this decision on the basis that the Law of Evidence Amendment Act could not apply, as a computer was not a person. As suggested elsewhere, this authority, although of little consequence today (decided prior to the ECT Act), is 'doubtful'.[35] In *Ndiki*,[36] the court rejected the reasoning above and stated as follows:

> Cutting away the frills, the suggested approach, based on the aforegoing decisions [*Narlis, Ex Parte Rosch* and *Mashiyi*], is that a computer is not a person and if it carried out active functions, over and above the mere storage of information, the disputed documents are inadmissible. For the same reason the provisions of the Law of Evidence Amendment Act relating to hearsay evidence is also of no assistance because hearsay evidence only extends to oral or written statements, the probative value of which depends upon the credibility of a 'person'. As I would indicate hereinunder, *such an approach to computer generated evidence is in my view incorrect and of very little assistance*. (my emphasis).

---

[29] Ibid.
[30] *S v Ndiki* supra note 11 paras 16 – 18 where Van Zyl J clearly and logically summarises the *S v Harper* judgment.
[31] [1998] 1 All SA 319 (W).
[32] Ibid at 321.
[33] 2002 (2) SACR 387 (TkD).
[34] Ibid at 390 – 391.
[35] Zeffertt & Paizes op cit note 2 at 432 see particularly footnote 313. See also D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 1)' (2010) 3 *TSAR* 563 where the author notes he cannot support the finding in *Mashiyi* and, correctly in my view, criticizes the judgment on the basis that the evidence could surely have been admitted as real evidence (as an object).
[36] *S v Ndiki* supra note 11 para 11 – 12.

A misunderstanding[37] of technology, and the nature of technology, most likely led to these early approaches. The primary position adopted by Van Zyl J in *Ndiki* (and his rejection of the logic above) should be endorsed and followed in subsequent decisions – it is a pragmatic and common-sense approach which aligns itself to international best practice.[38]

As noted elsewhere,[39] the view that a computer is not a person (and therefore its probative value does not depend on a person) misses the fact that at some stage in its genesis all computers (and data messages) rely on the credibility of some person to design,[40] activate,[41] program, enable, disable, etcetera, the computer and/or technology. Moreover, this view arguably does not take account of South Africa's position on evidence in general – that is, the distinction between real and documentary evidence where an object should be admissible in any event (subject to it being relevant and a court assessing its evidentiary weight).

The Law of Evidence Amendment Act notwithstanding, section 15 of the ECT Act provides for the admissibility of electronic evidence.[42] This section has had, and will continue to have a 'huge impact'[43] on the law of evidence – it reads as follows:

> 15. Admissibility and evidential weight of data messages
>
> (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
>
> (a) on the mere grounds that it is constituted by a data message; or
>
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
>
> (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;

[37] Fourie op cit note 7 at 31.
[38] D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 130 where the authors praise the Judgment in *Ndiki*.
[39] Zeffertt & Paizes op cit note 2 at 433.
[40] Fourie op cit note 7 at 31 – 32.
[41] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 68 – 69.
[42] This chapter only discusses admissibility of electronic evidence in the context of hearsay. For a full discussion on admissibility of all forms of electronic evidence, see chapter 5 below.
[43] D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)' (2010) 4 *TSAR* 731.

(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.

Early academic views[44] on this section favoured an interpretation[45] that would exempt electronic evidence from the rules regulating hearsay altogether, with a court being primarily focused on assessing the weight[46] of the electronic evidence and simply admitting all forms of electronic evidence.

The argument went along the following lines: s 15(2) of the ECT Act enjoins courts to give due evidential weight to data messages. Moreover, s 15(3) provides factors to assess evidential weight – these factors are remarkably similar to the questions a court must consider when performing a hearsay analysis. Accordingly, so the argument goes, data messages would be exempt from the rules pertaining to hearsay on the basis that courts must give data messages due evidential weight, and are then given factors (similar to the hearsay factors listed in the Law of Evidence Amendment Act) to consider.

Both courts and other academics have roundly rejected[47] the view above – to be fair to one of the authors of this initial view though, she did herself state in the article where this controversial view was espoused that the effect of s 15 of the ECT Act on the authenticity rule

[44] D Collier 'Evidently not so Simple: Producing Computer Print-outs in Court' 2005 *Juta Business Law* 6 – 9; Hofman op cit note 24 at 262.
[45] This interpretation appears to have been retracted by Collier herself in Schwikkard & van der Merwe op cit note 17 at 414 – 415, particularly footnote 42 – 43 thereof. The chapter dealing with electronic evidence in the latest version of this text (Schwikkard & van der Merwe op cit note 2 ch 21) is written by a different author and this initial view is not canvassed in any detail.
[46] Bellengère et al op cit note 8 at 76.
[47] *S v Meyer* supra note 11 para 299; *S v Brown* supra note 12 para 16; *Ndlovu* supra note 12 at 172; *LA Consortium* supra note 11 para 19; Theophilopoulos op cit note 7 at 474 – 775; M Watney 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 *Journal of Information, Law and Technology* 3 – 7.

and the hearsay rule is not clear. Moreover, in a later publication,[48] the author further stated that courts are unlikely to adopt this progressive view.

Consequently, since this early debate on the import and meaning of s 15 of the ECT Act, there is universal acceptance[49] that data messages are not exempt from the rules regulating hearsay. Rightly, in my view – it would clearly go against the principle of functional equivalence if data messages were to be exempt from hearsay.

In so far as s 15 of the ECT Act is concerned, in *Ndlovu*, the court held that 'there is no reason to suppose that s 15 seeks to override the normal rules applying to hearsay evidence'.[50] It further noted that the 'the rules relating to hearsay evidence have not been excluded entirely by s 15(1)'.[51] Finally, and logically so, the court opined that if a data message were to be rendered admissible in all circumstances 'without further ado', then that position would clearly 'elevate'[52] data messages above traditional form of evidence. In support of *Ndlovu*, Bozalek J in *S v Brown*[53] held:

> I agree with the observation of Gautschi AJ [in Ndlovu] that sec 15(1)(a) does not render a data message admissible without further ado. The provisions of sec 15 certainly do not exclude our common law of evidence.

Furthermore, in *Ndiki,*[54] the court held:

> The definition of hearsay quite clearly extends to documentary evidence. Whether or not the evidence contained in the document can be said to depend upon the credibility of a person, is a factual question that must in turn be determined from the facts and circumstances of each case. If a computer print-out contains a statement of which a person has personal knowledge and which is stored in the computer's memory, its use in evidence depends on the credibility of an identifiable person and would therefore constitute hearsay. On the other hand, where the probative value of a statement in the print-out is dependent upon the "credibility" of the computer itself, section 3 will not apply.

Moreover, in *LA Consortium*,[55] the court held:

> The principle of 'functional equivalence' does not free data messages from the normal strictures of the law of evidence but only from those referred to in s 15(1). It follows that,

---

[48] Schwikkard & van der Merwe op cit note 17 at 415 where Collier notes that it is 'unlikely' that courts will adopt this approach.
[49] *S v Meyer* supra note 11 para 299; *S v Brown* supra note 12 para 18; *LA Consortium* supra note 11 para 19; *S v Ndiki* supra note 11 para 31; *Ndlovu* supra note 12 at 172 – 173. See also Hofman op cit note 24 at 262; Theophilopoulos op cit note 7 at 474 – 475; Zeffertt & Paizes op cit note 2 at 432 – 435.
[50] *Ndlovu* supra note 12 at 172 – 173.
[51] *Ndlovu* supra note 12 at 172 – 173. See also Hofman & de Jager op cit note 7 at 767 – 768.
[52] *Ndlovu* supra note 12 at 173.
[53] *S v Brown* supra note 12 para 18.
[54] *S v Ndiki* supra note 11 para 31.
[55] *LA Consortium* supra note 11 para 13.

> 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.

More recently, in *S v Meyer*,[56] the court joined the chorus above and held:

> Section 15 (1) does not, however make all data messages automatically admissible. According to the ECT Act data messages are the functional equivalents of documents and therefore, except where the Act specifically provides for exceptions, the ordinary common law requirements for the admissibility of documents must be adhered to.

In summation then: can a data message constitute hearsay within the meaning of s 3 of the Law of Evidence Amendment Act? In short, yes. Simply put, s 15 of the ECT Act does not override the normal rules applying to hearsay in so far as data messages are concerned.[57] Moreover, the ECT Act ensures that data messages are functional equivalents[58] of paper. Consequently, except where specific exceptions are made, the normal position in so far as hearsay (in terms of the Law of Evidence Amendment Act) applies[59] equally to documentary hearsay as it does to electronic hearsay.

Finally, and the early academic debate about the import of s 15 of the ECT Act notwithstanding, the provisions thereof do not free data messages from the exclusionary hearsay rules[60] – if the credibility of the data message depends upon a natural person. Conversely, if a data message's credibility depends substantially upon an automated process, [61] (for example, GPS data or mobile phone call records) then that evidence should be regarded as real[62] in nature and should not be subject to a hearsay enquiry. [63]

---

[56] *S v Meyer* supra note 11 para 299.
[57] *S v Meyer* supra note 11 para 299; *S v Brown* supra note 12 para 18; *LA Consortium* supra note 11 para 19; *S v Ndiki* supra note 11 para 31; *Ndlovu* supra note 12 at 172 – 173. See also Theophilopoulos op cit note 7 at 474 – 475; Watney op cit note 47 at 8 – 11; Hofman & de Jager op cit note 7 at 776 – 777; Zeffertt & Paizes op cit note 2 at 432 – 435.
[58] S Papadopoulos & S Snail (eds) *Cyberlaw@SA III* (2012) 322.
[59] Van der Merwe et al op cit note 38 at 130.
[60] Subject to s 15(4) of the ECT Act.
[61] Theophilopoulos op cit note 7 at 474 and in particular footnote 31.
[62] D Bainbridge *Introduction to Information Technology Law* 6 ed (2008) 490.
[63] *Ndlovu* supra note 12 at 171 – 173; *S v Ndiki* supra note 11 para 31; *LA Consortium* supra note 11 para 13.

3.5 *HOW DOES ONE CONSISTENTLY DETERMINE WHETHER A DATA MESSAGE IS DOCUMENTARY EVIDENCE OR REAL EVIDENCE?*

Real evidence[64] consists of objects (things) – tangible items – that are in and of themselves evidence, and are available for inspection by a court, for example: A gun, a bullet, or a knife.[65] As noted in *S v M*:[66]

> Real evidence is an object which, upon proper identification, becomes, of itself, evidence (such as a knife, photograph, voice recording, letter or even the appearance of a witness in the witness-box).

Real evidence[67] is not subject to exclusion[68] if it is relevant (and if no other statutory exception excludes it).[69] Importantly for present purposes, real evidence is not subject to the hearsay rules[70] for the simple reason that it is what it purports to be. However, real evidence (traditionally, in any event) is typically only meaningful when supplemented by witness testimony i.e.: there must be someone present in court to explain its relevance.[71]

Consequently, as real evidence, a data message need not be admitted to court under one of the various hearsay exceptions,[72] and technically, is evidence in and of itself to which a court must accord appropriate weight (even without oral testimony – although, without oral testimony the evidence is likely to have little evidentiary weight). Therefore, if evidence is real in nature, it is not in my view conceptually correct to subject that evidence to a hearsay enquiry.

A further difficulty is that our courts have taken differing views on the meaning of the word document.[73] This inconsistency in approach is particularly problematic in the context of electronic evidence where the classification of evidence as real or documentary is an important

---

[64] S Mason & D Seng 'Real Evidence' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 39 define real evidence as 'material objects other than documents, produced for inspection of the court' relying on H Malek (ed) *Phipson on Evidence* 17 ed (2009). See further the newer version of this text, S Mason & D Seng 'Real Evidence' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 39 – 43.
[65] Zeffertt & Paizes op cit note 2 at 849; Schwikkard & van der Merwe op cit note 2 at 421.
[66] 2002 (2) SACR 411 (SCA) para 31. This definition and case is used by all major evidence text book authors in South Africa when referring to real evidence.
[67] See the discussion of real evidence in the context of electronic evidence in South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 35 – 37.
[68] Hofman op cit note 24 at 268.
[69] Hofman & de Jager op cit note 7 at 776 – 777.
[70] Hofman & de Jager op cit note 7 at 777; *S v Ndiki* supra note 11 para 31; *Ndlovu* supra note 12 at 173.
[71] Schwikkard & van der Merwe op cit note 17 at 395; Zeffertt & Paizes op cit note 2 at 849; Hofman & de Jager op cit note 7 at 776 – 779; van der Merwe et al op cit note 38 at 124 – 130.
[72] See para 3.6 below for a discussion of exceptions to the hearsay rule.
[73] Schwikkard & van der Merwe op cit note 2 at 313 – 315.

consideration[74] in determining the evidentiary rules applicable. For example, in the case of *Seccombe v Attorney-General* it was held that the word document is:

> a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made…[75]

This early definition clearly suggests that a data message could be included in the definition of document.[76] Conversely, however, in *S v Mpumlo,*[77] the court found that video evidence is not a *document*, and classified the evidence as real evidence[78] by finding that:

> I have no doubt that a video film, like a tape recording, is real evidence, as distinct from documentary evidence, and, provided it is relevant, it may be produced as admissible evidence, subject of course to any dispute that may arise either as to its authenticity or the interpretation thereof.[79]

On the logic followed by the court in *Mpumlo*, data messages could also be treated as real evidence requiring the court to focus on authenticity, accuracy and interpretation once the evidence is received (assuming it is relevant). In other words, on this logic, the only hurdle to the admissibility of real data message evidence is relevance.

In *S v Baleka (1),*[80] the court agreed with the approach in *Mpumlo* above, but only in so far as the video aspect of the evidence is concerned (leaving the categorisation and question of the audio aspect open). Van Dijkhorst J held as follows:

> I agree with the conclusion of Mullins J (in *Mpumlo*) that a video tape is real evidence. It remains to be considered whether the aural component thereof is to be equated to a tape sound recording and dealt with on the same basis as documentary evidence.[81]

However, in *S v Ramgobin*,[82] the court took the opposite view and found that video evidence is documentary evidence, and found the decision in *Mpumlo* to be incorrect. This view guards against the possibility of doctored or edited evidence being admissible. There is strong support for this decision by Zeffertt.[83]

---

[74] Fourie op cit note 7 at 31 at 8 – 14.
[75] 1919 TPD 270 at 277.
[76] See further discussion on this point, De Villiers (1) op cit note 35 at 564 – 572.
[77] 1986 4 All SA 197 (E). See also Fourie op cit note 7 at 8 – 14; G van Tonder *The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective* (LLM thesis, University of the Western Cape, 2013) 16 – 18.
[78] See Zeffertt & Paizes op cit note 2 at 854 where this decision is criticised.
[79] *S v Mpumlo* supra note 77 at 202.
[80] 1986 (4) SA 192 (T).
[81] Ibid at 433.
[82] 1986 (4) SA 117 (N).
[83] Zeffertt & Paizes op cit note 2 at 855 – 857.

Further, in *S v Baleka (3),*[84] the court had occasion to consider *Ramgobin*, and via Van Dijkhorst J, rejected the approach by Milne JP in *Ramgobin* and stated:

> I deal with tape recordings as I would deal with any other type of real evidence tendered where its admissibility is disputed. The test is whether it is relevant. It will be relevant if it has probative value. It will only have probative value if it is linked to the issues to be decided.[85]

In addition, in *S v Nieuwoudt,*[86] and in *S* v *Fuhri,*[87] in two appeal matters, it was held that the approach in *Baleka (3)* was preferable. How can these decisions be interpreted in the context of data messages? On one hand, the only hurdle to admissibility is relevance (if the data message is classified as real evidence); but on the other hand, in addition to relevance, the data message must also be authentic.

Based on the logic in *Baleka (3)*, and those cases that support it, the classification of a data message as real evidence will mean that if a court determines a data message is relevant, the evidence is admissible. On this logic and rationale, the enquiry about authenticity will be central when a court accords the evidence weight – rather than when a court considers admissibility.

However, in *S v Koralev*,[88] a child pornography matter involving data messages in the form of digital photographs, the court noted, 'because of modern technology, it is essential for evidence in relation to such images [digital images] to be approached with extreme caution'.[89] The court again endorsed the approach in *Baleka* (3), but in effect what it did was introduce a modified version of the rationale in *Ramgobin*,[90] by finding that in order to be admissible, real evidence must not only be relevant, but also authentic (with some form of corroboration as to the accuracy of the image), the court held:

> Before the images in question could be admissible in evidence against the appellants there had to be some proof of their accuracy in the form of corroboration that the events depicted therein actually occurred; and
>
> Corroboration in the sense required must be found in some independent source of evidence, which makes the evidence constituted by the images in the photographs and video recordings more acceptable in that it supports an aspect or aspects thereof.[91]

---

[84] 1986 (4) SA 1005 (T).
[85] Ibid at 1026.
[86] 1990 (4) SA 217 (A).
[87] 1994 (2) SACR 829 (A) 835.
[88] 2006 (2) SACR 298 (N).
[89] Ibid at 307.
[90] See Zeffertt & Paizes op cit note 2 at 852.
[91] *S v Koralev* supra note 88 at 306 – 307.

Consequently, before the digital images could be admissible in evidence, the court found that there had to be some proof of their authenticity in the form of corroboration – for example, a photographer or some other witness must testify as to the veracity of the images.

As noted by Hofman,[92] it is quite possible to adopt the interpretation taken in these video and audio admissibility cases to data messages. Consequently, if one prefers the approach in the KwaZulu-Natal cases[93] illustrated by *Ramgobin*, then a data message that relies on the credibility of a computer would be admissible if it is relevant *and authentic* (my emphasis).[94] Conversely, if one prefers the approaches taken in the Gauteng cases via *Baleka (1)* and *Baleka (3)* (and supported by Hefer JA in two appeal decisions), then authenticity is not a pre-requisite for admissibility and a data message that relies substantially on the credibility of a computer (automated process) will be admissible if relevant.[95]

Consequently, there is a strong argument in the context of data messages that where the credibility of the data message substantially depends on the credibility of a computer, application, machine or mechanical process, it is real evidence and only needs to be relevant to be admissible. Conversely, there is an equally strong argument to suggest that the data message evidence must not only be relevant to be admissible, but also authentic.[96]

In *Motata v Nair NO*,[97] the court weighed up the various approaches and held it was unnecessary to decide whether proof of authenticity is in fact a prerequisite for the admissibility of audio recordings. In these circumstances, in the context of electronic evidence, the issue that remains unclear relates to the admissibility of real evidence in the form of data messages.

Given the ease of manipulation[98] of data messages, the production of some evidence to show a court that a data message is authentic (accurate and reliable representation of the information) is probably desirable – but quite what that is in each case will turn on the relevant facts and be at the discretion of each respective judicial officer. Authenticity as a pre-requisite for admissibility (in addition to relevance) is supported by: *Koralev* (which dealt specifically

[92] Hofman & de Jager op cit note 7 at 778 – 779.
[93] See also *S v Singh* 1975 (1) SA 330 (N).
[94] N Whitear-Nel 'Admissibility of hearsay evidence' (2007) 20 *SACJ* 116 where the author notes that the approach of the court in Koralev 'leads to the possibility that relevant evidence may be excluded because it is not original or not corroborated, where its reliability is not placed in issue by the defence, only its admissibility. This is not in the interests of justice.'
[95] *Motata v Nair NO* 2009 (1) SACR 263 (T) para 21 where the court summarises the various approaches.
[96] See chapter 5, paragraph 5.3 and 5.4 below for a further discussion on real and documentary electronic evidence.
[97] Ibid.
[98] Theophilopoulos op cit note 7 at 461; Zeffertt & Paizes op cit note 2 at 852 – 854.

with data messages); widely quoted academics;[99] *Ramgobin*; and is consistent with the most recent High Court judgment of *LA Consortium*[100] (the Supreme Court of Appeal has not yet had occasion to consider this issue).

Conversely, there appears to be equal justification for a court to accept data messages as evidence (when the evidence is real in nature) on the basis that it is relevant – and then to consider accuracy when determining weight.[101]

As a result, in the context of electronic evidence, it is critical to determine the nature of the data message, and then to analyse the common law and/or statutory requirements for admission of that type of evidence. Questions that might be asked include: Does the data message rely substantially on the credibility of a machine, computer or mechanical process? Does the data message contain statements or conclusions that rely on a person? Is the data message substantially automated without human intervention?

There is an argument that video, audio and graphics more closely resemble documentary, rather than real evidence, and in this regard Hofman states:

> video, audio and graphics now resemble documents more than the knife and bullet that are the traditional examples of real evidence. In data message form, graphics, audio and video are susceptible to error and falsification in the same way as data messages that embody documentary content. They cannot prove themselves to be anything other than data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance.[102]

Accordingly, some authors are of the view that graphics, audio and video in data message form constitute documentary evidence.[103] This view was accepted by the Western Cape High Court in *Brown* by Bozalek J. Here,[104] where the court had occasion to discuss how best to classify electronic evidence as real or documentary, the decision in *Ndiki*[105] was endorsed – the court found that the best approach is to consider the nature[106] of the evidence, together with the reason for its admission. Furthermore, the court in *Brown* found, that much like in *Ndiki*, the

[99] Zeffertt & Paizes op cit note 2 at 852.
[100] *LA Consortium* supra note 11 para 12 – 13 where the court found that the evidence was both real and documentary – in so doing, it applied a hearsay enquiry to admit the evidence and considered the authenticity and reliability of the evidence as key factors to be considered before admitting the evidence.
[101] *S v Baleka (3)* supra note 84; *Motata v Nair NO* supra note 95 para 21. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 35 – 37.
[102] Hofman op cit note 24 at 268. This argument is endorsed by Bozalek J in *S v Brown* supra note 12 para 19.
[103] Hofman op cit note 24 at 268; Zeffertt & Paizes op cit note 2 at 852.
[104] *S v Brown* supra note 12 para 18.
[105] *S v Ndiki* supra note 11 para 53.
[106] *S v Brown* supra note 12 para 20.

transient and fluid nature of electronic communications meant that its admission into evidence was better suited as a document, rather than an object (real evidence).[107]

With that being the case, an electronic communication in the form of a document, in circumstances where it is not considered real in nature, in order to be admissible,[108] must be: produced, original, and authentic (subject to concessions provided in the ECT Act regarding originality and production).[109] As noted by Gautschi AJ:[110]

> For documentary evidence to be admissible, the statements contained in the document must be relevant and otherwise admissible; the authenticity of the document must be proved; and the original document must normally be produced.

More recently, in *S v Meyer*,[111] in the context of documentary evidence, the court found:

> According to the ECT Act data messages are the functional equivalents of documents and therefore, except where the Act specifically provides for exceptions, the ordinary common law requirements for the admissibility of documents must be adhered to.

Therefore, the question of whether a data message is a document (documentary evidence) or an object (real evidence) can be pivotal in determining whether evidence is admissible or inadmissible (due to hearsay), and will further dictate the hurdles to be overcome in its admission in evidence.

In *Ndlovu,* Gautschi AJ found that data messages could be either real evidence or documentary evidence, depending on the nature of the evidence by holding as follows:

> Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving the 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 (because information was processed by 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' evidence to be admitted, and due evidential weight to be given thereto according to an assessment having regard to certain factors.

[107] Ibid.
[108] Theophilopoulos op cit note 7 at 461 – 480.
[109] Schwikkard & van der Merwe op cit note 2 at 431 – 435.
[110] *Ndlovu* supra note 12 at 165 – 166.
[111] *S v Meyer* supra note 11 para 299.

In *Ndiki*[112](via Van Zyl J), the court followed similar logic used in *Ndlovu* by finding that a data message will be considered real evidence if its credibility depends on the reliability of the technology, by holding that:

> Evidence on the other hand that depends solely upon the reliability and accuracy of the computer itself and its operating systems or programs, constitutes real evidence. What section 15 of the ECT 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 subsection (2) and the Court's discretion simply relates to an assessment of the evidential weight to be given thereto.

However, the court in *Ndiki* did express reservations about the reliability of computer-based evidence and obiter expressed the view[113] that *all* electronic evidence should be hearsay.[114] The court did not deem it necessary to finally determine this issue and left the question open. As will be seen below in discussing the position in England, Canada, and the United States, this position should be avoided.

In *LA Consortium*, Malan J supported the distinction created in both *Ndlovu* and *Ndiki* by finding that evidence in the form of computer printouts were real evidence by stating that: 'this is real evidence the probative value of which depends on the reliability and accuracy of the computer and its operating systems'.[115] The court went further, unfortunately as noted elsewhere,[116] to state: 'the data messages relied upon in this case are not only real evidence but includes hearsay.' Perhaps the court meant to say the data message evidence was both real evidence and documentary hearsay evidence (as was the case in *Ndiki*). This is not clear from the judgment and it appears the court was referring to the printouts as being both real and documentary in nature – this classification is problematic as conceptually, real evidence cannot be subjected to a hearsay analysis – if the evidence is real in nature, it is therefore what it purports to be. It cannot be subject to the credibility of a person, it is in theory subject to the credibility of a computer or the relevant technology.

In *Brown*, Bozalek J took a conservative approach (although the court did endorse the decision in *Ndiki*), and found that even though the admissibility of photographs (stored via

---

[112] *S v Ndiki* supra note 11 para 7.
[113] *S v Ndiki* supra note 11 para 33. See also Hofman & de Jager op cit note 7 at 777 where the reservations expressed in *Ndiki* are based on the misgivings noted in the evidentiary portion of the *annual survey of South African law* by Bilchitz in 1998 where the view espoused is that all computer based evidence is subject to credibility of a natural person and should therefore always be regarded as hearsay. This view should be rejected as it is inconsistent with recent case law, the international position, and with South Africa's common law on real evidence.
[114] This view is only *obiter*, and Van Zyl J did not feel it necessary to decide this point.
[115] *LA Consortium* supra note 11 para 16.
[116] De Villiers (2) op cit note 43 at 733.

electronic means) were more akin to being real evidence, they were ultimately classified as documentary evidence. The court found that:

> Given the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device I consider that they are more appropriately dealt with as documentary evidence rather than '*real evidence'*. I associate myself, furthermore, with the approach followed in *S v Ndiki and others* [2007] 2 All SA 185 (CK) where Van Zyl J expressed the view that the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one was dealing with and what the requirements for its admissibility are.

Herein lies some of the controversy (or room for law reform) – when should data messages be considered documentary evidence and when should they be considered real evidence? Or do data messages constitute a hybrid of the two forms of evidence?

With the law as it currently stands, the solution is to:[117] consider the nature[118] of the data message, and the requirements of the relevant legislation (or common law requirements).[119] As noted in *Ndiki*:

> It is an issue that must be determined on the facts of each case having regard to what it is that the party concerned wishes to prove with the document, the contents thereof, the function performed by the computer and the requirements of the relevant section relied upon for the admission of the document in question.[120]

It may be that a data message exhibits characteristics of both real and documentary evidence, as was the case in both *Ndiki* and *LA Consortium*, making the distinction between real or documentary difficult to draw. As many have noted (sometimes with more concern than necessary in an advancing digital age), it is certainly possible to amend or surreptitiously edit data messages. These concerns and apparent difficulties notwithstanding, it should not mean all data messages are treated as documentary evidence. If a data message relies substantially

[117] De Villiers (1) op cit note 35 at 568 – 569 where the author suggests a five step approach. In my view, this is overly complicated – a court must concern itself, primarily, with the nature of the evidence and then apply the normal common law rules applicable to that type of evidence. See also Fourie op cit note 9 para 2.1.2 at 13 – 14 where the author suggests a purpose test. While I can agree that the purpose of the evidence is important, I cannot agree with the following statement: 'if the purpose is for the court to read or listen to and interpret the contents of a piece of evidence, such evidence should be considered documentary evidence'. The nature of the evidence must dictate its classification, not its purpose. In this regard, see *S v Brown* supra note 12 para 20; S *v Ndiki* supra note 11 para 53; Theophilopoulos op cit note 7 at 461 – 479.

[118] S v Brown supra note 12 para 20; *S v Ndiki* supra note 11 paras 20 – 21.

[119] *S v Ndiki* supra note 11 paras 20 – 21; De Villiers (1) op cit note 35 at 566 – 567; Fourie op cit note 7 at 8 – 11.

[120] *S v Ndiki* supra note 11 paras 20 – 21.

on technology (without human intervention) then that evidence should be real in nature. To guard against manipulation, a court must satisfy itself that the evidence is authentic (reliable, accurate) – i.e. it is what it purports to be. Furthermore, a court has a discretion when deciding what weight to give the evidence.

Much of the debate above arises in contexts where data message are produced as documents in the form of a print out. Would it make any difference if the data messages were produced via a different medium, for example, projection in court or transmission in some other electronic format? There does not appear to be any reason why the principles set out above should not apply: namely, the nature of the data message must be considered together with empowering legislation (or common law). If by its nature a data message relies predominantly or substantially on a computer or mechanical process, its manner of presentation to court is irrelevant, it should still be regarded as real evidence. Similarly, if a data message contains conclusions, statements or assumptions that rely on the credibility of a natural person, regardless of the manner of presentation, it should be subject to the hearsay rules.

3.6 EXCEPTIONS TO THE HEARSAY RULE

If a data message is classified as documentary evidence, and not real evidence, the hearsay trap may still mean the evidence is excluded.[121] The hearsay rule will apply if the probative value of the data message depends upon the credibility of any person other than the person giving evidence.[122] However, there are a number of statutory exceptions where hearsay evidence will be admitted.[123]

3.6.1 The Law of Evidence Amendment Act

The Law of Evidence Amendment Act changed the law of evidence by introducing a statutory definition for hearsay, and including several exceptions to the exclusionary hearsay rule.[124] The three exceptions created by s 3(1) are as follows:

- 3(1)(*a*) where the party against whom the hearsay evidence is to be adduced agrees to its admission;

[121] Hofman & de Jager op cit note 7 at 770 – 771.
[122] Hearsay as defined by s 3 (4) of the Law of Evidence Amendment Act 45 of 1988.
[123]Hofman op cit note 24 at 265 – 268; Schwikkard & van der Merwe op cit note 2 at 305 – 323; Zeffertt & Paizes op cit note 2 at 418 – 441.
[124] Ibid.

- 3(1)(*b*) where the person upon whose credibility the probative value of the hearsay evidence depends testifies; and

- 3(1)(*c*) where a court is provided with a list of factors,[125] and ultimately has a wide discretion to admit hearsay evidence if the court deems it to be in the interests of justice to admit such evidence.

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 via the broad discretion vested in a court via the Law of Evidence Amendment Act.[126]

3.6.2 The Civil Proceedings Evidence Act

The three primary exceptions created by the CPEA (in the context of data messages) relate to bankers' books, business records, and a general exception where the author of a data message is not available.[127] The promulgation of the CPEA took place when data messages were not fully contemplated or developed, but as noted by Hofman,[128] 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 in relation to the recording of another in the ordinary course of duty.

The details pertaining to these exceptions are largely nullified[129] by the Law of Evidence Amendment Act (and are therefore less applicable than they once were).[130] Even though

[125] See a reproduction of this section of the Law of Evidence Amendment Act above at para 3.2.
[126] *LA Consortium* supra note 11 para 16.
[127] Schwikkard & van der Merwe op cit note 2 at 310 – 316.
[128] Hofman & de Jager op cit note 7 at 771.
[129] Ibid.
[130] Schwikkard & van der Merwe op cit note 2 at 311 – 316; Zeffertt & Paizes op cit note 2 at 418 – 429; Bellengère et al op cit note 8 at 295 – 305.

controversial, the creation of a business records exception in s 15 of the ECT Act, discussed below, has further nullified the use of the older, more traditional hearsay exceptions.

3.6.3 The Criminal Procedure Act

As is the case with the CPEA, and the ECT Act discussed directly below, the CPA creates an exception for business records in terms of s 221.[131]

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

The conditions for admissibility are: 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.

Moreover, s 222 of the CPA incorporates s 33 – 38 of the CPEA making them applicable to all forms of criminal proceedings. In the present context, that means that the exception created by s 34 of the CPEA (for the admissibility of a data message where the author is not available), is also applicable to criminal proceedings.

Finally, s 236 and s 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.

3.6.4 The Electronic Communications and Transactions Act

Section 15(4)[132]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,[133] has been criticised because of the 'difficulties'[134] it creates. It reads as follows:

> 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

[131] Hofman & de Jager op cit note 7 at 773 – 776; Schwikkard & van der Merwe op cit note 17 at 290 – 301; Zeffertt & Paizes op cit note 2 at 418 – 441.
[132] A Duvenhage *An evidential analysis of section 15 (4) of the Electronic Communications and Transactions Act 25 of 2002* (LLM thesis, University of Pretoria, 2016) 9 – 34.
[133] *LA Consortium* supra note 11 at para 12.
[134] Hofman & de Jager op cit note 7 at 771 – 772; De Villiers (2) op cit note 43 at 734.

> 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 lists six difficulties with the section.[135] The two primary difficulties are: 1) the ECT Act exception is much wider than previous business records exceptions; and 2) the ECT Act exception creates a situation where there is an 'unjustified shifting of the onus of proof' in criminal cases (a so-called reverse onus provision). These difficulties appear to remain and although the section has been at issue in several cases, it has often received superficial judicial treatment.[136] In *LA Consortium*[137] the court found 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.

In *Absa Bank Ltd v Le Roux*,[138] 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'.[139]

In the Supreme Court of Appeal, in *Firstrand Bank Limited v Venter*,[140] in the context of s 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[141] dealing with s 15(4), in *Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited*,[142] Du Plessis J held:

---

[135] Hofman op cit note 24 at 267 – 268; Theophilopoulos op cit note 7 at 476; De Villiers (2) op cit note 43 at 733 – 734; South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 75.
[136] For example, in *S v Van der Linde* [2016] 3 All SA 898 (GJ) where the section was referred to, but only briefly, after the parties agreed on admitting the evidence concerned. In *Sublime Technologies (Pty) Ltd v Jonker* 2010 (2) SA 522 (SCA), although it appeared central to the dispute, it was only mentioned in passing.
[137] *LA Consortium* supra note 11 para 13.
[138] 2014 (1) SA 475 (WCC).
[139] Ibid para 19.
[140] [2012] JOL 29436 (SCA) para 16.
[141] Hofman & de Jager op cit note 7 at 772 – 773.
[142] [2005] ZAGPHC 311.

> In terms of s 15(4) of [the ECT Act] a printout of a data message can constitute *prima facie* proof [of the facts contained therein] 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'.[143]

Further, in *Ndlovu*, despite the court noting that s 15 does not override the normal rules relating to hearsay,[144] it went on to describe s 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.[145]

The dictum directly above appears to suggest that s 15(4) does override the hearsay trap via a statutory exception – created if a data message is made during the ordinary course of business, and certified to be correct. If these conditions are satisfied, a printout of a data message will be rebuttable proof of the facts contained therein.

In *Trend Finance (Pty) Ltd v Commissioner for SARS*,[146] the court pointed out that a party seeking to rely on s 15(4) must show that the document 'sought to be admitted is a printout of information existing in electronic 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. This requirement (that the data must still exist in electronic form) does not appear to have received any other judicial approval.

In addition, in *Director of Public Prosecution v Modise*,[147] the court catergorised s 15(4)[148] 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.[149]

---

[143] [2005] ZAGPHC 311 6.
[144] *Ndlovu* supra note 12 at 173.
[145] *Ndlovu* supra note 12 at 172 – 173.
[146] [2005] 4 All SA 657 (C) 678-679.
[147] 2012 (1) SACR 553 (GSJ).
[148] Duvenhage op cit note 132 at 34 – 38.
[149] *Modise* supra note 147 at 557.

In *Modise*, in an application to review a Magistrate's decision, Lamont J seemed to indicate that notwithstanding some of the academic concerns pointed out above s 15(4) is an intentional step by South Africa's legislature to subjugate the hearsay rule:[150]

> [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.[151]

This exception appears to go further than previous statutory exceptions, and may favour evidence in the form of a data message if in a business context. If a person in a business is able to comply with the statutory provisions of s 15(4) – which simply require certification from an employee that the printout of a data message is correct – then those facts are rebuttably presumed true. [152]

However, the wording of s 15(4), as noted by Lamont J in *Modise* is an intentional step by the legislature to subjugate the hearsay rule. This type of 'shop-book' or business records exception, as will be seen in the discussion on foreign law in paragraph 3.6 below, is common around the world.

Be that as it may, some argue[153] this creates a reverse onus[154] that may be constitutionally suspect in criminal cases[155] – even though it is a presumption which can be challenged. However, it may be argued that the wording of s 15(4) creates an evidentiary burden – and not a full reverse onus.[156] If this is the case, in a criminal context, this may

---

[150] Duvenhage op cit note 132 at 34 – 38.
[151] *Modise* supra note 147s at 557.
[152] Hofman op cit note 24 at 268; De Villiers (2) op cit note 43 at 731; Fourie op cit note 7 at 79.
[153] Hofman op cit note 24 at 268; De Villiers (2) op cit note 43 at 771 – 772; Fourie op cit note 7 at 78 – 80.
[154] According to the Constitutional Court in *S v Zuma* 1995 (2) SA 642 (CC) para 19 a reverse onus provision is one where a 'presumption with the legal burden of rebuttal on the accused' is created. It is submitted that in a criminal case, it may be argued that section 15(4) creates a presumption with the legal burden of rebuttal on the accused in that if a print-out is certified correct, the contents are rebuttably presumed true – this ensures that if an accused would like to challenge this evidence, at the very least, her right to silence is infringed (as contained in s 35(1)(a) of the Constitution of the Republic of South Africa).
[155] Hofman op cit note 24 at 267; Fourie op cit note 7 at 79; De Villiers (2) op cit note 43 at 731; Theophilopoulos op cit note 7 at 476.
[156] Schwikkard & van der Merwe op cit note 2 at 540; Zeffertt, Paizes & Skeen op cit note 18 at 212 – 214. See also the discussion on presumptions in chapter 4.2 below, and the discussion on the onus of proof and evidentiary

infringe on the right to remain silent in that an accused is placed in a position where she will have to show that the evidence that is rebuttably presumed true is not accurate or contains some falsehood. Accordingly, as this argument goes, it is not an infringement of the presumption of innocence, but rather a potential infringement on the right to remain silent. However, whether classified as an evidentiary burden, or as a full reverse onus, in a criminal context this section appears to be susceptible to criticism in that it either infringes on the right to remain silent, or worse, infringes on the presumption of innocence, and possibly on the right to a fair trial.[157]

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 correct. Conversely, however, as pointed out above in *Modise*, there is merit in the argument that this type of section is imperative in a modern society, and an intentional departure from the Model Law, 1996.

As suggested by the SALRC, the interplay between the statutory hearsay exceptions and s 15(4) is 'complex', creates 'unnecessary confusion' and requires 'greater alignment'. [158] These proposals will be discussed in chapter 7 below.

3.7 SELECTED INTERNATIONAL POSITIONS ON HEARSAY ELECTRONIC EVIDENCE

What follows below in paragraphs 3.7.1 to 3.7.4 is a consideration of several foreign jurisdictions. This does not purport to be a comprehensive comparative study of law in these jurisdictions. It is intended as a tool for identifying suitable approaches to hearsay electronic evidence in South Africa.

3.7.1 England and Wales

In England, the primary default rule governing evidence is that all evidence sufficiently relevant to an issue before court will be admissible, and that all irrelevant evidence should be excluded.[159] This default position is subject to a number of exceptions,[160] which include

burden in para 6.2 below. See further the discussion on the constitutional consequences of a shifting evidentiary burden in para 7.3.9 below when the SALRC proposals are discussed.

[157] Section 35(3) of the Constitution of the Republic of South Africa.

[158] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 31 – 32 and 69 – 71.

[159] C Tapper *Cross & Tapper on Evidence* 12 ed (2010) 64 – 65.

[160] S Mason, C Freedman & S Patel 'England & Wales' in S Mason (ed) *Electronic Evidence* 3 ed (2012) 347.

hearsay, opinion, character, and conduct on other occasions.[161] As a result, the English law of evidence (which the South African law of evidence is based on), has been referred to as being founded on exclusionary rules, which contain two fundamental guiding principles – the best evidence rule, and the hearsay rule.[162]

Tapper notes that in so far as hearsay is concerned, it is: 'one of the most complex and most confusing of the exclusionary rules of evidence.'[163] However, more recently, England has implemented fundamental statutory reform in relation to hearsay in the form of the Civil Evidence Act 1995 (CEA) in civil proceedings, and the Criminal Justice Act 2003 (CJA) in criminal proceedings.[164]

In civil proceedings,[165] evidence is not excluded on the basis that it is hearsay. Section 1 of the CEA states as follows:

> 1 *Admissibility of hearsay evidence*
>
> (1) In civil proceedings evidence shall not be excluded on the ground that it is hearsay.
>
> (2) In this Act—
>
> (a) 'hearsay' means a statement made otherwise than by a person while giving oral evidence in the proceedings which is tendered as evidence of the matters stated; and
> (b) references to hearsay include hearsay of whatever degree.

As a result, hearsay evidence is freely admitted in civil matters. However, s 2 of the CEA provides that notice of the hearsay evidence must be given to the opposing party, and provides in s 4 factors a court should consider when deciding on the weight the hearsay evidence should receive. In addition, s 3 of the CEA allows a party to call as a witness for cross-examination, any person who has made a statement containing hearsay.

Conversely, in criminal proceedings, the CJA excludes hearsay evidence – but subject to several exceptions where hearsay evidence will be admissible.[166] As with South Africa's Law of Evidence Amendment Act, a court in England will always retain an overarching discretion as to whether hearsay evidence should be admitted in criminal proceedings[167] in

[161] Tapper op cit note 159 at 66 – 67.
[162] O Leroux 'Legal Admissibility of Electronic Evidence' *International Review of Law, Computers & Technology* (2004) 18(2) at 202.
[163] Tapper op cit note 159 at 551.
[164] Ibid.
[165] Tapper op cit note 159 ch 13.
[166] Tapper op cit note 159 at 602 – 603.
[167] For further details on the other exceptions to hearsay applicable in criminal law, see Tapper op cit note 159 ch 13.

terms of s114 1(1) (d) of the CJA,[168] which sets out an *interests of justice* considerations. Simply, if a court feels it is in the interests of justice for hearsay evidence to be admissible, it has the discretion to accept the evidence – whether electronic or otherwise.

Much like South Africa, one of the core concerns in so far as computer evidence is concerned has been in relation to the hearsay rule.[169] In England,[170] the position is the same as South Africa's – that is, if the production of data occurs without human intervention, it is real evidence (no hearsay enquiry).[171] Conversely, if the data is a record of human assertions, then it is hearsay.[172] The key, as with many jurisdictions around the world, is to determine whether the credibility of the data relies on a person, or an automated process – and this distinction often leads to 'confusion' and has acted as a 'brake' on the introduction of new technology.[173]

In terms of hearsay electronic evidence, in *O'Shea v City of Coventry Magistrates' Court*,[174] the accused was charged with offences relating to accessing child pornography – automated transactions (involving the accused's credit card and the pornography website) were regarded as real evidence, and admissible. On review, the High Court of Justice found that a 'computer printout produced exclusively by a computer without the intervention of the human mind' is real evidence. More recently, in *McDonald v R*,[175] 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).

Earlier, in *R v Minors and Harper*[176] the following statement was accepted as an explanation of 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.

[168] For a detailed analysis of this legislation, see Tapper op cit note 159 at 586 – 621, see also 551 – 581 for a discussion on hearsay in general.
[169] Mason, Freedman & Patel op cit note 160 at 363.
[170] For a review of the English position, see Tapper op cit note 159 ch 12; see also C Gallavin & S Mason 'Hearsay' in S Mason (ed) *Electronic Evidence* 3 ed (2012) paras 4.1 – 4.4.5; C Gallavin & S Mason 'Hearsay' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 72 – 86.
[171] Mason, Freedman & Patel op cit note 160 at 329; Hofman & de Jager op cit note 7 at 776 – 777.
[172] Mason, Freedman & Patel op cit note 160 at 329.
[173] C Reed 'The Admissibility and Authentication of Computer Evidence – A Confusion of issues' in *5th Annual British and Irish Legal Education Technology Association Conference* (1990) 3 – 5.
[174] [2004] EWHC 905.
[175] [2011] EWCA Crim 2933 para 42.
[176] (1989) 89 Cr App R 102.

In *R v Spiby*,[177] an automated computer process monitored telephone calls, and a print-out of certain call details was accepted as real evidence because there was no human intervention in the production of the data – accordingly, it was not hearsay evidence.[178] However, it should be noted that *Spiby* was overturned in *R v Shephard*[179] where the court found that the empowering legislation (section 69 of the Police and Criminal Evidence Act 1984) requires a party to produce evidence that will establish that the electronic evidence is reliable in the circumstances. The evidence required will vary from case-to-case.[180]

As with many other jurisdictions that rely on technology and computerised records, England has a variety of business records exceptions. Typically, these exceptions require the data to be created during the ordinary course and scope of business, and the creator of the data to have had personal knowledge thereof.[181] In England, s 117 of the CJA contains the exception in criminal proceedings, and s 9 of the CEA contains a similar exception in a civil context.

In summary, in English law, 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), depending on whether the evidence was created with human input. If 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 substantial human intervention, then the evidence will be real evidence.

3.7.2 Canada

The Canadian law of evidence is predominantly based on English common law (except in Quebec),[182] and as is the case in England and South Africa, electronic evidence is subject to the same evidentiary regime as traditional (paper) based evidence.[183] This is consistent with the United Nations 'international standard' (the Model Law, 1996), and with the principle of functional equivalence.[184]

---

[177] [1990] 91 Cr App R 186.
[178] See also *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.
[179] [1993] 1 All ER 225.
[180] Ibid.
[181] For a full discussion on these exceptions, see Tapper op cit note 159 at 610 – 613.
[182] N Boyd *Canadian Law: An Introduction* 5 ed (2011) 87 – 105.
[183] Groulx, Rothman & Zawidzki '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* at 22, accessed 25 June 2017.
[184] J Gregory 'Canadian Electronic Commerce Legislation' (2002) 17 *Banking & Finance Law Review* 276 – 277.

As a federal state, Canada has a somewhat segmented[185] jurisdictional structure. In criminal matters and federal litigation,[186] where the federal state has jurisdiction, the Canada Evidence Act 1985 finds application.[187] Conversely, in civil and property matters, jurisdiction rests with the provinces and territories, where the applicable provincial evidence statute will apply.[188]

Consequently, jurisdiction will determine whether federal or provincial law applies – however, in so far as electronic evidence is concerned, both federal and provincial evidence statutes are based on the Model Law, 1996.[189]

As is the case with most provincial statutes regulating electronic evidence, section 31.1 – 31.8 of the Canada Evidence Act 1985 contains statutory provisions regulating the authenticity of electronic documents, and contains directives on the best evidence rule in relation to data and electronic evidence.[190] These provisions deal with the admissibility of the electronic document, not the admissibility of its contents (this is regulated by some other statutory provision, or the common law).[191]

In *R v Mondor*,[192] the Ontario Court of Justice[193] confirmed that electronic evidence (much like the position in South Africa and England above) can take the form of real evidence or documentary evidence. The court found:

> 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.

[185] R Currie & S Coughlan 'Canada' in Mason S (ed) *Electronic Evidence* 2 ed (2010) 265 – 266.
[186] M Shortt 'The Applicable Rules of Evidence in Federal Court: A Short Primer on a Tricky Question' (2016) 46(2) 252 – 259.
[187] D Paciocco 'Proof and Progress: Coping with the Law of Evidence in a Technological Age' (2013) 11 *CJTL* 181 – 228.
[188] Section 40 Canada Evidence Act 1985.
[189] M Smith ' Facilitating Electronic Commerce Through the Development of Laws to Recognize Electronic Documents and Transactions' available at *http://publications.gc.ca/Collection-R/LoPBdP/BP/prb0012-e.htm* where the author notes the Uniform Electronic Evidence Act 1999 is 'a model law designed to implement the principles of the UNCITRAL Model Law on Electronic Commerce', accessed on 28 April 2019. See also L Duranti, C Rogers & A Sheppard 'Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later' (2010) 70 *Archivaria* 104.
[190] In general, for a comprehensive overview and discussion on the Canadian law of evidence, see D Paciocco & L Stuesser *The Law of Evidence* 7 ed (2015).
[191] Paciocco op cit note 187 at 193 – 194 where reference is made to the approach adopted in *R. v. Morgan* [2002] N.J. No. 15, Flynn Prov. J. (N.L. Prov. Ct.).
[192] 2014 ONCJ 135 para 17.
[193] See also G Underwood & J Penner *Electronic Evidence in Canada* (2010) 186 which the court in *R v Mondor* used as authority.

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.[194] Using similar logic to the South African decisions in *Ndlovu* and *Ndiki*, 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.

Ultimately, after analysing previous cases dealing with hearsay electronic evidence,[195] the court found the evidence to be 'inadmissible for the truth of their contents.'[196]

In *Saturley v CIBC World Markets Inc*.,[197] the Nova Scotia Supreme Court set out the position as follows (similar to what in my view is the correct position 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.[198]
>
> 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.[199]

The court went further to note that the real issue lies in deciding, 'when electronic information should be treated as real evidence, rather than documentary.'[200] Ultimately, and as with the position in England and South Africa, electronic evidence will be real evidence when its production is 'without human intervention.'[201] This position has received judicial support including in the matter of *R v McCulloch*,[202] where the admission of telephone records were introduced to court as real evidence because of the automated nature of the data.

Moreover, in *R v Hall*,[203] the court found that automated billing records were real evidence (although they also fell under the hearsay business records exception). The court

[194] Section 30 and 31 of the Canada Evidence Act, 1985
[195] *R v Mondor* supra note 192 paras 34 – 39 where previous Canadian cases dealing with hearsay electronic evidence are discussed.
[196] *R v Mondor* supra note 192 para 43.
[197] 2012 NSSC 226.
[198] Ibid para 11.
[199] Ibid para 13.
[200] Ibid para 14.
[201] Ibid para 21.
[202] [1992] B.C.J. 2282 para 18.
[203] [1998] B.C.J. No. 2515.

referred with approval to the English case of *R v Spiby*[204] where the English court found that an automated process monitoring phone calls was also real evidence (not subject to hearsay rules).

As with South Africa and England, in Canada the classification of electronic evidence (as real or documentary) will be important. It guides the admissibility enquiry, and consequently, a critical determination is to find out whether the data produced (and which a litigant seeks to rely on to prove or disprove an issue) was created with or without human intervention. Thereafter, it will be necessary to consider the empowering legislation (or common law) for the applicable admissibility requirements.

3.7.3 The United States of America

It is almost impossible to concisely summarise the legal position on any issue in the United States – primarily, because of the federal system. Each state has its own independent judiciary, and applies its own nuanced procedural and evidentiary rules.[205]

That said, holistically, the legal system of the United States is similar to South Africa and the jurisdictions discussed above in that it is a predominantly common law system based on English common law (at a federal level).[206] As a general position, the United States adopts a similar stance in relation to hearsay electronic evidence: it recognises a business records hearsay exception,[207] and distinguishes between computer-generated records (no human intervention – real evidence), and computer-stored records (human intervention – documentary hearsay).[208]

In terms of the Federal Rules of Evidence, hearsay is not admissible as evidence,[209] but this is subject to several exceptions.[210]

The basis for considering the admissibility of electronic evidence in the United States is similar to 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.[211]

---

[204] [1990] 91 Cr App R 186.
[205] J Schwerha, J Bagby & B Esler 'United States of America' in S Mason (ed) *Electronic Evidence* 3 ed (2012) para 19.03.
[206] L Friedman & G Hayden *American Law: An Introduction* (2017) 35 – 55.
[207] Schwerha, Bagby & Esler op cit note 205 at 797 – 835.
[208] D Seng & S Chakravarthi 'Computer Output as Evidence' *https://www.sal.org.sg/Portals/0/PDF%20Files/Law%20Reform/TLDG-2003-09%20-%20Computer%20Output%20as%20Evidence.pdf*, accessed on 25 June 2017.
[209] Fed. R. Evid. 802. See also, Fed. R. Evid. Article VIII – Hearsay, and sections 801 – 807.
[210] Fed. R. Evid. 803. See also, Fed. R. Evid. Article VIII – Hearsay, and sections 801 – 807.
[211] L Kemp 'Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations)' (2007) 9 *North Carolina Journal of Law & Technology* 20

The distinction between real and documentary evidence drawn in South Africa, England and Canada is similarly made 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 production is solely automated or mechanical, then it is not subject to the hearsay rules.[212]

For example, in *U-Haul Intern Inc. v Lumbermens*,[213] 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 [certain] criteria constitute an exception to the prohibition against hearsay evidence.'[214]

In *Telewizja Polska USA Inc. v Echostar Satellite Corp*,[215] 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). In addition, in *United States v Rollins*,[216] the court found that computer generated evidence (without human intervention) was admissible without requiring admissibility in terms of the hearsay rules.

In the seminal matter of *Lorraine v Markel American Insurance Company*,[217] the court delivered a comprehensive 101 page opinion outlining the admissibility of electronically stored information. The thorough opinion canvasses all relevant United States law (in so far as electronic evidence is concerned) and may well be a point of departure if United States electronic evidence is at issue.[218] In summary, the court comprehensively reviewed the applicable statutory regime for admissibility of electronic evidence (at a federal level) – and found that if evidence is primarily generated by a computer, it cannot be subject to hearsay as it is not produced by a person.[219] In the context of hearsay electronic evidence, the court found that:[220]

– 21; J Frieden & L Murray 'The Admissibility of Electronic Evidence under the Federal Rules of Evidence' (2011) 17 *Richmond Journal for Law and Technology* 2 – 6.

[212] G Joseph 'A Simplified Approach to Computer-Generated Evidence and Animations' available at *http://www.jha.com/us/articles/viewarticle.php?8*, accessed 5 June 2017.

[213] 576 F.3d 1040 (9th Cir. 2009).

[214] Ibid at 1043.

[215] 2004 WL 2367740.

[216] 2004 WL 26780.

[217] 241 F.R.D. 534.

[218] B Esler 'Lorraine v Markel: Unnecessarily Raising the Standard for Admissibility of Electronic Evidence' 2007 *Digital Evidence and Electronic Signature Law Review* 80 – 82.

[219] Similar logic was used in the South African cases of *Ex Parte Rosch* and *Narlis*.

[220] Kemp op cit note 211 at 2 – 7.

> When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the 'report' 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*,[221] 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.'[222]

Consequently, the key issue in the United States in so far as computer generated evidence and hearsay is concerned, 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, and the best evidence rule), the evidence will be admissible. Of course, as with 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).

3.7.4 Comment

In all the foreign jurisdictions considered the accepted position appears to favour electronic evidence being admissible without hearsay considerations if produced by machine or computer without substantial human intervention. However, in South African, this issue can be controversial,[223] and arguably requires law reform, or clear judicial guidance. The South African Law Reform Commission noted as follows:[224]

---

[221] 2015 WL 3772772 (9th Cir. 2015).

[222] Ibid at 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).

[223] Zeffertt & Paizes op cit note 2 at 432 – 433 where the authors disagree with the proposition that a computer can produce real evidence and rely on Bilchitz's contribution to the *Annual Survey of South Africa Law* in 1998 to support their position. In my view, although understandable, this position is not consistent with modern international practice and does not accord with the South African common law in relation to real evidence – as a result, the proposition that computers cannot produce real evidence should be rejected as appears the case with most recent case law in South Africa dealing with the issue – for example, *S v Ndiki* supra note 11; *Ndlovu* supra note 12; *LA Consortium* supra note 11.

[224] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 70.

> The SALRC supports the maintenance of a distinction between automated data messages and data messages 'made by a person' and proposes statutory reform to guide the production and proof of both types of evidence in court. In addition, the SALRC supports the development of a handbook on obtaining and producing electronic evidence that will provide clarity, to practitioners and judicial officers, on the legal position and advice on technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

The law reform proposals, and law reform recommendations, will be discussed in chapter 7 below.

3.8 CONCLUSION

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 new Cybercrimes legislation, the evidentiary position will remain unchanged by that legislation (which barring one minor procedural section, leaves the law of evidence untouched).
Consequently, 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. 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 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 s 15(4) of the ECT Act remains a cause for disagreement.

In the foreign jurisdictions considered above it appears settled law that electronic evidence that relies on a computer or automated system (such as phone records or GPS data) 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, will benefit from law reform, or clear judicial guidance.

CHAPTER 4:[1] *ELECTRONIC DEVICES – A PRESUMPTION OF RELIABILITY, A PRESUMPTION OF REGULARITY, JUDICIAL NOTICE, OR NONE OF THE ABOVE?*

4.1 INTRODUCTION

Electronic devices have become part of the fabric of every-day life – their omnipresent nature ensures that in a post information-revolution society, it is likely that a person will use, rely on, or interact with technology every day. Consequently, technological developments have ushered in a 'revolution' that requires some adaption from the law of evidence.[2]

In the context of data messages and electronic communication, a presumption of reliability is a presumption that electronic equipment was working and reliable at the relevant time, unless there is evidence to the contrary.[3] The primary rationale being expediency – to save time and money; and to avoid proving the obvious.[4]

In *Trustees for the time Being of the Delsheray Trust v ABSA Bank Limited* ('*Delsheray Trust'*),[5] the Western Cape High Court invoked what it referred to as a common law presumption of reliability in order to ensure seemingly valid computer-based evidence was admitted to court.

Consequently, the purpose of this chapter is to examine a presumption of reliability in relation to electronic evidence, paying particular attention to recent case law in South Africa in order to critically analyse whether the law reform proposed by the SALRC in the context of presumptions is necessary and/or desirable.

---

[1] A version of this chapter was published as L Swales 'Electronic instruments – a presumption of reliability, a presumption of regularity, judicial notice, or none of the above?' *SACJ* 2018 (2) 189 – 211.

[2] *Trustees for the time Being of the Delsheray Trust* v *ABSA Bank Limited* [2014] 4 All SA 748 (WCC) para 18; *S v Meyer* 2017 JDR 1728 (GJ) where the court applied the ECT Act in the context of fraudulent VAT refunds totalling over 200 million Rand; *S v Brown* 2016 (1) SACR 206 (WCC) where electronic evidence from a mobile phone and the application of the ECT Act were central issues in the context of a murder trial; *S v Miller* 2016 (1) SACR 251 (WCC) where electronic evidence was required in the context of organised crime involving abalone. See also *Uramin Incorporated v Perie* 2017 (1) SA 236 (GJ) where technology was 'simply another tool for securing effective access to justice' in the context of evidence being led via video link.

[3] *Delsheray Trust* supra note 2 at para 40 – 41. See also D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)' (2010) 4 *TSAR* 722 – 734 where a presumption is discussed in the broader context of electronic evidence; C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 477 where the author discusses courts taking judicial notice of the 'integrity and reliability of the operation of electronic hard drive systems and software programs'.

[4] S Mason 'Mechanical Instruments: the presumption of being in order' in S Mason (ed) *Electronic Evidence* 3 ed (2012) at 149. See also D van der Merwe 'Evidence' in *Law of South Africa* (2015) 18(3) para 230 and para 235; C Tapper *Cross and Tapper on Evidence* 12 ed (2010) 131.

[5] *Delsheray Trust* supra note 2 at para 41.

4.2 PRESUMPTIONS: AN OVERVIEW

A presumption is a legal device or method of reasoning.[6] It is a form of logic where conclusions may or must be drawn in the absence of contrary evidence.[7] Presumptions ultimately augment and aid reasoning in legal enquiries[8] – the primary aim being to alleviate the need to prove every item of evidence adduced in court, or to reduce the need for evidence to prove the obvious.[9]

In South Africa, presumptions are traditionally classified in three categories:[10] irrebuttable presumptions of law, rebuttable presumptions of law, and rebuttable presumptions of fact.[11]

An irrebuttable presumption of law, as the name suggests, is conclusive proof of the fact presumed and cannot be rebutted by evidence to the contrary. For example, a child under 10 years old is irrebuttably presumed to lack criminal capacity.[12] The term presumption in this context is a misnomer: an irrebuttable presumption of law applies as a rule of substantive law and not as a presumption.[13] In *Scagell v Attorney-General, Western Cape*, in the context of the constitutionality of certain statutory presumptions, the court found: 'the legal character of an irrebuttable presumption is not that it is a rule of evidence, but that it is a rule of substantive law.'[14]

Conversely, a rebuttable presumption of law provisionally accepts a fact as true; the fact will be presumed true unless there is evidence to the contrary. For example, the ownership of a thing is rebuttably presumed to be unencumbered, and free from servitudes – consequently, this 'fact' or position will operate until countervailing evidence proves the opposite.[15] In *R v Fourie*, the Appellate Division held that a rebuttable presumption 'must be accepted as proof of the fact presumed until rebutted'.[16]

---

[6] D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) 181 – 182.
[7] P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) 536.
[8] Thayer *Preliminary Treatsie of Evidence at Common Law* (1898) in Schwikkard & van der Merwe op cit note 7 at 537. See also D Zeffertt & A Paizes *The South African Law of Evidence* 3 ed (2017) 191 – 197.
[9] S Mason 'The Presumption that Computers are reliable' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 101.
[10] Schwikkard & van der Merwe op cit note 7 at 536; Zeffertt & Paizes op cit note 6 at 181.
[11] *Tregea v Godart* 1939 AD 16 at 28 where the court notes: '…presumptions in all the text books are commonly said to be of three kinds, viz., (1) *Presumptiones juris et de jure*, (2) *Presumptiones juris* and (3) *Presumptiones hominis*' in D Zeffertt & A Paizes *Essential Evidence* (2010) at 55 – 57.
[12] This legal position is comprehensively regulated by statute – see section 7 of Child Justice Act 75 of 2008.
[13] Schwikkard & van der Merwe op cit note 7 at 538.
[14] *Scagell v Attorney-General, Western Cape* 1997 (2) SA 368 para 30.
[15] C van der Merwe 'Servitudes' in *Law of South Africa* (2010) 24 para 543.
[16] 1937 AD 31 at 44 in Schwikkard & van der Merwe op cit note 7 at 538. See also Zeffertt & Paizes op cit note 6 at 183 where the authors in addition refer to *S v Steyn* 1963 (1) SA 797 (W).

Finally, a rebuttable presumption of fact is a provisional inference that must be drawn based on probabilities, ordinary use, and common-sense; ultimately, it is a presumption based on what one would usually expect to happen in similar situations.[17] For example, if an automated computer process that produces telephone records is usually reliable, and its results are normally credible, then a rebuttable presumption of fact may well presume the mechanical process that produces telephone records to be working at the relevant time until contrary evidence is produced.

4.3 PRESUMPTIONS OF FACT

A presumption of fact is often likened to circumstantial evidence[18] and inferential reasoning,[19] and has been described as:

> merely frequently recurring examples of circumstantial evidence;[20]
>
> an inference of probability which a court may draw if on all the evidence it appears to be appropriate;[21]
>
> really only another way of indicating that the specific circumstances of the case are such that inferential reasoning is permissible.[22]

In *R v Fourie*[23] the Appellate Division described a rebuttable presumption of fact as follows: '[It] is the Judge's own; an inference which he draws from the established premises'. As a result, some writers have noted that it is misleading to refer to ordinary reasoning and common sense as presumptions.[24] In the context of electronic evidence, others have noted that a presumption of fact that all computers were working at the material time is too crude to be applied to modern technology, and too vague.[25]

As Mason points out,[26] by way of analogy, the presumption that all computers (or technology) is working would be similar to suggesting all motor vehicles, regardless of quality

---

[17] Zeffertt & Paizes op cit note 6 at 182; Schwikkard & van der Merwe op cit note 7 at 538; van der Merwe op cit note 4 para 230 and 235.
[18] A Paizes 'The law of evidence: Seven wishes for the next twenty years' (2014) 3 *SACJ* 280 – 282; Zeffertt & Paizes op cit note 6 at 23 – 24.
[19] *R v Blom* 1939 AD 188 at 202–203 and the *two cardinal rules of logic* espoused by Watermeyer JA. Zeffertt & Paizes op cit note 6 at 99 – 100; Schwikkard & van der Merwe op cit note 7 at 538 – 539. In so far as the *cardinal rules of logic* are concerned, see Piazes op cit note 18 at 280 – 282.
[20] Schwikkard & van der Merwe op cit note 7 at 579.
[21] Zeffertt & Paizes op cit note 6 at 182 – 184.
[22] Schwikkard & van der Merwe op cit note 7 at 579.
[23] 1937 AD 31 at 44.
[24] Schwikkard & van der Merwe op cit note 7 at 539.
[25] Mason op cit note 9 at 176; Mason op cit note 4 at 177 – 181.
[26] Mason op cit note 9 at 175 – 176.

and/or age and/or other surrounding factors are reliable – this type of presumption would be absurd. Accordingly, as argued by Mason, a presumption that all computers are presumed to be working at the relevant time requires a re-think, or at the very least a court should be satisfied that the surrounding factors suggest the presumption ought to be applied in the circumstances.

In *Arthur v Bezuidenhout and Mieny*,[27] a South African court referred with approval to the seminal United States academic text on evidence by Wigmore[28] where it was stated: the term 'presumption of fact' should be discarded as useless and confusing. Earlier, in *R v Fourie*,[29] in a South African context the Appellate Division noted:

> Presumptions of fact are as numerous as the facts on which they are founded, they cannot be catalogued and ought not, in my view, to find a place in a legal treatise, for the simple reason that being so individual and varied no generalisation can be made in respect of them.

Consequently, in the context of electronic evidence, given that presumptions of fact are little more than 'ordinary inferences drawn by the courts from the facts presented to them',[30] a party to criminal or civil proceedings would need to satisfy a court that the appropriate inference, in the particular circumstances, would be to infer that the electronic process was reliable at the relevant time – or, as the case may be, not reliable at the relevant time. For example, if bank records were required to prove some unlawful transaction, and in the event a common law presumption was relevant: a commercial bank, particularly those with many different branches and international locations should easily be able to satisfy a court that computer systems it used at a point in time relevant to an evidentiary dispute were of the appropriate industry standards, and usually reliable. If this is found to be the case, it is likely a court will by relying on this circumstantial evidence (and adopt inferential reasoning) to conclude that the relevant computer process was reliable at the applicable time, unless there is evidence to the contrary.[31]

---

[27] 1962 (2) SA 566 (A) 574 in Schwikkard & van der Merwe op cit note 7 at 539. See also Zeffertt & Paizes op cit note 6 at 183.
[28] J Wigmore *A treatise on the system of evidence in trials at common law* 3 ed (1940).
[29] 1937 AD 31 at 44.
[30] van der Merwe op cit note 4 para 236.
[31] *Delsheray Trust* supra supra note 2 at para 43 where the court invoked what it called a presumption of reliability (akin to a presumption of fact) and found that as ABSA was a 'large commercial bank with branches all over the country. It can safely be assumed that its computer system is as sophisticated, efficient and reliable as those of financial institutions competing with it', and that 'it can also be assumed that respondent would employ the personnel (or outside contractors) with the experience, expertise and responsibility which the proper operation of such a computer system would require.' The court therefore, via inferential reasoning and circumstantial evidence drew this presumption of fact which it referred to as a presumption of reliability. It further found, at para 37, that 'this presumption is not generally applied in the South African case law under that name but the underlying

4.4 DOCTRINE OF JUDICIAL NOTICE

The doctrine of judicial notice allows a judicial officer to accept a fact as true (take notice of a fact) if the court, in the circumstances, regards that fact as established[32] and true[33] without the need for any evidence. The rationale for judicial notice is based on expediency and consistency – much like the presumptions discussed above. Once a court has taken judicial notice of a fact, it will then be accepted into evidence without any evidence necessary to prove the point.[34] These facts are 'well known to all reasonable persons or to a reasonable court in a specific location.'[35]

Judicial notice is said to be taken of four types of facts.[36] First, facts that are so notorious as to be known by all reasonable persons[37] – for example, that Durban is in KwaZulu-Natal, or that Cape Town in early 2018 was in severe drought. Second, facts which are objectively speaking, capable of being verified by an outside source[38] – for example, the prime lending rate in South Africa on 25 February 2010. Third, facts relating to published law and related legal matters, for example, judicial notice will be taken of any South African statute, as well as the common law. Fourth, legal commentators[39] have created a further category of facts a court will take notice of when dealing with constitutional matters – for example, a court can take judicial notice of apartheid in South Africa and the socio-economic conditions that followed such a system.[40]

In the Appellate Division case of *S v Mthimkulu*,[41] (later endorsed in *S v Fuhri*),[42] in the context of taking judicial notice of the trustworthiness of a scale measurement, the court held that expert evidence as to the trustworthiness of a process may not always be required and stated: 'expert evidence as to the trustworthiness of the process may be obviated by the doctrine of judicial notice.'[43] The court further noted: 'judicial notice is similarly taken of

---

principles, we suggest, are indeed established…' Although this case is civil in nature, the court's rationale is based on an Appellate Division criminal matter discussed below – *S v Mthimkulu* 1975 (4) SA 759 (A).

[32] Zeffertt & Paizes op cit note 6 at 865 – 866; Zeffertt and Paizes op cit note 11 at 278.

[33] Schwikkard & van der Merwe op cit note 6 at 515 – 516.

[34] Zeffertt & Paizes op cit note 6 at 865 – 866; Zeffertt and Paizes op cit note 11 at 278.

[35] Schwikkard & van der Merwe op cit note 7 at 518.

[36] Zeffertt & Paizes op cit note 11 at 277 – 281 where the authors suggest there are four categories. See also Zeffertt & Paizes op cit note 6 at 865 – 881 and Schwikkard & van der Merwe op cit note 7 at 515 – 530.

[37] Zeffertt & Paizes op cit note 6 at 865 – 866; Schwikkard & van der Merwe op cit note 7 at 515 – 518.

[38] Ibid.

[39] Zeffertt & Paizes op cit note 11 at 277 – 281; Zeffertt & Paizes op cit note 6 at 865 – 866; Schwikkard & van der Merwe op cit note 7 at 515 – 530.

[40] Ibid.

[41] *S v Mthimkulu* 1975 (4) SA 759 (A) (*Mthimkulu*).

[42] 1994 (2) SACR 829 (A).

[43] *Mthimkulu* supra note 41 at 764.

other scientific instruments or processes, such as tape-recording, telephony and ordinary photography.'[44] Corbett JA relied on John Henry Wigmore[45] to justify this finding, and found as follows:

> in order to justify testimony based on [electronic] instruments…: Preliminary professional testimony (1) to the trustworthiness of the process or instrument in general (when not otherwise settled by judicial notice); (2) to the correctness of the particular instrument, such testimony being usually available from one and the same qualified person. Any process or instrument, furnishing abnormal aid to the senses, may thus be employed as a source of testimonial knowledge.[46]

As recently noted in the Western Cape High Court in *S v Helm*:[47]

> Corbett JA referred to the third edition of Wigmore on Evidence and held that, in order to justify testimony based on scientific instruments or processes, professional testimony is required as to the trustworthiness of the process, or to the instrument, and, in addition, to the correctness of the particular instrument. Recognising that the doctrine of judicial notice may suffice in certain cases as to the trustworthiness of the process, the learned Judge of Appeal considered the circumstances in which a court will insist upon, or relax, the standards of proof which apply when assessing evidence involving the use of scientific instruments. These will include the nature of the process and instrument involved in the particular case, the extent, if any, to which the evidence is challenged, the nature of the inquiry and the facta probanda in the case. But at the end of the day the learned judge of appeal reminds us that there is no hard and fast rule and that much I will depend on the facts of each case.

Moreover, in *S v Fuhri*,[48] the court held that where a relevant science advances to a level of general acceptance, it is not necessary for further evidence and human verification, and a court can take judicial notice thereof. Consequently, much will depend on the facts of the matter, and the scientific or electronic process involved as to whether judicial notice is appropriate in the circumstances.

4.5 *TRUSTEES FOR THE TIME BEING OF THE DELSHERAY TRUST V ABSA BANK LIMITED*: ADMISSIBILITY AND ADEQUACY OF VERIFYING AFFIDAVITS, COMPUTER GENERATED EVIDENCE, AND PRESUMPTIONS OF RELIABILITY

In *Delsheray Trust*,[49] the Western Cape High Court relied on a common law presumption of reliability (based on the rationale in *Mthimkulu*) to accept electronic evidence. Curiously, instead of relying on the provisions of s 15 of the ECT Act, which provides expressly for data message evidence, ABSA chose to rely on the common law in arguing that its electronic

[44] Ibid.
[45] Wigmore op cit note 28 at 189 – 190.
[46] *Mthimkulu* supra note 41 at 764.
[47] 2015 (1) SACR 550 (WCC) para 104.
[48] *S v Fuhri* supra note 42.
[49] *Delsheray Trust* supra note 2.

evidence was admissible.[50] As a result of ABSA's approach, the court sat on the horns of a dilemma as it was forced to use South African common law to ensure apparently valid electronic evidence was admissible.[51]

4.5.1 Delsheray Trust v ABSA

ABSA, a large commercial bank, instituted action against the trustees of the Delsheray Trust for payment of R1 588 208,85 plus interest as a result of the trust's breach of a loan agreement in which the bank lent and advanced three separate amounts totalling R1 700 000.00. To secure this debt, ABSA held three mortgage bonds over an immoveable property owned by the trust. Consequently, in addition to the claim for payment of R1 588 208,85, ABSA sought an order declaring the mortgaged property specially executable.[52]

In response to ABSA's summons, the trust filed a notice of intention to defend – almost predictably in modern litigation of this nature, the response to the notice of intention to defend was an application for summary judgment. In terms of Rule 32(2) of the Uniform Rules of Court,[53] in summary judgment proceedings, the applicant must file an affidavit verifying the cause of action, amount claimed, and further stating that in the deponent's opinion there is no bona fide defence to the action. Although not directly stated in the rule itself, these allegations must also be made by a person with personal knowledge.[54]

An ABSA employee deposed to an affidavit as required in terms of Rule 32(2), and duly confirmed the cause of action and appropriate details. In response the Delsheray Trust claimed that the affidavit did not comply with Rule 32(2) in that the deponent did not have personal knowledge of the facts therein. Essentially, the Delsheray Trust claimed that an ABSA employee relied on computer data and records of ABSA, and not on his own direct personal knowledge.[55] This procedural interpretation notwithstanding, the court a quo (a single

---

[50] Para 17 where the court noted this, and confirmed that section 3 of the ECT Act does not exclude the operation of common law.
[51] Various recent cases (reported in the last 2 years) discuss s 15 of the ECT Act and the admissibility of data messages – see for example, *S v Meyer* supra note 2; *S v Miller* supra note 2; *S v Brown* supra note 2.
[52] *Delsheray Trust* supra note 2 para 2 – 8. For more on declaring immoveable property specially executable, see *Nedbank v Fraser* 2011 (4) SA 363 GSJ and J*aftha v Schoeman and Van Rooyen v Stoltz* 2005 (2) SA 140 (CC).
[53] Rules regulating the conduct of the proceedings of the several provincial and local divisions of the Supreme Court of South Africa in terms of the Supreme Court Act 59 of 1959, hereafter referred to as the 'Uniform Rules of Court'.
[54] *Maharaj v Barclays National Bank Ltd* 1976 (1) SA 418 (A) as the *locus classicus*, and the more recent *Rees v Investec Bank Limited* 2014 (4) SA 220 (SCA). Summary judgment is said to be extraordinary and drastic: the affidavit in support thereof must be made by someone with personal knowledge of the facts.
[55] Para 10.

judge in the Western Cape High Court) nevertheless granted summary judgment against the appellants.[56]

4.5.2 Central issue in Delsheray Trust

The appeal, heard before three judges in the Western Cape Division of the High Court, was concerned with the admissibility and adequacy of ABSA's verifying affidavit which was based exclusively on its computerised records.[57] Specifically, the central issue was: whether an affidavit, in terms of Rule 32(2) of the Uniform Rules of Court, can be validly executed where the deponent's knowledge is based exclusively on computerised data.[58] For the reasons to be discussed below, the appeal court sensibly decided in the affirmative, namely, that a deponent can rely *exclusively* on electronic data and validly declare that the information is within his or her personal knowledge.

4.5.3 Decision of the court in Delsheray Trust

The court noted that electronic evidence is regulated by the ECT Act,[59] but that s 3 (interpretation) of the ECT Act expressly provides that its application should not exclude the common law. Given that ABSA presented and argued its case on common law principles, the court considered the admissibility and adequacy of the verifying affidavit in terms thereof.[60]

If it had elected to do so, the court could have also validly applied the ECT Act by relying on s 4 of the ECT Act (sphere of application) read together with s 15 (admissibility and evidential weight of data messages). Section 4 states that, subject to its internal limitations,[61] the Act applies 'in respect of any electronic transaction or data message.'[62]

---

[56] Para 11.
[57] Para 1.
[58] Para 16.
[59] Para 17.
[60] Para 17.
[61] Primarily aimed at ensuring certain acts cannot be performed via data message, such as the execution of a will or the sale of immovable property. See sch 1 and sch 2 read together with s 4 (1) of the ECT Act.
[62] *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA) para 16.

4.5.4 Admissibility and adequacy of a verifying affidavit in terms of Rule 32(2) of the Uniform Rules of Court

The court faced a dilemma in that there are a string of high court judgments which suggest that a deponent to a verifying affidavit cannot rely exclusively on a perusal of records and documents. For example, in *Shackleton Credit Management (Pty) Ltd v Microzone Trading 88 CC,*[63] Wallis J noted that:

> I do not understand any of the cases as going so far as to say that the deponent to an affidavit in support of an application for summary judgment can have no personal knowledge whatsoever of the facts giving rise to the claim and rely exclusively on the perusal of records and documents in order to verify the cause of action and the facts giving rise to it.

This position, which requires a deponent to have personal knowledge beyond a perusal of electronic records and documents was endorsed in*, inter alia*, the Western Cape High Court in *ABSA Bank Limited v Le Roux*,[64] and *Standard Bank of South Africa v Han-Rit Boerdery CC*[65] in the North Gauteng High Court. In the latter case, the court was constrained by the generic affidavits presented to it – standard-form precedent which is often ill-suited to the facts and applicable law.[66] The court pointed out that 'difficulties arise only where plaintiffs attempt to bend the rules and take short cuts' – the court further noted that the summary judgment rules are 'straightforward and can easily be complied with'.[67]

Further, in *ABSA Bank Limited v Smith*[68] the court found that a verifying affidavit did not comply with Rule 32(2) and labelled the affidavit deficient and unreliable.[69] In *ABSA Bank Limited v Le Roux*[70] the court found that the affidavit in support of summary judgment fell

---

[63] 2010 (5) SA 112 (KZP).
[64] 2014 (1) SA 475 (WCC).
[65] [2011] ZAGPPHC 120.
[66] From a reading of the cases discussed in this paragraph 4.5.4, and from my own personal experience as an attorney of the High Court of South Africa (practicing in Gauteng and KwaZulu-Natal), typically, many colleagues who litigate for credit providers and similar clients collecting debt do so on large volume, and will usually rely on standard-form, generic precedent; and snappy, apparently clever automated systems. Usually, this results in an end-product which is not entirely suitable. These colleagues are typically pitted against one another, and under significant pressure – financially and from the credit provider client – and will consequently rely on standard pleadings, notices and strategies when colleting debts on seemingly similar matters, all in the name of cost-savings and efficiencies. In addition, at times, there appears to be a lack of appreciation for certain provisions in the ECT Act. The end-result in matters of this ilk is that one often finds that the documents are unreliable and/or vague.
[67] See also *ABSA Bank Limited v Le Roux* 2014 (1) SA 475 (WCC) para 20 where in my view the court correctly points out that a plaintiff can rely on the provisions of s 15(4) of the ECT Act in the affidavit supporting summary judgment.
[68] [2016] ZAWCHC 147.
[69] Ibid para 15.
[70] *ABSA Bank Limited v Le Roux* supra note 67.

'materially short' of Rule 32(2). In *ABSA Bank Limited v Future Indefinite lnvestments 201 (Pty) Ltd*,[71] the court noted several 'generic references', which required 'educated guesswork', and found the affidavit was entirely 'unsatisfactory'.[72] Finally, in *Delsheray Trust*, the court found that the verifying affidavit of ABSA's representative was 'not a model of clarity'.[73]

Be that as it may, it is worth pointing out that in the cases above where summary judgment was refused, the courts noted the age-old summary judgment rationale set out by Corbett JA in the Appellate Division in *Maharaj v Barclays National Bank Limited*: summary judgment proceedings are inherently extraordinary – and should only succeed where the claim is valid, and where the defendant has no defence thereto, particularly because summary judgment deprives a defendant of the opportunity to raise his or her defence in trial proceedings.

The judgments in *Shackleton, Le Roux, Han-Rit Boerdery CC* and others notwithstanding, the three judges in *Delsheray Trust v ABSA* found that a deponent to a verifying affidavit can rely exclusively on records and data; the court noted: *'We do not, with respect, agree with the approach adopted in these high court judgments'* (referring to *Shackleton* and the line of cases which support that approach). The court further held that on a proper interpretation of Corbett JA's seminal decision in *Maharaj*, a bank manager or person in a similar position is not expected to have personal knowledge of every fact, and is expected to rely on records – the court held:

> We believe that our approach herein is not inconsistent with the principles applied in [Maharaj]. Corbett JA accepted, for pragmatic reasons, that the manager of the branch of the respondent bank who deposed to the verifying affidavit could not have been expected to have personal knowledge of every entry in the client's statement of account. He 'must rely upon the bank records which show the amounts paid into his account and the amounts withdrawn by the client'.[74]

In *Delsheray Trust v ABSA* it was ultimately held that an exclusive review of computer generated information was perfectly acceptable – and found it was: 'sufficient to allow [the ABSA employee] to depose to a valid and adequate verifying affidavit'.

In addition, two recent Supreme Court of Appeal decisions also deal the with the adequacy of verifying affidavits in terms of Rule 32(2), namely: *Rees v Investec Bank*

[71] [2016] ZAWCHC 118. See also *ABSA Bank Ltd v Expectra 423 (Pty) Ltd* 2017 (1) SA 81 (WCC) para 19 – 28.
[72] *ABSA Bank Limited v Future Indefinite lnvestments 201 (Pty) Ltd* supra note 71 para 18.
[73] *Delsheray Trust* supra note 2 para 14.
[74] Ibid para 52.

Ltd,[75] and *Stamford Sales & Distribution (Pty) Limited v Metraclark (Pty) Limited*.[76] In both instances, the affidavits supporting summary judgment were found to be valid. However, as pointed out in *Delsheray Trust v ABSA*, neither of these cases dealt with deponents exclusively relying on knowledge of computerised records.

However, the Supreme Court of Appeal in *Rees* noted with approval the following logic from *Maharaj*: 'undue formalism in procedural matters is always to be eschewed', and confirmed that personal knowledge of every fact is not required (particularly for a corporate plaintiff), and finally, confirmed that a deponent averring facts obtained in the ordinary course of his or her duties as an employee of a bank is valid, and in compliance with Rule 32(2).[77]

Consequently, reading the Supreme Court of Appeal decisions together with *Delsheray Trust v ABSA*, as some practicing attorneys have pointed out,[78] the requirements of Rule 32 (and the rationale laid out by Corbett JA in *Maharaj*) can be easily met if an employee of a bank (or similar corporate entity) properly pleads its case by: a) setting out the data and information relied upon by the plaintiff's employee obtained while in the ordinary course of duty; and b) swearing positively to the facts contained therein.

In order to properly swear positively to the facts contained in the affidavit, generic precedent must be avoided, and each case should be properly drafted according to its facts – this will allow the court to deduce whether the deponent is able to validly hold the opinion that the defendant has no *bona fide* defence to the action, and that the notice of intention to defend was solely filed for purposes of delay. This type of verifying affidavit must hold enough detail and fact for a court to validly preclude a defendant from raising his or her defence in trial proceedings – and enable the court to do this without having to presume or guess.

Moreover, and crucially when acting on behalf of a corporate entity, as pointed out by Binns-Ward J in *ABSA Bank Limited v Le Roux*,[79] a deponent should also comply with the requirements of s 15(4) of the ECT Act.[80] Section 15(4) provides an exception to the hearsay rule for data messages created in the ordinary course and scope of business, and creates a rebuttable presumption that the information contained in a data message is accurate. The

---

[75] 2014 (4) SA 220 (SCA).
[76] [2014] ZASCA 79.
[77] *Rees v Investec Bank Ltd* supra note 75 para 10.
[78] N Van Vuuren 'Summary Judgment Proceedings' *Without Prejudice* July 2014 at 24 – 25.
[79] 2014 (1) SA 475 (WCC) para 19.
[80] *Trend Finance (Pty) Ltd v Commissioner for SARS* [2005] 4 All SA 657 (C); *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 4 SA 577 (GSJ); *S v Van der Linde* [2016] 3 All SA 898 (GJ). See also, J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 267 – 268; J Hofman & J de Jager 'South Africa' in Mason (ed) *Electronic Evidence* 3 ed (2012) 766 - 767; Theophilopoulos op cit note 3 at 476 – 477.

section has been described as 'controversial',[81] and is discussed in detail in chapter 3 above.[82] Consequently, according to Binns-Ward J in *ABSA Bank Limited v Le Roux*:

> the deponent to a supporting affidavit in summary judgment proceedings [should] aver that he is (i) an officer in the service of the plaintiff, (ii) that the salient facts - which should be particularised - are electronically captured and stored in the plaintiff's records (iii) that he had regard thereto (iv) that he is authorised to certify and has executed a certificate certifying the facts contained in such record to be correct and (v) on the basis thereof is able to swear positively that the plaintiff will - having regard to the provisions of s 15(4) of Act 25 of 2002 - be able to prove the relevant facts at the trial of the action by producing the electronic record or an extract thereof, the requirements of rule 32(2) would be satisfied.

Ultimately, a plaintiff in summary judgment proceedings must avoid generic, standard-form precedent – and legal practitioners should ensure that the facts are carefully considered, and the appropriate averments made in order to comply with Rule 32(2) of the Uniform Rules of Court, read together with s 15(4) of the ECT Act.[83]

4.5.5 Computer generated evidence according to Delsheray Trust v ABSA

In coming to its decision in *Delsheray Trust v ABSA*, the court provided the judgment with context by confirming that:

> [i]t is well known that modern technological developments have brought about a revolution in the way that information, including legal information, is captured and disseminated. These developments brought about substantial changes in the law of computer generated evidence, internationally and in South Africa.

Further, the court quoted with approval the celebrated English case of *R v Minors, R v Harper*:[84]

> The Law of Evidence must be adapted to the realities of contemporary business practise. Main frame computers, mini computers play a pervasive role. Often the only record of a transaction which nobody can be expected to remember, will be in the memory of a computer. In versatility, power and frequency of use of computers will increase. If computer output cannot relatively readily be used as evidence in criminal cases, much crime and notably offences of dishonesty will in practice be immune from prosecution.

[81] *LA Consortium* supra note 80 para 12.
[82] See chapter 3.5.4 above.
[83] Section 15 (4) is beyond the scope of this chapter, for a more in-depth analysis, see chapter 3 above.
[84] [1989] 2 All ER 208.

In addition, the court quoted with approval English barrister and author Mason,[85] who sets out three categories of electronic evidence: 1) data written by one or more people – will be necessary to demonstrate that content is reliable and can be trusted; 2) data generated automatically by a computer (data logs, GPS, ATM transactions) – will be necessary to demonstrate that the computer program that generated the record was reliable and can be trusted; and 3) data comprising a mix of 1) and 2) above.

Essentially, this analysis distinguishes real evidence from documentary evidence and assists a court with the classification of evidence. The court found that the relevant evidence fell into Mason's third category – a combination of human input and mechanical automation. Further, the court identified that in the first phase of the evidence's generation – where a human inputs data and/or captures transactions – the evidence would be classified as hearsay, but that these problems can be overcome by statutory exceptions.[86] In the second phase – automated generation of data by a computer process – the evidence, the court found, can be admitted on the basis of a common law presumption of reliability to the effect that: in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time.[87]

4.5.6 Presumption of reliability

The court held that 'a presumption [of reliability] is not generally applied in the South African case law … but the underlying principles … are indeed established'. In supporting this view, the court referred to another judgment by Corbett JA – *S v Mthimkulu,*[88] where it was held that expert evidence may in certain circumstances be obviated by the doctrine of judicial notice. Further, the court referred to the pre-ECT Act matter of *Ex parte Rosch*[89] where it was held that:

> Many gadgets have been invented which are capable of automatically recording material facts without human agency. Courts in this country as well as England have recognised that evidence produced by such gadgets is prima facie accurate. This accords with reality and common experience…

[85] S Mason 'Electronic Evidence, The Presumption of Reliability and Hearsay – a Proposal' *Criminal Law & Justice Weekly* 28 September 2013. See also Mason op cit note 9 for a more comprehensive overview of this legal position by the same author at 101 – 120. In general, for a South African perspective on electronic evidence see Hofman & de Jager op cit note 80 at 761 – 797.
[86] Section 15 (4) of the ECT Act; s 3 of the Law of Evidence Amendment Act 45 of 1988; s 221 of the Criminal Procedure Act and s 34 of the Civil Proceedings Evidence Act 25 of 1965.
[87] *Delsheray Trust* supra note 2 para 37 – 43; para 49 – 51.
[88] 1975 (4) SA 759 (A).
[89] [1998] 1 All SA 319 (W).

In addition, the court referred to the Supreme Court of Appeal's decision in *S v Fuhri*[90] where the SCA, approving the Appellate Division matter of *Mthimkulu*, accepted as admissible photographs produced by a machine and the information contained in such photographs (including the digital time report). Importantly however, the court found its primary justification in *S v Mthimkulu*, where Corbett JA listed factors which may influence a court to relax the strict standards of proof as follows:

> (a) the nature of the process and instrument involved in the particular case;
>
> (b) the extent, if any, to which the evidence is challenged; and
>
> (c) the nature of the enquiry and the facta probanda in the case.
>
> No hard and fast rule can, or should, be laid down. Much will depend upon the facts and circumstances of each individual matter.

After applying the applicable factors, the full bench of the Western Cape High Court in *Delsheray Trust v ABSA* ultimately concluded that in the particular circumstances, the application of a presumption of reliability could be supported – primarily, because of ABSA's stature as a large commercial bank (i.e.: sophisticated systems and experienced, qualified staff). The court further noted that this type of common law presumption overlaps with a presumption of regularity – and can be relied upon as an alternative solution when admitting electronic evidence.[91] The court quoted with approval a passage from Zeffertt and Paizes:[92]

> The scope of the presumption of regularity, usually expressed in the maxim omnia praesumuntur rite esse acta, is very ill-defined . . . In some cases it appears to be no more than an ordinary inference, based upon the assumption that what regularly happens is likely to have happened again. In other cases it is treated as a presumption of law, sometimes placing an onus upon the opposing party and sometimes creating only a duty to adduce contrary evidence. It has been applied in a wide variety of cases which are impossible to catalogue exhaustively.

Ultimately, the court concluded as follows: 'There is clearly a significant degree of overlap between this presumption and the presumption of reliability… [I]t seems to us therefore that the arguments in favour of the application of the presumption of reliability in this case… applies mutatis mutandis to the application of the presumption of regularity.'

---

[90] *S v Fuhri* supra note 42. See also *Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W); *S v Ndiki* 2008 (2) SACR 252 (CK); *LA Consortium* supra note 80.
[91] Where the court refers to Zeffertt & Paizes op cit note 6 at 212.
[92] Ibid.

Consequently, it appears that in the context of electronic evidence, whether this type of common law presumption is referred to as a *presumption of reliability* or a *presumption of regularity* is important only for academic debate and conceptual clarity – ultimately, both incarnations of the presumption create a method for the same outcome: to receive evidence when applying the common law. However, in my view, should a court elect to do so, it can receive any data message evidence directly in terms of s 15 of the ECT Act without having to consider presumptions and/or judicial notice.[93]

4.6 DISCUSSION

4.6.1 Concerns about a presumption of reliability and South African Law Reform

Is this presumption too crude to apply to modern technology? Mason, widely quoted by the court in *Delsheray Trust v ABSA* in reaching its decision, is of the view that this type of presumption is too vague to be implemented as a default position with electronic evidence, and that it should be reconsidered.[94] His reasons are as follows:

> There is no authoritative guidance in relation to the meaning of the words 'reliable', 'in order', 'accurate', 'properly set or calibrated' or 'working properly' as variously used by judicial authorities, and the language used in legislation in the context of digital data.
>
> The Presumption of Reliability is difficult to rebut. The party contesting the presumption will rarely be in a position to offer substantial evidence to substantiate any challenge, because the party facing the challenge will generally be in full control of the computer or computer systems that are the subject of the challenge, although that is not always the case, given the promotion of cloud computing and recourse to sub-contracting on a significant scale.
>
> A fundamental problem is caused by the fact the software errors can be present (in large numbers), but not observable in use until a specific situation is encountered.
>
> The term 'computers' is used solely to reinforce the point that a computer or computer-like device is far more sophisticated than any pure mechanical machine, and such devices only work because a human being has written code to allow it to function.

In the most recent law reform commission paper dealing with electronic evidence,[95] which is pending before the responsible Minister, issue 10 deals directly with a presumption of regularity. The key issue is phrased as follows:

---

[93] *Ndlovu v Minister of Correctional Services* supra note 90 at 172 – 173; *S v Ndiki* supra note 90 at para 20 – 21; *S v Brown* supra note 2 at para 18; *S v Meyer* supra note 2 at para 298.
[94] Mason op cit note 5 at 179 – 183; Mason op cit note 9 at 173.
[95] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) Issue 10: A Presumption of Regularity 78 – 80.

> Should the law of evidence prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breath-testing devices)?

The LSSA favours a presumption of regularity, provided it does not affect the onus of proof, by stating:

> such a presumption should be included in the law of evidence [and] … such a presumption would be a factual presumption and will not affect the onus of proof
>
> To expect the prosecution to prove the workings or functioning of a computer, especially in circumstances where such function is not challenged by the accused, would place an unnecessary and time consuming burden on the prosecution

Conversely, Legal Aid South Africa[96] suggests the presumption should not find application. It alludes to the fact that this presumption may place an unconstitutional evidential burden on the accused by stating:

> It would have the effect of placing at the very least an evidential burden on an accused person who would normally not have the resources to meaningfully rebut as it would involve the leading of expert evidence.

The NPA adopts a more pragmatic approach by stating:

> It would be prudent to lay a sufficient factual basis for reliability and then to apply this ... presumption ... to prove that the evidence in the instant case is reliable.

Further, Mason wrote to the SALRC to note his published concerns[97] – ultimately, he argued that this type of presumption fails to take into account the complex nature of electronic evidence. However, the SALRC proposes to introduce a presumption *in civil proceedings only*, by stating:[98]

> the SALRC proposes rather to introduce (in clause 6.4) a presumption in civil proceedings only, if and when, upon receiving notice of an intention to produce documentary evidence, no objection is raised by the party against whom such evidence is intended to be produced. The presumption is that "the nature, origin, and contents of the document are as shown on its face" and places an evidential burden on the other party to show evidence to the contrary.

The proposed law reform reads as follows:

---

[96] Legal Aid South Africa is a non-profit organisation established by the Legal Aid South Africa Act 39 of 2014 with its primary aim being to 'give legal aid or to make legal aid available to indigent persons within its financial means.'

[97] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 78.

[98] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 79.

> 6.4 In any civil proceedings, where the notice in terms of subsection (1) relates to documentary evidence, and no party objects to the notice in terms of subsection (1), or if the court dismisses an objection on the ground that no useful purpose would be served by requiring the party concerned to call a witness to produce the documents, –
>
> (a) the document, if otherwise admissible, may be admitted in evidence; and
>
> (b) it will be presumed, in the absence of evidence to the contrary, that the nature, origin, and contents of the document are as shown on its face.

Arguably, this type of statutory presumption may not fully take into account the complex nature of electronic evidence.[99] These concerns notwithstanding, the SALRC noted that a presumption of *integrity* is present in Canadian law,[100] as well as in Australian law[101] – as well as in Article 7 of the draft United Nations Electronic Evidence Model Law.[102]

Typically, a party seeking to rely on a presumption of integrity must establish that the computer system was operating properly, or that the electronic document was recorded or stored in the usual and ordinary course of business.[103]

It appears that integrity and reliability substantially deal with the same concept. In the context of data messages, the SALRC use the terms reliability and integrity interchangeably.[104] Reliable appears to be synonymous with integrity of data.[105] Furthermore, the SALRC refer to this presumption as a presumption of *regularity* (as opposed to the court in *Delsheray Trust*, where the presumption was referred to as a presumption of *reliability*). There is no substantial difference between the two presumptions, both presumptions are vehicles to achieve the same result in the context of data messages.[106]

Ultimately, the SALRC recommends the introduction of a statutory presumption only in civil proceedings – referred to as a *limited* presumption, placing an evidential burden on a

---

[99] Mason op cit note 5 at 101 – 185.
[100] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 44 where reference is made to s 31 (3) of the Canada Evidence Act 1985.
[101] South African Law Reform Commission Discussion Paper 131 (Project 126) Review of the Law of Evidence (2014) 44 where reference is made to the provisions facilitating proof of documents in the Australian Evidence Act 1995. See also A Stanfield *The Authentication of Electronic Evidence* (PhD thesis, Queensland University of Technology, 2016) 95 – 120.
[102] Commonwealth Secretariat 'Model Law on Electronic Evidence' available at *http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf*, accessed on 30 April 2018.
[103] Section 31.3 of the Canada Evidence Act which deals with a *presumption of integrity*. See also *R v Oland* 2018 NBQB 259 para 12 – 23 for a discussion of a presumption of integrity.
[104] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 24.
[105] South African Law Reform Commission Discussion Paper 131 (Project 126) 'Review of the Law of Evidence' (2014) 41 – 45.
[106] *Delsheray Trust* supra note 2 at para 51 where a full bench of the Western Cape high court reached this conclusion.

party to civil proceedings who does not object.[107] Additionally, the SALRC recommends the creation of a standing committee (working group) to review the question of presumptions (in addition to other issues identified in the discussion paper).[108]

Currently, in the absence of this type of statutory presumption, a court in South Africa has several mechanisms by which it can properly receive electronic evidence, including relying on the common law and/or statute. Introducing a presumption of this nature to only civil proceedings and leaving a lacuna in the regulation of criminal law will likely cause confusion and potentially inconsistent application. A review of recent case law[109] indicates there is no urgent need to adopt such a presumption in its suggested form, and for the short to medium term, the current legislative and common law framework is better off as it stands.

4.6.2 Application of a presumption of reliability moving forward

It is necessary to facilitate the admission of data messages in an expedient and cost-effective manner, while taking account of the inherent difficulties one may face with electronic data.[110] The common law currently achieves this effectively without the need for further statutory confusion. Although it dealt with the doctrine of judicial notice[111] – the Appellate Division's *Mthimkulu* judgment could inform how future courts receive and deal with electronic evidence when applying the common law.

The key principle: no hard and fast rule should be set out. The facts of each case, the type of hardware and software at issue, the nature and size of the business and its employees, whether the evidence is disputed, the form and characteristics of the data message itself, amongst many others, must be considered to form a view as to whether a court can draw an inference of probability based on frequently recurring examples of circumstantial evidence.[112]

---

[107] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 79.
[108] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 84 – 87.
[109] *S v Meyer* supra note 2, *S v Miller* supra note 2, *S v Brown* supra note 2, *S v Helm* supra note 47 for four recent criminal law examples. See also *Delsheray Trust* supra note 2, and *LA Consortium* supra note 80 for two recent civil law examples.
[110] South African Law Reform Commission Issue Paper 27 (Project 126) Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues (2010) 7 – 13 where several concerns with electronic evidence are discussed. See also, South African Law Reform Commission *Discussion Paper 131, Project 126 - Review of the Law of Evidence* (2014) Issue 10: A Presumption of Regularity 78 – 80.
[111] *Delsheray Trust* supra note 2 para 53, where the court noted: 'Had computers, as we know them today, been used in the ordinary course of banking business, Corbett JA might well have applied the approach which he himself articulated in the *Mthimkulu* judgment.'
[112] Schwikkard & van der Merwe op cit note 7 at 579; Zeffertt & Paizes op cit note 6 at 182 – 184.

If the circumstances so dictate, as they did in *Delsheray Trust v ABSA*, then a court should consider:[113]

1. the nature of the process and instrument involved in the particular case

This would require a court to consider the nature and characteristics of the data message. It could ask: What type of electronic instrument was used to generate the data message? What software was being used? Objectively, how reliable is the hardware and software? What circumstances surrounded the creation of the data message? For example, what experience and expertise did the relevant employee have? Was the message generated by a business or in a personal capacity? This type of enquiry is dynamic and should not be restricted to a closed list of factors as it will naturally require the consideration of any relevant fact.

2. the extent, if any, to which the evidence is challenged

The extent to which the evidence is challenged has a 'bearing on the cogency of the evidence rather than its admissibility.'[114] Clearly, the absence of a challenge does not relieve the opposite party of any evidential burden it may have.[115]

3. the nature of the enquiry and the facta probanda in the case

Regardless of whether the matter is civil or criminal in nature a court must consider the facts that need to be proved holistically – for example, in *Delsheray Trust v ABSA* it was found that a verifying affidavit in contested legal proceedings will only have a minor effect; the court found it did not create any onus or evidential burden and played no role in the enquiry as to whether a defendant raised a valid defence to the claim.

In summary: much will depend upon the facts and circumstances of each individual matter. The application of a presumption as set out in *Delsheray Trust v ABSA* (applying the Appellate Division *Mthimkulu* judgment) is preferable to the proposed SALRC reform which will leave a large lacuna in relation to criminal law. As it stands, the intention is to only introduce a statutory presumption into civil proceedings. Any solution created must be

[113] *Delsheray Trust* supra note 2 para 41.
[114] Ibid.
[115] Ibid. See also *Mthimkulu* supra note 41 at 764 – 765.

implemented universally – across both civil and criminal law in South Africa. The now repealed Computer Evidence Act 57 of 1983 received wide-spread criticism[116] for only regulating civil law, and ignoring criminal law – this mistake should not be made twice.

As pointed out by Mason, in the absence of evidence, the presumption that mechanical instruments were working at the relevant time is a little crude and probably too simplistic in 2018, the advanced nature of technology means we cannot simply accept 'the machine was working'. A person must show the relevant court, whether on affidavit or via viva voce evidence, that the evidence is reliable and can be trusted – there must be some basis for a court to confirm its reliability and veracity. It would not be overly onerous for a business owner or a relevant employee of a corporate entity to depose to an affidavit setting out a factual basis for a court to conclude that a presumption is appropriate.

4.7 CONCLUSION

Although there are many instances where a presumption of reliability can and should apply there are equally as many where this type of presumption should not apply given the nature of modern technology. Consequently, evidence must be adduced, or circumstantial evidence together with inferential reasoning must demonstrate that a presumption of reliability is appropriate in the circumstances.

Currently, the ECT Act adequately facilitates the admission of data message evidence into court. A court can directly rely on the provisions of the ECT Act; or if it so wishes, rely on the common law.[117]

The SALRC suggests a statutory presumption of reliability applicable to only civil law in their latest investigation into electronic evidence, together with a standing committee on electronic evidence. My view is that the working group should be created with a mandate to further consider this issue, but that for short term, South Africa is better off with the ECT Act and common law interpretation as it stands; and South African should only implement law reform in the context of electronic evidence that applies to both civil and criminal proceedings. Accordingly, the law reform proposed by the SALRC in the context of presumptions may well be desirable, but it is not necessary.

[116] D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 112.
[117] As was the case in *Delsheray Trust* supra note 2.

*CHAPTER 5:*ADMISSIBILITY AND EVIDENTIAL WEIGHT OF ELECTRONIC EVIDENCE*

5.1 INTRODUCTION

Technology is more accessible and affordable than ever before. More than half of the South African population can access the internet.[1] The natural inference one must draw is that data and data messages[2] will play a significant role in most, if not all forms of legal and administrative proceedings – now and in the future.[3]

As a result, to accommodate the development and change in societal norms, the legislative environment governing data and electronic evidence, both in South Africa[4] and worldwide, has seen significant change – and it is likely we will continue to see more change as we progress further into the 21st century.[5]

Currently, the primary legislative instrument regulating electronic forms of evidence is the ECT Act.[6] However, the SALRC, in its most recent publication on evidence,[7] suggest a

---

* A version of this chapter has been published by Oxford University Press, L Swales 'Electronic and Cyber Evidence' in A Bellengère et al (eds) *The Law of Evidence in South Africa* 2 ed (2019) 120 – 156.

[1] Internet World Stats 'South Africa' available at *http://www.internetworldstats.com/africa.htm#za*, accessed on 7 July 2018. Approximately 53.7% of South Africa's population has internet access as at December 2017. In 2008, the South African penetration rate was approximately 9%.

[2] Although the umbrella term electronic evidence is sometimes used, the technically correct term in South African law is *data messages* and/or *data*. However, for ease of reference, this chapter will use the terms data messages and electronic evidence interchangeably. See South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) at 27 where the SALRC states: '[the] definition of data message in any event appears largely consistent with the term electronic evidence.' See also section 1 of the ECT Act where data is defined as 'electronic representations of information in any form', and where data message is defined as 'data generated, sent, received or stored by electronic means.' See also the discussion in para 2.1 above.

[3] P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) at 437 where the authors note that electronic communications have become pervasive in legal interactions; R Davey & L Dahms-Jansen *Social Media in the Workplace* (2017) 287.

[4] For an overview of the South African position in relation to electronic evidence, see J Hofman & J de Jager 'South Africa' in S Mason (ed) *Electronic Evidence* 3 ed (2012). See also C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461 – 477; Davey & Dahms-Jansen op cit note 3 at 287 – 299; D Van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 107 – 147; S Papadopoulos & S Snail (eds) *Cyberlaw@SA III* (2012) 322 – 323; D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 1)' (2010) 3 *TSAR* 558 – 575.

[5] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) at 22 – 23 where the SALRC propose three options to reform the current regulatory landscape. See also R Susskind *Tomorrow's Lawyers An Introduction to the Future* 2 ed (2017) 1 – 10.

[6] Read together with the common law, the relevant rules of court, and other applicable legislation such as the Law of Evidence Amendment Act 45 of 1988 in so far as hearsay is concerned, and the Civil Proceedings Evidence Act 25 of 1965, together with the Criminal Procedure Act 51 of 1977 in the context of civil and criminal proceedings respectively.

[7] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014).

partial repeal thereof, together with a comprehensive *Law of Evidence Bill* to codify the law of evidence in South Africa.[8] The original closing date for comment was October 2014. This was extended to March 2015, with an intended completion date of March 2016.[9] The final report was presented to the Minister of Justice in November 2016, the process is yet to be completed. Consequently, in light of the proposals put forward by the SALRC, this chapter aims to critically evaluate the admissibility, authentication, and weight of electronic evidence.

5.2. HISTORY OF ELECTRONIC EVIDENCE IN SOUTH AFRICA

5.2.1 Background[10]

Our courts have been cautious[11] and 'conservative'[12] in relation to electronic transactions in general – however, it appears that this approach is changing as electronic transactions and a plethora of electronic means of communication become common-place.[13] However, South African courts are not yet equipped to deal with a variety of types of data messages that would

[8] See Annexure A, which is the *Law of Evidence Bill* proposed by the SALRC in South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 90 – 95.
[9] Information gleaned from e-mail correspondence with Advocate van Vuuren (Principal State Law Adviser) in August 2015, and again in April 2018.
[10] As noted above in paragraph 3.1, there is no *sui generis* category for electronic evidence in South African law. Depending on the nature of the evidence, and the purpose it will serve, it will be admitted to court as documentary evidence in the form of a document, or real evidence in the form of a tangible thing – typically supplemented by expert oral evidence to explain relevance or some related issue. See Schwikkard & van der Merwe op cit note 3 at 438; van der Merwe et al op cit note 4 at 107 – 147; M Watney 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 *Journal of Information, Law and Technology* 11; P Fourie *Using Social Media as Evidence in South African Courts* (LLM thesis, North-West University, 2016) 6 – 16.
[11] *Maseti v S* [2014] 1 All SA 420 (SCA) para 33.
[12] Hofman & de Jager op cit note 4 at 762.
[13] For example, *ABSA Bank Ltd v Le Roux* 2014 (1) SA 475 (WCC) para 19 where the court found what must be close to trite in 2018, that any electronically stored data (within the meaning of data message in section 1 of the ECT Act) is admissible in evidence in terms of s 15 of the ECT Act (unless a ground of exclusion operates – for example hearsay or similar fact evidence). See also, *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD) where substituted service was authorised via Facebook; *Delsheray Trust v ABSA Bank Limited* [2014] 4 All SA 748 (WCC) where the court accepted that a deponent to a verifying affidavit in summary judgment proceedings may validly rely exclusively on electronic data; *Dutch Reformed Church v Sooknunan* 2012 (6) SA 201 (GSJ) and *Isparta v Richter* 2013 6 SA 529 (GP) where the courts ordered monetary damages after the publication of defamatory material on social media networks. Moreover, the promulgation of legislation such as the Protection from Harassment Act 17 of 2011 and the Protection of Personal Information Act 4 of 2013, together with the soon to be published Hate Speech Bill and Cybercrimes Bill indicate a clear shift in priority in so far as electronic communication is concerned.

ordinarily be required as evidence. Consequently, for the short to medium term at least, electronic evidence will for practical reasons be admitted to court in the form of a print-out.[14]

5.2.2 *Development and history of electronic evidence in South Africa*

The first computer is reported to have landed in South Africa in the 1950's,[15] but the statutory evolution of electronic evidence is often traced to the decision of *Narlis*.[16]

Following the decision in *Narlis*,[17] the South African Law Commission (as it was then called)[18] investigated the need for law reform in relation to electronic evidence. Ultimately, the Law Commission found that legislative reform was required, and suggested the promulgation of a separate statute.[19]

Before the separate statute was promulgated, and in the interim, in *S v Harper*[20] the court was concerned with the meaning of the word document in the context of a criminal trial where the admissibility of a computer-print out was at issue. It was held that in the absence of specific governing legislation (in terms of s 221 of the Criminal Procedure Act 51 of 1977) the word document in s 221(5), in its ordinary grammatical sense, was wide enough to include print-outs from a computer. However, the court held that the computer itself, and the information thereon, could not fall under the wider definition of the word document.

Following the Law Commission's recommendation, the Computer Evidence Act 57 of 1983[21] commenced operation on 1 October 1983. As discussed above in chapter 2, the

---

[14] *S v Brown* 2016 (1) SACR 206 (WCC) 28 para 18. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 29. This also accords with my own personal experience as a practicing attorney from 2007 to date.

[15] Y Lulat *United States Relations with South Africa: A Critical Overview from the Colonial Period to the Present* (2008) 73 where date is stated as 1952 and the computer was imported by IBM; Hofman & de Jager op cit note 4 at 761 where the date is stated 1959, and Mybroadband 'South Africa's First Computers' (2015) *https://mybroadband.co.za/news/hardware/132408-south-africas-first-computers.html* where the date is also stated as 1959. The actual date is of little consequence to this research, but it appears the first computer arrived in South Africa at the end of the 1950s.

[16] 1976 (2) SA 573 (A). See also van der Merwe et al op cit note 4 at 111 and the discussion in para 2.3.1 above in chapter 2.

[17] See also the discussion in paragraph 2.3.1.

[18] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 19. The South African Law Commission changed its name to the South African Law *Reform* Commission in 2002. See South African Law Reform Commission (2013) *http://salawreform.justice.gov.za/anr/2012-2013-anr-salrc.pdf* at 7, accessed on 5 April 2017.

[19] South African Law Commission Project 6 *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computer, Review of the Law of Evidence* 1982.

[20] 1981 (1) SA 88 (D).

[21] For a perspective on the now repealed Computer Evidence Act No 57 of 1983, see S Mapoma *A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM thesis, University of South Africa, 1997) 3 – 32. See further the discussion in paragraph 2.3.2 above.

Computer Evidence Act was South Africa's first attempt at legislating rules and norms for computer and electronic based evidence – it only applied to civil proceedings, [22] and while in effect, was criticised[23] for being overly technical and for ignoring the regulation of electronic evidence in criminal matters.[24] This cautious approach was based on the general belief that alterations of electronic data are far harder to detect than alterations to paper documents,[25] which have certain attributes which assist with verification – such as signature, ink and handwriting.[26] In my view, technology has developed to a point where these attributes are easily mirrored. Moreover, forensic science has progressed and an expert should be able to provide a court with a considered opinion regarding the authenticity of an electronic communication should that be in dispute.

5.2.3 Background to the Electronic Communications and Transactions Act

In response to modern trends involving technology, and various new forms of communication, in 1996, UNCITRAL published the Model Law, 1996.[27] The broader goal of the UNCITRAL is to facilitate and encourage international trade. Consequently, the Model Law, 1996 is intended to serve as a guide for member states regarding e-commerce and related issues (such as electronic evidence). But for two sections,[28] dealing with certification and electronic signatures,[29] the ECT Act is based entirely on the United Nations guidance, and is South Africa's primary legislative tool regulating electronic commerce.

---

[22] D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) at 843; South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 19.

[23] *Ndlovu v Minister of Correctional Services* [2006] 4 All SA 165 (W) at 171 where the court noted that the Computer Evidence Act had two major shortcomings: first, that is was 'cumbersome' to comply with its provisions, and secondly, that it only applied to civil proceedings. See also *S v Brown* supra note 14 para 16 where it was stated that the Computer Evidence Act was 'generally considered to have failed to achieve its purpose'. See also Schwikkard & van der Merwe op cit note 3 at 440; van der Merwe op cit note 4 at 112; Hofman & de Jager op cit note 4 at 761 – 763; Zeffertt & Paizes op cit note 22 at 431 – 432. See also D Zeffertt & A Paizes *The South African Law of Evidence* 3 ed (2017) at 455 – 456.

[24] Hofman & de Jager op cit note 4 at 761 – 763.

[25] Theophilopoulos op cit note 4 at 467 – 468; J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 258.

[26] Davey & Dahms-Jansen op cit note 3 at 291.

[27] United Nations 'Model Law on Electronic Commerce with Guide to Enactment' (1996) *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, accessed 25 April 2017.

[28]United Nations Commission on International Trade Law 'Status' (2018) *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html*, accessed on 25 April 2017 where the Secretariat lists member states that comply with the UN 1996 Model Law, there are 71 States in a total of 150 jurisdictions that have adopted it. South Africa is largely compliant: '*…except for the provisions on certification and electronic signatures.*'

[29] On electronic signatures generally, see *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a* 2015 (2) SA 118 (SCA) para 27 – 29. See also S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17 *PELJ*

In *Ketler Investments CC t/a Ketler Presentations v Internet Service Providers' Association*,[30] the court noted that the ECT Act: 'Recognises both the economic and social importance of electronic communications as well as the need to promote technology neutrality in the application of legislation.' The ECT Act facilitates this modern methodology in South Africa by recognising data messages as the functional equivalent of paper – this approach has been endorsed by various decisions,[31] and technological neutrality is codified as one of the objects of the ECT Act.[32]

In *MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises*,[33] the court confirmed what is surely now trite law: the ECT Act facilitates proof of facts by way of data messages.

5.3 OVERVIEW OF THE COMMON LAW POSITION IN RELATION TO DATA MESSAGES

Section 3 of the ECT Act, interpretation, reads as follows:

> This Act must not be interpreted so as to exclude any statutory law or the common law from being applied to, recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act.

This provision was at issue in *Trustees for the time Being of the Delsheray Trust v ABSA Bank Limited*,[34] where the admissibility of electronic evidence was central. In this context, the court found as follows:

> The subject of computer evidence in South Africa, it should be noted, is regulated by the ECT Act but respondent did not present or argue its case on the basis of the provisions of ECT Act. In terms of the express wording of s 3, however, it does not exclude the application of the common law.

2805 – 2820; Y Mupangavanhu 'Electronic signatures and nonvariation clauses in the modern digital world: The case of South Africa' (2016) 133 *SALJ* 853 – 873; L Swales 'The regulation of electronic signatures: Time for review and amendment' (2015) 132 *SALJ* 257 – 270.

[30] 2014 (2) SA 569 (GJ) para 30.

[31] *S v Miller* 2016 (1) SACR 251 (WCC) para 52; *LA Consortium & Vending CC v MTN Service Provider* 2011 (4) SA 577 (GSJ) para 12 – 13; *Ndlovu v Minister of Correctional Services* supra note 23 at 165. See also the court's analysis in one of the seminal cases involving electronic evidence, *S v Ndiki* 2008 (2) SACR 252 (CK), where although the term *functional equivalence* is not specifically used, the analysis performed by the court (para 53) uses similar logic; see also the South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 62 – 63.

[32] Section 2 (f) of the ECT Act. See also *LA Consortium* supra note 31 para 15.

[33] 2011 (4) SA 562 (WLD). Confirmed on appeal in the South Gauteng High Court in Johannesburg in *LA Consortium* supra note 31.

[34] [2014] 4 All SA 748 (WCC) para 17. This case is discussed in detail in chapter 4 above.

In S *v Ndiki*,[35] in the context of data messages, the court confirmed the common law position by noting:

> As a point of departure it may be appropriate to restate the common law position with regard to evidence generally, namely, that evidence tending to prove or disprove an allegation which is in issue is admissible unless a specific ground for exclusion operates.

Therefore, even if probative material is relevant, it will only be admissible as evidence if it is not excluded by a common law or statutory rule precluding the admissibility of a certain type of evidence,[36] or precluding the admissibility of evidence obtained in a certain manner.[37] The fact that evidence is in data message format should not shield it from normal evidentiary rules applicable. For example, with similar fact evidence,[38] the Constitutional Court recently confirmed that, when looked at in totality, similar fact evidence will only be admissible if has sufficient probative value to outweigh its prejudicial effects.[39] The fact that similar fact evidence may be contained in data message format will not preclude it from being considered in the same light as if the evidence was in traditional form.

In so far as data messages are concerned, as pointed by out by Bozalek J in *S v Brown*:[40]

> … the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document.

In the context of determining whether electronic communications are admissible, in *S v Ndiki*:[41]

> A preferable point of departure in my view is to rather closely examine the evidence in issue and to determine what kind of evidence it is that one is dealing with and what the requirements for its admissibility are.

---

[35] *S v Ndiki* supra note 31 paras 20 – 21.
[36] For example, hearsay evidence as a default position is not admissible unless an exception applies. For more on hearsay evidence see Schwikkard & van der Merwe op cit note 3 at 287 – 304; Zeffertt & Paizes op cit note 22 at 385 – 441.
[37] Evidence obtained in an unconstitutional manner is generally inadmissible, but subject to the overriding factor of the administration of justice balanced against the right of an accused to have a fair trial – consequently, even evidence obtained in an unconstitutional manner may (in certain instances) be admissible. For example, see *Harvey v Niland* 2016 (2) SA 436 (ECG). For more on unconstitutionally obtained evidence see Schwikkard & van der Merwe op cit note 3 at 198 – 283; Zeffertt & Paizes op cit note 22 at 721 – 736; *S v Brown* supra note 14 para 14. See also Davey & Dahms-Jansen op cit note 3 at 287 – 299 and Zeffert & Paizes op cit note 23 at 798 – 805.
[38] *Savoi v National Director of Public Prosecutions* 2014 (5) SA 317 (CC).
[39] Ibid para 55.
[40] *S v Brown* supra note 14 para 18.
[41] *S v Ndiki* supra note 31 para 53.

As discussed above in chapter 3,[42] in order to be received into evidence, a court will classify a data message as either documentary evidence, or real evidence (or a combination of both). The classification of the data message will dictate the admissibility rules it will have to overcome.[43] Depending on the circumstances, some of these admissibility hurdles (for example the requirement of a document being an original) will be qualified[44] by the ECT Act.

In *Ndlovu v Minister of Correctional Services*, the court summarised the admissibility requirements for documentary evidence:[45]

> Documentary evidence, in order to be admissible in evidence, generally has to comply with three rules (a) the statements contained in the document must be relevant and otherwise admissible; (b) the authenticity of the document must be proved; and (c) the original document must normally be produced.

Conversely, for real evidence to be admissible, it must only be relevant.[46] Alternatively, if in data message form, there is some debate[47] as to whether the evidence must be relevant *and in addition*, authentic.[48] In *Motata v Nair NO*,[49] the court weighed up the various approaches and held it was unnecessary to decide whether proof of authenticity is in fact a prerequisite for the admissibility of data messages. My view is that data messages must be authentic before being accepted into evidence – particularly given the nature of electronic evidence.[50]

5.4. ADMISSIBILITY OF DATA MESSAGES

5.4.1 Overview

Section 15 of the ECT Act regulates the admissibility and evidential weight of data messages.[51] Section 15 (1) deals with admissibility, while s 15 (2) and s 15 (3) provide guidance in so far

---

[42] See paragraph 3.5 above.
[43] Schwikkard & van der Merwe op cit note 3 at 445 – 446; Hofman & de Jager op cit note 4 at 776 – 779.
[44] *S v Brown* supra note 14 para 20.
[45] *Ndlovu v Minister of Correctional Services* supra note 23 at 172.
[46] *S v Baleka (3)* 1986 (4) SA 1005 (T), and *S v Fuhri* 1994 (2) SACR 829 (A). Hofman op cit note 25 at 268; Schwikkard & van der Merwe op cit note 3 at 445.
[47] See paragraph 3.5 above.
[48] N Whitear-Nel 'Admissibility of hearsay evidence' (2007) 20 *SACJ* 116.
[49] 2009 (1) SACR 263 (T) para 21.
[50] *S v Brown* supra note 14 para 20; South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7 – 13 for a discussion on some of the difficulties with electronic evidence, including: ease of manipulation, difficulty of detecting manipulation, changing technology, and evolving software and hardware. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 27 – 46.
[51] Papadopoulos & Snail op cit note 4 at 322; Hofman & de Jager op cit note 4 at 261 – 264; Theophilopoulos op cit note 4 at 464 – 474.

as assessing evidential weight is concerned; finally, s 15 (4) creates a further statutory exception[52] to the hearsay rule by introducing an exception for business records.[53]

In *S v Meyer*,[54] the court confirmed that admissibility and weight are distinct concepts. A court will first determine admissibility – either evidence is admissible, or not. Only once a court finds that evidence is admissible will it turn to consider evidential weight.[55] Clearly, if a court finds evidence is inadmissible, there is no need to consider its weight.

5.4.2 Section 15(1) of the ECT Act

Section 15(1) reads as follows:

> 15. Admissibility and evidential weight of data messages
>
> (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence
>
> (*a*) on the mere grounds that it is constituted by a data message; or
>
> (*b*) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

Section 15(1) of the ECT Act seeks to facilitate[56] the admissibility of data messages, and follows an inclusionary rather than an exclusionary approach.[57] The section follows global trends illustrated by the Model Law, 1996 and prohibits the exclusion of evidence on the mere grounds that it is generated by a computer and not by a natural person.[58] Moreover, evidence cannot be excluded on the grounds that it is not original – if the evidence is the best evidence reasonably available.[59]

As noted by the Supreme Court of Appeal in *First Rand Bank Ltd v Venter*,[60] s 15 of the ECT Act can be summarised as facilitating the use of data messages. Importantly, in *Ndlovu v Minister of Correctional Services,*[61] the court held:

---

[52] In addition to the exceptions created in s 34 of the Civil Proceedings Evidence Act 25 of 1965, s 221 – 222 of the Criminal Procedure Act 51 of 1977, and s 3 of the Law of Evidence Amendment Act 45 of 1988.
[53] See the discussion in chapter 3 above.
[54] 2017 JDR 1728 (GJ) para 310.
[55] *S v Meyer* supra note 54 para 310; Schwikkard & van der Merwe op cit note 3 at 20.
[56] *Ndlovu v Minister of Correctional Services* supra note 23 at 165 – 166; *LA Consortium* supra note 31 para 7.
[57] *S v Brown* supra note 14 at para 17.
[58] Section 15 (1)(a). *Ndlovu v Minister of Correctional Services* supra note 23 at 172.
[59] Section 15 (1)(b). *Ndlovu v Minister of Correctional Services* supra note 23 at 172; *LA Consortium* supra note 31 para 18 – 19; *Maseti v S* supra note 11 para 33.
[60] [2012] JOL 29436 (SCA) para 16.
[61] *Ndlovu v Minister of Correctional Services* supra note 23 at 172.

> Section 15(1) does not… do away with these three requirements [referring to common law requirements in so far as documentary evidence is concerned]. The data message must be relevant and otherwise admissible, be proved to be authentic and the original be produced, unless (in regard to the latter aspect) section 15(1)(b) applies.
>
> The only exemption created by section 15(1)(a) is that it is admissible, all other requirements being in place, despite the fact that it was generated by a computer and not by a natural person.

In S *v Ndiki*,[62] the court held that a court should consider the nature[63] of the data message, and determine whether it relies on the credibility of a person, or a machine.[64]

> It is an issue that must be determined on the facts of each case having regard to what it is that the party concerned wishes to prove … the contents thereof, …the function performed by the computer and the requirements of the relevant section relied upon for the admission of the document in question.[65]

In *S v Brown,*[66] the decision in *Ndiki* was endorsed, and the court held:

> the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one was dealing with and what the requirements for its admissibility are.

In *S v Meyer*,[67] the court confirmed the importance of functional equivalence, and reiterated the position that s 15 does not do away with the common law; Klein AJ held:

> According to the ECT Act data messages are the functional equivalents of documents and therefore, except where the Act specifically provides for exceptions, the ordinary common law requirements for the admissibility of documents must be adhered to.

Consequently, the provisions of s 15 must be considered in light of the common law of evidence, and s 15 certainly does not render all data messages admissible 'without further ado'.[68] Moreover, as noted in *S v Brown:*[69] 'the provisions of s 15 [of the ECT Act] certainly do not exclude our common law of evidence'.

---

[62] *S v Ndiki* supra note 31 para 20 – 21.
[63] *S v Brown* supra note 14 para 20; *S v Ndiki* supra note 11 para 20 – 21.
[64] *S v Ndiki* supra note 31 para 20 – 21; De Villiers supra note 4 at 566 – 567.
[65] *S v Ndiki* supra note 31 para 20 – 21.
[66] *S v Brown* supra note 14 para 20.
[67] *S v Meyer* supra note 54 para 298; *Liberty Group Limited v K & D Telemarketing CC* 2015 JDR 1846 (GP) para 33. See also *S v Panayiotou* [2018] 1 All SA 224 (ECP) para 85 where the court relies on s 15 of the ECT Act.
[68] *Ndlovu v Minister of Correctional Services* supra note 23 at 172; *La Consortium* supra note 31 para 12 – 14. See also Schwikkard & van der Merwe op cit note 3 at 446; Theophilopoulos op cit note 4 at 474 – 475; Hofman & de Jager op cit note 4 at 766 – 767; De Villiers op cit note 4 at 572.
[69] *S v Brown* supra note 11 at para 18.

As noted by Hofman,[70] data messages are subject to the ordinary laws of evidence. In this regard, the purpose of the ECT Act is to facilitate electronic forms of communications and transactions, and to provide for functional equivalence and technological neutrality.[71] The purpose of the ECT Act is 'not to reform the law of evidence', nor is its purpose to elevate data messages above other forms of evidence which would undoubtedly lead to format shopping.[72]

Cassim notes there is a dearth of case law in a civil context, and submits that the ECT Act creates a 'rebuttable presumption that data messages or printouts are admissible in evidence.'[73] To support this view, reference is made to *Ndlovu v Minister of Correctional Services,*[74] and a 2005 academic article.[75] The view that data messages are automatically admissible – which would destroy functional equivalence and encourage format shopping – is incorrect, and has been universally rejected by South African courts in, *inter alia: Ndlovu v Minister of Correctional Services,*[76] *La Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty)*,[77] *S v Brown*,[78] and *S v Meyer.*[79] General consensus amongst academic opinion also rejects this approach.[80]

Does the ECT Act – or any other law – make provision for mandatory notice when a party relies on electronic evidence? No. In *Liberty Group Limited v K & D Telemarketing*

[70] Hofman & de Jager op cit note 4 at 766.
[71] Section 2 of the ECT Act.
[72] Hofman & de Jager op cit note 4 at 766.
[73] J Cassim 'The use of electronic discovery and cloud computing technology by lawyers in practice: lessons from abroad' (2017) 42 *Journal for Juridical Science* 27. To be entirely accurate, this statement should refer to s 15(4) of the ECT Act and its requirements. Section 15(4) creates a business records exception where data messages are rebuttable proof of the contents contained therein *only if*: a) created during the ordinary course and scope of business; and b) certified correct by an officer of the business concerned.
[74] *Ndlovu v Minister of Correctional Services* supra note 23 at 172. However, in my view, *Ndlovu v Minister of Correctional Services* is not authority for the proposition that all data messages are automatically admissible in evidence. The court clearly notes that data messages are not admissible without further ado, and that doing so would 'elevate a data message evidentially above an ordinary document', and that s 15 does not do away with the ordinary common law requirements in relation to documentary evidence. See further *S v Brown* supra note 14 para 18; *S v Meyer* supra note 54 para 299.
[75] D Collier 'Evidently not so simple: Producing computer print-outs in court' (2005) *Juta Business Law* 6 – 9. This interpretation appears to have been retracted by Collier herself in Schwikkard & van der Merwe *Principles of Evidence* 3 ed (2009) 414 – 415, particularly footnote 42 – 43 thereof. The chapter dealing with electronic evidence in the latest version of this seminal text, Schwikkard & van der Merwe op cit note 3 ch 21 is written by a different author and this early view is not canvassed in any detail.
[76] *Ndlovu v Minister of Correctional Services* supra note 23 at 171 – 174.
[77] *La Consortium* supra note 31 para 11 – 15.
[78] *S v Brown* supra note 14 para 18.
[79] *S v Meyer* supra note 54 para 299 where it is noted: 'Section 15 (1) does not, however make all data messages automatically admissible. According to the ECT Act data messages are the functional equivalents of documents and therefore, except where the Act specifically provides for exceptions, the ordinary common law requirements for the admissibility of documents must be adhered to.'
[80] Hofman & de Jager op cit note 4 at 765 – 766; Theophilopoulos op cit note 4 at 461 – 481.

CC,[81] the court confirmed that it is not mandatory to produce a certificate in terms of s 15(4) in order to rely on electronic evidence, and correctly it is submitted held as follows:

> However, with reference to the matter of *Ndlovu v Minister of Correctional Services and Another* I am of the respectful opinion that firstly it is not necessary for the Plaintiff to produce a certificate in terms of Section 15(4) of the ECT Act. The production of such a certificate makes the particular computer printout prima facie evidence without more. However there is no such certificate available and accordingly the admissibility and weight of the computer printouts must be established with reference to the provisions of Section 15(1), (2) and (3) of the Act read together with the Law of Evidence Amendment Act 45 of 1988 that makes provision for the acceptance of hearsay evidence.

It would be nonsensical to suggest that electronic evidence can only be relied upon with notice in terms of the ECT Act (or notice in terms of some other law) – this interpretation, to the extent it exists, would clearly impose further restrictions on electronic evidence than currently exist with ordinary evidence and would conflict with functional equivalence.[82]

5.4.3 Admissibility of data messages as documentary evidence

In *Ndlovu v Minister of Correctional Services,*[83] it was held that for documentary evidence to be admissible, it has to comply with three rules:

> (a) the statements contained in the document must be relevant and otherwise admissible;
> (b) the authenticity of the document must be proved; and
> (c) the original document must normally be produced. [84]

This view is endorsed by text book authors and academics.[85] Similarly, in *S v Brown,*[86] the court echoed this sentiment and held:

> the ordinary requirements of our law for the admissibility of such evidence [data messages in documentary form] is that the document itself must be produced, which document, ordinarily speaking, must be the original and the authenticity of the document must be proved. These requirements are, of course, qualified by those specific provisions of the ECTA having a bearing on electronic communications.

---

[81] 2015 JDR 1846 (GP) para 33.
[82] *Director of Public Prosecution v Modise* 2012 (1) SACR 553 (GSJ) where it was found that the provisions of s 15 of the ECT Act do not require a party to provide another with notice when relying on data message (or print-outs thereof) evidence.
[83] *Ndlovu v Minister of Correctional Services* supra note 23 at 172.
[84] Ibid.
[85] Schwikkard & van der Merwe op cit note 3 at 431 – 436; Zeffertt & Paizes op cit note 22 at 827 – 843; Theophilopoulos op cit note 4 at 465; Watney op cit note 10 at 3; De Villiers op cit note 4 at 572.
[86] *S v Brown* supra note 14 para 20.

Moreover, in the recent matter of *S v Meyer*,[87] the court held:

> Section 15 places electronic information on the same footing as traditional paper-based transactions, and thus does not do away with the requirements governing the admissibility of documentary evidence which are relevance, authenticity and originality.

Consequently, for a data message classified as documentary evidence to be admissible, it must be relevant, otherwise admissible, authentic and original (subject to concessions in the ECT Act).[88]

5.4.3.1 Relevance

Relevance is always critical in an evidentiary dispute. What does this term mean? As noted by Zeffertt:[89]

> There have been many attempts to define relevance; but it is important to grasp that for the purposes of the law of evidence we are not required to act like philosophers or logicians. Relevance, in this context, is largely a matter of common sense and practicality… [R]elevance is not determined in a vacuum but on the facts of each case.

Comparatively, Rule 401 of the Federal Rules of Evidence of the United States of America provides a test for relevance:[90]

> Evidence is relevant if:
>
> > (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and
> >
> > (b) the fact is of consequence in determining the action.

Some academic authors define relevance as a matter of 'reason and common sense'.[91] In *R v Matthews*, it was held that relevance is 'based upon a blend of logic and experience lying outside the law.'[92] When will a fact be relevant? According to the Appellate Division more than one hundred years ago in *R v Mpanza*: A fact is relevant if from its existence 'inferences

[87] *S v Meyer* supra note 54 para 298.
[88] *S v Brown* supra note 14 para 20; Hofman & de Jager op cit note 4 at 765 – 770.
[89] D Zeffert & A Paizes 'Essential Evidence' (2010) 75 – 77. See also Schwikkard & van der Merwe op cit note 3 at 49 – 63.
[90] Schwikkard & van der Merwe op cit note 3 at 50.
[91] Zeffertt & Paizes op cit note 23 at 237 – 242.
[92] 1960 (1) SA 572 (A) at 758 in Zeffertt & Paizes op cit note 22 at 237. See also *S v Meyer* supra note 54 para 291 – 294.

may properly be drawn as to the existence of the fact in issue'.[93] Stated in the positive,[94] according to *R v Trupedo*: 'all facts relevant to the issue in legal proceedings may be proved'.[95] In *DPP v Kilbourne*,[96] it was held that facts are relevant if 'logically probative or disprobative of some matter which requires proof'. The question of relevance can 'never be divorced from the facts of a particular case before court'.[97]

5.4.3.2 Otherwise admissible

In addition to being relevant, the data message must otherwise be admissible – it must comply with South Africa's common law of evidence. A data message must be treated the same as all other forms of evidence, subject of course to the concessions in the ECT Act.[98] If a data message contains hearsay, it should be admissible in terms of one of the statutory hearsay exceptions before it is accepted by a court.[99]

Further, if data message evidence is obtained in an unlawful manner, a court will have a general discretion to admit or exclude this evidence.[100] In *S v Brown,*[101] in the context of data messages, the court noted:

> As a starting point, sec 35(5) of the Constitution provides that evidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the admission of that evidence would render a trial unfair or otherwise be detrimental to the administration of justice.

In *S v Coetzee*[102] Sachs J explained:

> There is a paradox at the heart of all criminal procedure, in that the more serious the crime and the greater the public interest in securing convictions of the guilty, the more important do constitutional protections of the accused become. The starting point of any balancing enquiry where constitutional rights are concerned must be that the public interest in ensuring that innocent people are not convicted and subjected to ignominy and heavy sentences, massively outweighs the public interest in ensuring that a particular criminal is brought to book.

---

[93] 1915 AD 348 at 352 – 352 in Zeffertt & Paizes op cit note 22 at 237.
[94] Schwikkard & van der Merwe op cit note 3 at 49.
[95] 1920 AD 58 62 in Schwikkard & van der Merwe op cit note 3 at 49.
[96] 1973 AC 729 756 in Schwikkard & van der Merwe op cit note 3 at 51.
[97] *S v Zuma* 2006 (2) SACR 191 (W) 199 in Schwikkard & van der Merwe op cit note 3 at 51
[98] *S v Brown* supra note 14 para 20; Hofman & de Jager op cit note 4 at 765 – 770.
[99] See discussion above in paragraph 3.5 above.
[100] For more on unconstitutionally obtained evidence see Schwikkard & van der Merwe op cit note 3 at 198 – 283; Zeffertt & Paizes op cit note 23 at 721 – 736; A Bellengère *et al The Law of Evidence in South Africa* (2013) 292 – 305; see also *S v Brown* supra note 14 para 12 – 14 for a discussion of unconstitutionally obtained evidence in the context of a case dealing with electronic evidence.
[101] *S v Brown* supra note 14 para 14.
[102] 1997 (1) SACR 379 (CC) at para 220.

Further, in In *Gumede v S,*[103] the court found that 's 35(5) requires the court to exclude evidence obtained in a manner that violates any right in the Bill of Rights if either the admission of that evidence will render the trial unfair or otherwise be detrimental to the administration of justice.'[104] The application of s 35(5) is a value judgment that a trial judge is best placed to make on a case-by-case basis, depending on the relevant circumstances and facts.

However, in civil matters, section 35(5) of the Constitution naturally does not apply given that it regulates rights pertaining to arrested, detained and accused persons. At common law, as pointed out in *Harvey v Niland*:[105]

> all relevant evidence [is] admissible in a civil court irrespective of how it was obtained. That rule is not absolute: it is subject to a discretion to exclude unlawfully obtained evidence.

In exercising its discretion to exclude unlawfully obtained evidence, 'all relevant factors must be considered'[106] by a court. In *Harvey*, Niland's right to privacy had been infringed, and the court was tasked with determining whether to exclude the unlawfully obtained evidence. This matter arose in the context of an application to the Eastern Cape Division of the High Court to interdict Niland from breaching fiduciary duties imposed by s 42 of the Close Corporation Act.[107]

Harvey was a former business partner with the Niland, where they operated a hunting and safari guide business. Although the parties ended their business relationship acrimoniously, and they no longer worked together, Niland remained an owner of members interest in the Close Corporation (Huntershill) that was operated by Harvey.

One of Harvey's employees knew Niland's Facebook password – Harvey instructed his employee to access Niland's account unlawfully (this was accepted as a fact by the court) and review his private messages – this conduct was in contravention of section 14 of the Constitution, and section 86 of the ECT Act. However, the evidence revealed that Harvey had no other lawful means to obtain the evidence, and it resulted in him being able to prove that Niland was 'conducting himself in a duplicitous manner contrary to the fiduciary duties he

[103] 2017 (1) SACR 253 (SCA).
[104] See also *Key v Attorney-General, Cape Provincial Division* 1996 (4) SA 187 (CC) para 13.
[105] *Harvey v Niland* supra note 37 para 47 – 53.
[106] Ibid para 47.
[107] Act 69 of 1984.

owed to Huntershill.'[108]The evidence was found to be admissible; the court reasoned as follows:

> [R]ight-thinking members of society would believe that Niland's conduct, particularly in the light of his denials and the undertakings that he gave, ought to be exposed and that he ought not to be allowed to hide behind his expectation of privacy: it has only been invoked, it seems to me, because he had something to hide.

As a result, it is likely that illegally obtained electronic evidence will be more readily admitted in civil matters, as opposed to in criminal matters. However, the final determination must depend on the unique facts of every matter, and be decided on a case-by-case basis.

5.4.3.3 Authentic

Despite providing guidance on how to attribute evidential weight to data messages in s 15(3) of the ECT Act, and on how to assess whether a data message is an original in s 14. The ECT Act is silent on how to authenticate a data message.[109] In *Ndlovu v Minister of Correctional Services*,[110] the court interpreted the requirement of authenticity – in the context of data messages – to mean 'proof that a document was written or executed by the person who purports to have done so'. The court noted:

> I consider the authenticity of the printout to have been proved. Proof that a document was written or executed by the person who purports to have done so could be presented in various ways, such as to call as a witness the author to identify the document, or someone who saw the author sign or write it, or who can identify his handwriting.

In *S v Brown,*[111] in so far as authenticity is concerned, the court adopted a similar approach to *Ndlovu* in that it required expert oral evidence to confirm the authenticity of digital images. The court accepted oral evidence from a Lieutenant Colonel in a technical division of the South African Police Service and noted:

> Applying these requirements [for documentary evidence] to the present matter, the images in question were downloaded from the phone, reproduced in hard copy (paper) form and enlarged. There was no suggestion that either the devices or the software which Linnen [Lieutenant Colonel in a technical division of the South African Police Service] used to produce or enlarge the images was unreliable or that he manipulated the data or electronic communication in any way.

[108] *Harvey v Niland* supra note 37 para 49.
[109] *S v Meyer* supra note 54 para 306. See also Papadopoulos & Snail op cit note 4 at 322 – 323.
[110] *Ndlovu v Minister of Correctional Services* supra note 23 at 174.
[111] *S v Brown* supra note 14 para 19 – 22.

In the context of documentary evidence generally, academic authorities appear ad idem in that authenticity relates to tendering evidence relating to authorship.[112] The document must be what it purports to be, as De Villiers notes, authentication deals with:

> [T]he nature or character of the document… for example, whether it is actually a will, a contract, a death certificate or cash slip. The question about the truth of the contents of the specific document is not an issue at this stage."[113]

In *S v Meyer*,[114] the court quoted with approval guidelines set out by the Irish Law Commission,[115] who noted that authenticity must be established by expert evidence relating to:

> how the document was generated or otherwise brought into existence; on the reliability of the processes and on the accuracy of the electronic systems or devices which were used to store, transmit or generate the document, may be necessary to establish authenticity.

Further, according to the Irish Law Commission, in order to establish authenticity, one should consider:

> whether the secondary media (CD, USB) upon which the information was stored have been damaged or interfered with in any way;
> whether proper record management procedures were in operation;
> whether proper security procedures were in place to prevent the alteration of the information of the information contained in the drive file or secondary storage device prior to the information being reproduced in permanent legible through a printout.

Theophilopoulos points out that the ECT Act does not contain a set of defined criteria for determining authenticity, and notes that this has created confusion. Moreover, that an increasing amount of e-documents are routinely admitted for trial purposes with only 'lip service being paid to the threshold rules of … authenticity'.[116] In *S v Meyer*,[117] the court defined the authenticity requirement as follows:

> Looking at the authenticity requirement we note that it is defined as the capacity to prove the digital object is what it purports to be. It authenticity is preserved by the use of techniques to prevent the data from being manipulated, altered or falsified deliberately or inadvertently

---

[112] Schwikkard & van der Merwe op cit note 3 at 434 – 435; Zeffertt & Paizes op cit note 22 at 837 – 838; Bellengère op cit note 100 at 62; Davey & Dahms-Jansen op cit note 3 at 290.
[113] De Villiers op cit note 4 at 572.
[114] *S v Meyer* supra note 54 para 307.
[115] Irish Law Reform Commission Consultation Paper 'Documentary and Electronic Evidence' (LRC CP 57) December 2009 available at: *http://www.lawreform.ie/_fileupload/consultation%20papers/cpdocumentaryandelectronicevidence.pdf*, accessed on 25 May 2017.
[116] Theophilopoulos op cit note 4 at 466.
[117] *S v Meyer* supra note 54 para 305.

Further, the court provided guidance in so far as authenticating a data message:

> The most common way of proving the authenticity of private documents would be to call the author(s) to identify the documents: The ECT Act does not attempt to enumerate any specific criteria that should be applied, this is due to the fact that there are different types of data messages so it would be difficult to formulate prerequisites for authentication which would apply to all types.

In terms of the threshold requirement for admissibility in so far as authenticity is concerned, what must be established? The common law read together with the case law above answers this: A party must adduce evidence as to the authorship of the data message; together with evidence that speaks to the use of software (and/or manual techniques) that prevent data from being deliberately or mistakenly altered.[118]

Typically, this would entail describing how the data message was created, and giving detail as to who created the data message. This information would usually be supplemented, in order to give a court the full factual matrix, with information as to the reliability of the data message, and how it was stored and/or transmitted, and it how it came to being in paper format in the particular court in question. There is a certain degree of overlap with this enquiry and when one considers whether a data message is original; moreover, there is further overlap with this authenticity requirement and when a court considers what weight to accord evidence. However, the similarity in the two distinct stages of admissibility and weight notwithstanding, each phase must be viewed individually – they should not be conflated into one test. Whether a data message is original or authentic are two separate enquiries. Moreover, whether a data message is authentic on the one hand and what weight to accord the evidence once admitted on the other hand are clearly distinct enquiries as well. As noted in *S v Meyer*: 'evidence is either admitted or not admitted. It should conceptually not be confused with what degree of weight is given to evidence'.[119]

It would be unwise to fetter a judge's discretion with a list of rigid factors to apply when authenticating a data message. South Africa does not operate with a jury system. Cases are presided over by judicial officers who are trained and experienced. These judicial offices are well placed to determine on a case by case basis whether a document is authentic.

Although the factors in s 15(3), read together with the factors set out for establishing originality in s 14 do appear to contain overlap with authenticity, the issues should not be conflated. Authenticity aims to establish whether the document is what it purports to be – in

[118] *S v Meyer* supra note 54 para 305 – 306; Schwikkard & van der Merwe op cit note 3 at 434 – 435; Zeffertt & Paizes op cit note 22 at 837 – 838; Bellengère op cit note 100 at 62; Papadopoulos & Snail op cit note 4 at 322 – 323.
[119] Where the court quotes Schwikkard & van der Merwe op cit note 3 at 20.

order for a court to decide whether a print out of a data message is authentic, it must establish how the data message was created, and who created it. As correctly noted in *S v Meyer*, there are a plethora of possible types of data message that may be at issue – therefore, it is unwise to compile a closed list of factors in attempting to authenticate.[120]

5.4.3.4 Original produced

With traditional paper-based evidence, the production of an original document would often allay fears about manipulation and prove integrity and reliability. Consequently, even in the digital realm – and in order to stay true to functional equivalence principles – the concepts of 'original' and 'produced' are retained in the context of electronic evidence.[121]

In *Ndlovu v Minister of Correctional Services*,[122] the court found that an original must be produced unless s 15(1)(b) applies.[123] Section 15(1)(b) provides that a data message should not be denied admissibility on that basis that it is not in original form – if the evidence is the best evidence[124] reasonably available. This section is essentially a codification of the best evidence rule in the context of data messages.[125]

In *S v Brown*[126] the court explained the section's operation as follows:

> s 15(1)(b) of ECTA gives data messages a further exemption from the requirement of original form 'if it is the best evidence that the person adducing it could reasonably be expected to obtain.

Consequently, the test to determine if s 15(1)(b) applies is an objective one: A court must decide whether the evidence a party seeks to adduce is – reasonably measured – the best a party can obtain in the particular circumstances. These considerations are fluid and will depend on the facts and the practice in the relevant court at the time.

Section 14 of the ECT Act provides direct guidance in so far as originality is concerned, it reads as follows:

> 14 Original

[120] *S v Meyer* supra note 54 para 306. See also discussion of foreign law below in para 5.6.
[121] De Villiers op cit note 4 at 573 – 575.
[122] *Ndlovu v Minister of Correctional Services* supra note 23 at 172.
[123] Van der Merwe et al op cit note 4 at 119 – 120; Davey & Dahms-Jansen op cit note 3 at 291; Papadopoulos & Snail op cit note 4 at 322.
[124] A Kruger *Hiemstra's Criminal Procedure* (2018) 24 – 79 where the author notes that the best evidence rule only applies to traditional documents in practical terms.
[125] Van der Merwe et al op cit note 4 at 119 – 120; 127. For a history of the best evidence rule, see Zeffertt & Paizes op cit note 22 at 381 – 383. See also Schwikkard & van der Merwe op cit note 3 at 432 – 433.
[126] *S v Brown* supra note 14 para 24.

(1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if-

(a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and

(b) that information is capable of being displayed or produced to the person to whom it is to be presented.

(2) For the purposes of subsection 1 *(a)*, the integrity must be assessed-

(a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;

(b) in the light of the purpose for which the information was generated; and

(c) having regard to all other relevant circumstances.

Consequently, in order for a data message to be considered original, its integrity must be assessed, and it must be capable of being displayed or produced.[127] In *Maseti v S*,[128] the Supreme Court of Appeal in the context of a text message from a mobile phone, took a conservative view in the context of data message admissibility and stated:

> Whilst the best evidence rule seems everywhere to be in retreat that does not mean that a court must accept as accurate secondary evidence of a document or other form of writing, such as a text message. The fact that it has been thought necessary to make elaborate provision in a statute for the admissibility in evidence of such messages demonstrates the need for caution in this regard.

Section 14 has been dealt with in a superficial fashion by South Africa's judiciary so far,[129] primarily because it seems that the guidance provided in the section is sufficiently clear as it stands.

In so far as production is concerned,[130] s 17[131] facilitates the use of data messages as a document: As pointed out above, for the most part data messages are reduced to paper form for presentation purposes in court, and s 17 has not, in my experience, and based on the case law

[127] Papadopoulos & Snail op cit note 4 at 322 – 323.
[128] *Maseti v S* supra note 11.
[129] *Maseti v S* supra note 11 para 33; *Makate v Vodacom* (Pty) Ltd 2014 (1) SA 191 (GSJ) para 38; S v *Meyer* supra note 54 para 302.
[130] Papadopoulos & Snail op cit note 4 at 322.
[131] Van der Merwe et al op cit note 4 at 121 – 122.

above, been relied upon in any instances thus far – with the exception of *S v Meyer*,[132] where a court dealt with s 17 for this first time and noted:

> The use of data messages as documents is permitted by Section 17(1) provided that certain conditions are met namely: that the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document S17(1)(a); and that it was reasonable to expect that the information contained in the data message would be readily accessible so as to be usable for subsequent reference S17(1)(b).

Consequently, s 17 allows the use of a data message as a document if two conditions are met: the first condition has two parts – a) the data message must be reliable, and b) the integrity of information in the document must have been maintained. In addition, the second requirement provides that when a data message was sent, it must have been reasonable to expect that information contained therein would be accessible and useable – this is to ensure that that data is actually readable and can be relied upon for future use. In the circumstances, where the law requires the production of a document, s 17 facilitates the use of data messages should that be required.

5.4.4 Law Reform Commission proposals on printouts and the Best Evidence Rule

The SALRC[133] suggest law reform is required and state as follows:

> Given that in most cases (at least in the short to medium term) so-called electronic evidence will be produced in court in the form of a printout, it may be prudent to clarify the position on printouts, and on the best evidence rule more generally.

In order to address the perceived shortcomings with the current legal position, the SALRC proposes a comprehensive *Law of Evidence Bill*;[134] in this context, the proposed definitions read as follows:

> 'Copy' in relation to a document, means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly, and regardless of how many removes from the original;

---

[132] *S v Meyer* supra note 54.
[133] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 29.
[134] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 29 – 30 and Annexure A.

> 'Document' means anything in which information of any description is recorded, and includes a copy;
>
> 'Electronic document' means data that is recorded or stored on any medium in or by a computer system or other similar device that can be read or perceived by a person and includes a display, printout or other output of that data;

Although comprehensive law reform would certainly clarify certain aspects in relation to electronic evidence, my view is that s 15 – read together with the common law and the data message admissibility cases discussed above – adequately regulates the legal position in the short to medium term.[135] Moreover, as pointed out by Mason:[136]

> rather than question whether a document in digital form is an original or a copy, it might be more useful and relevant to refer to the proof of authenticity, or provenance, or reliability of a digital file…
>
> This in turn encapsulates proof of the integrity of the content of the data. Because of the ease in which a digital document may be migrated from one storage device to another, and undergo format and other changes, including content and metadata changes, it is vital to require any such changes to be documented in such a way as to preserve the integrity and authenticity of the copy.
>
> Thus it might be more relevant, when referring to digital data, to concentrate on establishing which version of the data is required, particularly whether the making of copies of the digital document is properly documented.

5.4.5 Admissibility of data messages as real evidence

As discussed above in chapter 3, real evidence consists of material objects that are in and of themselves evidence.[137] Can data messages be classified as real evidence?[138]

In *Ex Parte Rosch,*[139] an appeal matter heard prior to the promulgation of the ECT Act, the court found that computer generated evidence should be regarded as real evidence if produced automatically, and with no human input. In deciding that evidence relating to

---

[135] However, law reform is desirable in the following areas: definition of data message; definition of document in the statutes applicable to hearsay exceptions; a distinction between types of electronic evidence created with human intervention, and without human intervention; more cohesion and alignment with the statutory exceptions dealing with documents and hearsay; and amendment of procedural court rules relating to discovery to take account of data messages and their characteristics (metadata).

[136] S Mason & D Seng 'Foundations of evidence in electronic form' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 57.

[137] *S v Gumede* 2017 (1) SACR 253 (SCA) para 32 where the court refers to a firearm as real evidence. See also what appears to be the *locus classicus* when describing real evidence: *S v M* 2002 (2) SACR 411 (SCA) para 31.

[138] As real evidence data messages are not subject to hearsay considerations. See, however, D Bilchitz 'Law of Evidence' in C Lewis et al (eds) *Annual Survey of South African Law* (1998) 735 – 821. See also the views of American jurist Teppler in S Mason 'Software code as the witness' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 88.

[139] *Ex Parte Rosch* [1998] 1 All SA 319 (W).

software that automatically registers the numbers, time, date, length of phone call, was admissible as evidence, the court found as follows:

> The printout is *real evidence in the sense that it came about automatically* and not as result of any input of information by a human being. There is therefore no room for dishonesty or human error… Chronologically the world is approaching the 21st century. Many gadgets have been invented which are capable of automatically recording material facts without human agency. Courts in this country as well as England have recognised that evidence produced by such gadgets is prima facie accurate. This accords with reality and common experience. [my emphasis]

Following *Ex Parte Rosch*, some criticism suggested that as all computer systems rely on natural persons to enable, disable, program, etcetera, all computer evidence is hearsay without evidence from the person who is responsible for the technology.[140] In *S v Ndiki,*[141] the court confirmed that data messages can be classified as real evidence, depending on the function performed by technology, and held as follows:

> it is not desirable to attempt to deal with computer print-outs as documentary evidence simply by having regard to the general characteristics of a computer. It is an issue that must be determined on the facts of each case having regard to what it is that the party concerned wishes to prove with the document, the contents thereof, the function performed by the computer and the requirements of the relevant section relied upon for the admission of the document in question.

Further, in *Ndlovu v Minister of Correctional Services*,[142] the court found that data messages can be either real evidence or documentary evidence, depending on the nature of the evidence, and its purpose, by holding as follows:

> Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving the 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 (because information was processed by the computer), section 3 of the Law of Evidence Amendment Act 45 of 1988 will not apply.

In *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd*,[143] in a dispute over outstanding monies in relation to mobile telephones and mobile telephone services, the court found that data messages can be classified as real evidence if 'the probative value…depends on the reliability and accuracy' of a computer system.[144] As noted by Theophilopoulos:[145]

---

[140] Bilchitz op cit note 138 at 735 – 821.
[141] *S v Ndiki* supra note 31 para 33.
[142] *Ndlovu v Minister of Correctional Services* supra note 23 at 172.
[143] *La Consortium* supra note 31.
[144] Ibid para 16.
[145] Theophilopoulos op cit note 4 at 474, see footnote 31. See also discussion on real evidence in context of data messages in Hofman op cit note 25 at 268 – 269.

> 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.

In in *S v Brown,*[146] however, the court quoted with approval a cautionary note from Hofman who submits that audio, video and graphics should be treated the same as documentary evidence, he stated:

> To be admitted real evidence only has to be relevant and meaningful. This view is conceptually simple and appeals to those who dislike excluding any evidence. But it does not take account of the way graphics, audio and video are, to an ever-increasing extent, recorded, stored and distributed in digital form and fall under the definition of a data message. This means that graphics, audio, and video now resemble documents more than the knife and bullet that are the traditional examples of real evidence. In data message form, graphics, audio and video are susceptible to error and falsification in the same way as data messages that embody documentary content. They cannot prove themselves to be anything other than data messages and their evidential value depends on witnesses who can both interpret them and establish their relevance.

Zeffertt shares this view,[147] citing *S v Ramgobin*[148] in support thereof. The justification being that data messages should be treated as documents to guard against intentional or accidental changes to the data message.[149] In *S v Brown,*[150] the court supported this proposition and held that digital images more closely resemble documents, and found as follows:

> Given the potential mutability and transient nature of images such as the images in this matter which are generated, stored and transmitted by an electronic device, I consider that they are more appropriately dealt with as documentary evidence rather than 'real evidence'.

Those views notwithstanding, the treatment of data messages as real evidence is consistent with similar common law based foreign jurisdictions – where electronic evidence has had more time to mature judicially; for example, the United Kingdom, Canada, and the United States.[151] For example, as discussed above in chapter 3, in England, it has been suggested that records generated by software without any input from a human should be treated as real evidence.[152] In *R v Coventry Justices*,[153] automated transactions that involved pornography purchases from

[146] *S v Brown* supra note 14 para 18.
[147] Zeffertt & Paizes op cit note 22 at 852.
[148] 1986 (4) SA 117 (N).
[149] Hofman op cit note 25 at 268.
[150] *S v Brown* supra note 14 para 18.
[151] S Mason 'Software code as the witness' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 91 – 100.
[152] Ibid 97 – 98.
[153] [2004] All ER (D) 78.

a credit card were regarded as real evidence. Further, in *R v Spiby*,[154] where an automated program monitored telephone calls this evidence was real evidence because there was no human intervention in the production of the data (similar to the South African decision of *Ex Parte Rosch*[155] discussed above).

In the seminal American decision, in *Lorraine v Markel American Insurance Company*,[156] the court held that where an 'electronically generated record is entirely the product of the functioning of a computerized system or process'[157] it cannot constitute hearsay. In what has been described as the 'watershed opinion'[158] in relation to electronic evidence, the court set out the basic requirements for the admissibility of electronic evidence. In legal proceedings instituted to enforce an arbitrators award, it was found that:

> In order for electronically stored information (ESI) to be admissible, it must be (1) relevant, (2) authentic, (3) not hearsay or admissible under an exception to rule barring hearsay evidence, (4) original or duplicate, or admissible as secondary evidence to prove its contents, and (5) probative value must outweigh its prejudicial effect. [159]

Further, in *United States v Lizarraga-Tirado*,[160] the Ninth Circuit Court of Appeals found that automated computer evidence – without any substantial human intervention is not hearsay. The court stated as follows: 'we join other circuits that have held that machine statements aren't hearsay'.[161]

Data messages can be treated as real evidence if a court is satisfied that the data message in question is generated automatically without human input – put in the terminology used by recent South African cases: If the data message depends substantially upon the credibility of the technology concerned.[162]

What are the admissibility requirements for real data messages? At common law, the only requirement for real evidence to be admissible is that it is relevant.[163]

---

[154] [1990] 91 Cr App R 186.
[155] *Ex Parte Rosch* supra note 139.
[156] *Lorraine v Markel American Insurance Company* 241 FRD 534 (2007).
[157] Ibid 564.
[158] *Tienda v State* 358 SW3d 633 Texas Criminal Appeal (2012) 639.
[159] Ibid 538.
[160] *United States v Lizarraga-Tirado* 2015 WL 3772772 9th Circuit (2015).
[161] Ibid 7 – 8.
[162] *S v Ndiki* supra note 31; *S v Fuhri* 1994 (2) SACR 829 (A) 835; *Ndlovu v Minister of Correctional Services* supra note 23; *La Consortium* supra note 31; *Ex parte Rosch* supra note 139.
[163] Hofman & de Jager op cit note 4 at 776 – 777; Hofman op cit note 25 at 268. For an English perspective, see S Mason & D Seng 'Real Evidence' in S Mason and D Seng (eds) *Electronic Evidence* 4 ed (2017) 39.

However, as discussed above in chapter 3,[164] in the context of graphics, audio and video, there is some debate as to how the evidence should be classified. In *Motata v Nair NO*[165] the court cogently summarised the various approaches as follows:

> There has been considerable judicial debate concerning the prerequisites for admissibility in evidence of video and tape recordings. Ranged against the decisions in the Natal Provincial Division in the cases, in particular, of *S v Singh & another* 1975 (1) SA 330 (N), and *S v Ramgobin & others* 1986 (4) SA 117 (N) are the decisions in the Transvaal Provincial Division, in particular, in *S v Baleka & others (1)* 1986 (4) SA 192 (T) and *S v Baleka & others (3)* 1986 (4) SA 1005 (T), in which latter cases the *Singh* and *Ramgobin* decisions were expressly disapproved of. See too *S v Mpumlo* & others 1986 (3) SA 485 (E). In *S v Nieuwoudt* 1990 (4) SA 217 (A) Hefer JA pointed out that the difference in approach between these cases came down to the question of whether proof of the authenticity of a recording tendered in evidence was a prerequisite for admissibility. Whereas in the *Singh* and *Ramgobin* cases it was held that it was indeed a prerequisite, the contrary was held in the *Baleka* cases on the grounds that a distinction must be drawn between the originality of a recording and the authenticity thereof, Van Dijkhorst J stating that, whereas originality affected admissibility, authenticity did not.

In the context of data messages generally, the difference in approach can be summarised further as follows: the KwaZulu-Natal *Singh* and *Ramgobin* decisions require relevance *and* authenticity for admissibility, whereas according to the Gauteng *Baleka* cases authenticity is an issue to consider when considering the weight of evidence. Moreover, the *Baleka* cases believe that originality affects admissibility, and should be considered as part of an admissibility enquiry.

In *S v Nieuwoudt,*[166] and in S v *Fuhri,*[167] it was held that the approach in the Gauteng *Baleka* cases should be preferred. However, in *S v Koralev*,[168] although the court appears to endorse the *Baleka* cases, what in effect it does is endorse the KwaZulu-Natal *Singh* and *Ramgobin* approach because, according to the court's rationale, digital images must not only be relevant, but also *corroborated*; the court held as follows:

> Before the images in question could be admissible in evidence against the appellants there had to be some proof of their accuracy in the form of corroboration that the events depicted therein actually occurred; and
>
> Corroboration in the sense required must be found in some independent source of evidence, which makes the evidence constituted by the images in the photographs and video recordings more acceptable in that it supports an aspect or aspects thereof.[169]

[164] See paragraph 3.4.
[165] 2009 (1) SACR 263 (T) para 21.
[166] 1990 (4) SA 217 (A).
[167] 1994 (2) SACR 829 (A).
[168] 2006 (2) SACR 298 (N).
[169] Ibid 306 – 307.

In the direct context of data messages and real evidence, the Supreme Court of Appeal and/or Constitutional Court is yet to decisively adjudicate on the matter. The issue that remains unclear relates to the admissibility of real evidence in the form of data messages. On the one hand, in matters that follow the logic of the Gauteng *Baleka* cases, and the Appeal Court in *Fuhri*, real evidence in the form of a data message need only be relevant in order for it to be admissible. Conversely, on the basis of *Koralev, Singh* and *Ramgobin's* rationale, real evidence in the form of a data message must be relevant *and authentic*.

Given the nature[170] of electronic evidence, it may well be desirable for a court to be sure the data message is authentic before considering that evidence admissible. It follows logically that to be relevant, the data message evidence must be authentic – consequently, as was found in *Tienda v State*, evidence has no relevance if it is not authentically what its proponent claims it to be.[171]

5.5 EVIDENTIAL WEIGHT OF DATA MESSAGES

5.5.1 Section 15(2) of the ECT Act

Section 15(2) reads as follows: 'Information in the form of a data message must be given due evidential weight'.[172] The section speaks for itself and enjoins a court to give due evidential weight to a data message.[173] This section ensures that evidence will never be excluded for the sole reason it is not created by a person, and to ensure electronic evidence is *potentially* admissible. Section 15(2) is based verbatim on a portion of art 9(2) of the Model Law, 1996 and is consistent with the legal position globally (where information in electronic format is given due evidential weight).[174]

5.5.2 Section 15(3) of the ECT Act

Section 15(3) of the ECT Act[175] provides direct guidance on evidential weight of data messages, and reads as follows:

---

[170] *S v Brown* supra note 14 para 20; South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7 – 13 for a discussion on some of the difficulties with electronic evidence, including: ease of manipulation, difficulty of detecting manipulation, changing technology and evolving software and hardware. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 27 – 46.
[171] *Tienda v State* supra note 153 at 638.
[172] *La Consortium* supra note 31 para 19.
[173] Papadopoulos & Snail op cit note 4 at 322 – 323; Davey & Dahms-Jansen op cit note 3 at 287 – 296.
[174] See the discussion on the foreign position in para 5.6 below.
[175] Based on art 9 of the Model Law, 1996.

(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.

In *S v Meyer*,[176] the court explained the operation of s 15(2) and s 15(3) of the ECT Act as follows:

> Only once a data message is admitted into evidence, it must be given the due evidential weight in terms of s15(2) of the ECT Act. In assessing the evidential weight of a data message, regard must be had to the reliability of the process of generation, storage and communication of the data, of the preservation of integrity, of the identification of the originator (proof of authenticity and any other relevant factor (s 15 (3))

In *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd*[177] the court applied s 15(2) and s 15(3) of the ECT Act to find accounting software evidence was admissible:

> A data message must, according to s 15(2) of the ECT Act, be given 'due evidential weight'. In assessing the evidential weight of a data message, s 15(3) requires that regard must be had to the manner in which it was generated, stored or communicated; the reliability of the manner in which its integrity was maintained; the manner in which its originator was identified; and any other relevant factor.

The primary guidance in so far as evidentiary weight of data messages is concerned is found is s 15(3) of the ECT Act. In addition, the factors contained in s 14(2), which deals with assessing integrity, can also be considered – but this really adds nothing new.[178]

In *S v Ndiki*[179] the court found that where there are doubts as to the accuracy of the technology in question, these concerns should be reflected in the weight a court accords the evidence – ultimately, the final decision as to the weight evidence receives in particular circumstances is down to the discretion of the judicial officer in question. Watney[180] and Hofman[181] point out that it is likely a court will rely on expert evidence when assessing evidential weight – although each judicial officer must clearly retain a discretion in making a

[176] *S v Meyer* supra note 54 para 308. See also *S v Miller* supra note 31.
[177] *La Consortium* supra note 31.
[178] Hofman & de Jager op cit note 4 at 781.
[179] *S v Ndiki* supra note 23.
[180] Watney op cit note 10 at 10.
[181] Hofman op cit note 25 at 269.

final decision. For example, in *Jafta v Ezemvelo KZN Wildlife*,[182] in one of the first reported decisions dealing with the ECT Act, the court relied on expert evidence to determine issues relating to the conclusion of a contract via data message.

5.5.3 Data message evidentiary weight: South African law reform proposals

In the context of evidentiary weight, the SALRC ask whether s 15(3) is sufficient:

> [W]hether these guidelines for evidential weight are adequate to guide parties and the courts when addressing issues of admissibility, authentication or reliability; or whether additional guidance should be provided?[183]

On evidentiary weight, advocate Eiselen in a response to the SALRC's 2010 issue paper[184] notes: '15(3) provides clear guidance, and... this is an issue that should be considered on a case by case basis rather than by tying the courts' hands'.[185] The Law Society of South Africa, also in response to the SALRC's 2010 issue paper, notes that the current statutory regime in the context of evidentiary weight is adequate and points out that a court should retain discretion to test the authenticity of evidence as it deems appropriate.[186] Heyink, similarly, cautioned against fettering the discretion of judicial officers,[187] while the NPA noted that the current position is satisfactory and that authenticity should not be conflated with truth of the contents.[188] In my view, in so far as evidentiary weight is concerned, the current position is satisfactory for the short to medium term, and a court or tribunal has sufficient guidance in the ECT Act.

[182] (2009) 30 ILJ 131 (LC) para 17 – 29 where experts from both sides produced a substantially agreed set of facts regarding e-mail usage and Google Mail.
[183] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 72.
[184] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 28 – 49.
[185] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 72.
[186] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 72.
[187] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 73.
[188] Ibid.

5.6. COMPARATIVE POSITION IN FOREIGN LAW

5.6.1 United Kingdom

Although South Africa's law of evidence is based on English law, it is worth noting the primary distinction between the two legal systems: In England and Wales, criminal matters are determined by a jury[189] (unless the offence is deemed minor), whereas in South Africa all matters are determined by a judge or magistrate (a trained legal expert). However, that distinction aside, the systems of evidence are remarkably similar. As with South Africa, evidence is primarily considered admissible if relevant – subject to several exclusions.[190] In England and Wales, weight and sufficiency of evidence is largely left to the jury to decide, unless it is a matter with no jury, in which case, the judicial officer will decide.[191] A clear distinction is drawn between admissibility and weight of evidence: [192]

> Questions concerning the admissibility of evidence must be distinguished from those relating to its weight. The former is a matter of law for the judge; the weight of evidence, on the other hand, is a question of fact.

In the context of electronic evidence, to be admissible, it must be authentic.[193] Authentic means 'the record is what it claims to be'.[194] Mason and Stanfield note:[195]

> Each case is necessarily considered on its merits, and in the case of authenticating electronic evidence, there is very little clear guidance on how to determine authenticity, since traditional rules look at individual documents rather than the digital system in which digital data are created.

According to Mason and Stanfield,[196] challenges to authenticity include:

1. Claiming that records were altered, manipulated or damaged between the time they were created and the time they appeared in court as evidence.
2. Questioning the reliability of the program that generated the record.
3. Disputing the identity of the author of the electronic evidence: for instance, the person ostensibly responsible for writing a letter in the form of a word processing file, SMS or email

---

[189] C Tapper *Cross and Tapper on Evidence* 12 ed (2010) at 6.
[190] S Mason & D Seng 'Foundations of evidence in electronic form' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 57.
[191] Mason & Seng op cit note 190 at 58. At times, South Africa's exclusionary rules (designed to protect a jury from hearing prejudicial evidence) appear outdated when one considers a jury system has long since been abolished in South Africa, and that the trier of fact in a South African context will invariably be a trained legal expert working within the conscripts of a Constitutional democracy.
[192] Tapper op cit note 189.
[193] D Seng 'Computer output as evidence' (1997) *Singapore Journal of Legal Studies* 161 – 163.
[194] S Mason & A Stanfield 'Authenticating electronic evidence' in S Mason & D Seng (eds) *Electronic Evidence* 4 ed (2017) 193.
[195] Ibid 193 – 194.
[196] Mason & Stanfield op cit note 194 at 196 – 197.

may dispute he wrote the text, or sufficient evidence has not been adduced to demonstrate the nexus between the evidence and the person responsible for writing the communication.
4. Questioning the reliability of the evidence from a social networking website.
5. Even if it might be agreed that an act was carried out and recorded in an electronic message, failing to prove the message was directed to a particular person, especially where others might have access to the device (such as a mobile telephone) that produced the message.
6. Questioning whether the person alleged to have used his PIN, password or clicked the 'I accept' icon was the person who actually carried out the action.

In *Nobel Resources SA v Gross*[197] the court relied on expert evidence to determine the authenticity of electronic evidence – in this case, SMS messages sent to a Blackberry mobile phone, the court held:

> Prior to the start of the trial Mr. Gross attempted to cast doubt on the reliability or authenticity of the SMS evidence. However the technical evidence subsequently served by Noble explaining: (a) how the SMS messages were identified and recovered; (b) that it was not possible to alter an SMS message on a BlackBerry once it has been received or sent; and (c) that it would be very difficult to alter data on a server back-up, meant that when it came to trial there was no realistic attack by Mr. Gross on the reliability or authenticity of the SMS messages or any suggestion to the effect that they had been doctored or deleted.

Electronic evidence has become a natural part of most trials; in the recent criminal appeal of *Khan v R*,[198] for example, the court was required to consider Blackberry messages, Facebook messages, and Instagram messages when coming to a decision. Moreover, in *Kay v R*,[199] the basis of the appeal was again evidence from social media – the conviction was ultimately quashed, and the court noted:

> Fresh evidence in the form of Facebook messages are now available that go directly to A's credibility. Edited and misleading copies of the Facebook messages were adduced at trial.[200]

Kay v R shows the inherent danger of electronic evidence where it is relied upon without proper authentication. In the court *a quo* the accused was convicted – the conviction was based, in no small part, on inaccurate and misleading Facebook messages. Often, electronic evidence will be decisive – for example, in *Burns v R*,[201] in the context of stirring up racial hatred on Facebook, the key evidence was electronic in nature; the court had to consider offensive comments directed at the Afro-Caribbean and Jewish communities posted on Facebook, and the appropriateness of the sentence imposed.[202]

---

[197] [2009] EWHC 1435 (Comm) para 60. See discussion in Mason & Stanfield op cit note 194 at 196.
[198] [2015] EWCA Crim 1816 para 9.
[199] [2017] EWCA Crim 2214.
[200] Ibid para 20.
[201] [2017] EWCA Crim 1466.
[202] Ibid para 2 – 7. See also *R v Sheppard and Whittle* [2010] EWCA Crim 65 in the context of where publication takes place where servers are hosted outside of the jurisdiction in question.

What considerations should be taken into account when authenticating data? This will very much depend on the electronic evidence in question, the statute being relied upon for admissibility, and no rigid hard-and-fast rules should exist. Mason and Stanfield note:[203]

> The tests of authenticity for digital data…will vary, depending on the source and type of the data. Lawyers must look to the digital forensic professionals for guidance. For instance, the print-out from a mainframe computer will demand a different approach in comparison to the data held on a personal computer; this in turn will be different if data is stored with a cloud service provider.

5.6.2 United States

Electronic evidence, and machine output in particular has been at issue in legal proceedings for many years in the United States, and has been actively discussed for decades.[204] Although a 'machine does not exhibit a character for dishonesty or suffer from memory loss',[205] the conveyances[206] cannot always be trusted – even if a machine generated the result without any apparent human involvement. Roth notes:

> a machine's programming, whether the result of human coding or machine learning, could cause it to utter a falsehood by design. A machine's output could be imprecise or ambiguous because of human error at the programming, input, or operation stage, or because of machine error due to degradation and environmental forces. And human and machine errors at any of these stages could also lead a machine to misanalyze an event.

However, machine learning (and technology in general) has advanced to a sophisticated state, and can be relied upon:

> machine learning algorithms are used to detect patterns in data in order to automate complex tasks or make predictions. Today, such algorithms are used in a variety of real-world commercial applications including Internet search results, facial recognition, fraud detection, and data mining. Machine learning is closely associated with the larger enterprise of "predictive analytics" as researchers often employ machine learning methods to analyze existing data to predict the likelihood of uncertain outcomes.[207]

---

[203] Mason & Stanfield op cit note 194 at 193 – 194.
[204] The Harvard Law Review Association 'Scientific Gadgets in the Law of Evidence' (1939) 53 *Harvard Law Review* 285 – 296 where the authors discuss breathalysers, blood tests, polygraphs and photographs, quoted in A Roth 'Trial by Machine' (2016) 104 *Georgetown Law Journal* 1253.
[205] A Roth 'Machine Testimony' (2017) 126 *Yale Law Journal* 1972 – 2259.
[206] The term conveyances is used to denote output. See Roth op cit note 205 at 1976.
[207] H Surden 'Machine Learning and Law' (2014) 89 *Washington Law Review* 89 – 95. See also R Susskind 'Tomorrow's Lawyers An Introduction to the Future' 2 ed (2017) 1 – 10.

Some point out that this type of evidence should be 'subject to a heightened showing of reliability and testability'.[208] Teppler notes:[209]

> Digital data is inherently malleable or mutable. The inherently mutable nature of computer-generated data creates new issues that have a significant and detrimental effect on reliability, authentication, and ultimately on the issue of admissibility. This mutability, in turn, exposes the inherent frailty of digital data sought to be introduced as evidence.

In *Perfect 10 Inc v Cybernet Ventures Inc*[210] the court noted the position in so far as authentication of electronic evidence is concerned: '[T]he foundational requirement of authentication is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims'.[211] In *re FP*,[212] the court confirmed that admission of evidence is in the discretion of the judicial officer, and that a wide variety of methods may be used to authenticate electronic evidence.[213]

In *Tienda v State*,[214] in a criminal appeal, the court took a common sense approach in finding that there is no specific procedure applicable when authenticating electronic evidence – best practice and procedure is very much dependant on the nature of the evidence. In *Tienda*, the appellant was convicted of murder in what appeared to be a gang related shooting involving three moving vehicles on a major highway. On appeal, the court found that the trial court did not misdirect itself, nor did it abuse its discretion in admitting social media posts from *MySpace* as evidence. The posts in question appeared incriminating and seemingly boasted about a gang shooting with a direct reference to the deceased in question: 'You aint BLASTIN You aint Lastin; I live to stay fresh!!; I kill to stay rich!!' – all made under the heading 'RIP David Valadez'. In so far as authentication is concerned, the court noted as follows:

> Evidence may be authenticated in a number of ways, including by direct testimony from a witness with personal knowledge, by comparison with other authenticated evidence, or by circumstantial evidence. Courts and legal commentators have reached a virtual consensus that, although rapidly developing electronic communications technology often presents new and protean issues with respect to the admissibility of electronically generated, transmitted and/or stored information, including information found on social networking web sites, the rules of evidence already in place for determining authenticity are at least generally adequate to the task.[215]

---

[208] S Teppler 'Testable Reliability: A Modernized Approach to ESI Admissibility' (2014) 12 *Ave Maria Law Rev* 213.
[209] Ibid 217.
[210] 213 F. Supp. 2d 1146 (C.D. Cal. 2002).
[211] Ibid 1154.
[212] 878 A.2d 91 (2005).
[213] Ibid 92. See also the *locus classicus* American case: *Lorraine v Markel* supra note 156 at 539 – 540.
[214] *Tienda v State* supra note 158.
[215] *Tienda v State* supra note 158 at 638 – 639.

As with South Africa, the bedrock admissibility requirement in the United States is relevance.[216] In order to be relevant, the evidence must be authentic – it follows then that evidence has no relevance if it is not authentic.[217] It is submitted that although differences exist, American jurisprudence[218] can assist in unlocking some of the debate surrounding classification and treatment of real data message evidence in South Africa.[219]

For example, courts in South Africa must categorically reject the notion that all electronic evidence is hearsay.[220] Further, it should be a requirement that all electronic evidence is authentic before it is admissible.[221] Consequently, as with the United States – which requires a 'prima facie showing of authenticity'[222] before evidence is admissible – South Africa ought to confirm the KwaZulu-Natal *Singh* and *Ramgobin* rationales, which require relevance *and* authenticity for admissibility.[223] Conversely, according to the Gauteng cases via *Baleka (1)* and *Baleka (3)* (and supported by two appeal decisions), authenticity is an issue to consider when considering the weight of evidence. Moreover, the *Baleka* cases believe that originality affects admissibility, and should be considered as part of an admissibility enquiry.

In the digital context, originality is not a relevant consideration – an 'original' is not a concept that assists with determining the veracity of the evidence (as *is* the case with paper documents). Rather, the key factor must be authenticity, and determining whether the evidence is otherwise admissible. As a result, the proposition that authenticity should only be considered with determining weight of evidence is flawed when considering electronic evidence – manipulation of data and determining authenticity is critical, not considering whether data is original. Accordingly, South Africa's appeal court, when it gets the opportunity, should reject an approach which categorises all electronic evidence as hearsay, and should further find that all

---

[216] *Tienda v State* supra note 158 at 638. See also See also the plaintiff's brief regarding admissibility of electronic evidence in *Van Dusen v Alcurt Landings LLC* 2011 WL 530834 (Texas District) where admissibility and authenticity are discussed.
[217] *Tienda v State* supra note 158 at 638.
[218] See *Lorraine v Markel* supra note 156 at 538 – 539.
[219] See discussion on real electronic evidence at para 3.4 above. See also *Motata v Nair NO* 2009 (1) SACR 263 (T) para 21 which summarises the differing schools of thought in the South African judiciary. See further Schwikkard & van der Merwe op cit note 3 at 426 – 427.
[220] See chapter 2 note 118 above.
[221] See chapter 3, paragraph 3.5, footnote 95 above.
[222] *Lorraine v Markel* supra note 156 at 541 – 542 where the court noted: 'In order for ESI [electronically stored information] to be admissible, it also must be shown to be authentic.' See also *Tienda v State* supra note 159 at 638 where the court noted 'evidence has no relevance if it is not authentic.'
[223] Ibid.

electronic evidence must be authenticated (whether real or documentary evidence) before it is admissible. Further, there must also be recognition that electronic evidence is subject to the same evidentiary regime as all other evidence – it is not automatically admissible.[224] Finally, South Africa's appeal court should note the distinction between automatically produced electronic evidence (real evidence – which is not subject to the hearsay rules), and documentary electronic evidence (which is subject to the hearsay rules).[225]

5.7 SECTION 15(4)[226] OF THE ECT ACT AND BUSINESS RECORDS

In the context of admissibility of electronic evidence, s 15(4) creates a statutory exemption for data messages where the data message is created in a business context; and certified to be correct – a so-called *business records* or *shopbook* exception.[227] The section is a departure from the Model Law, 1996[228] and has been criticized by courts[229] and academics.[230] That notwithstanding, in *Director of Public Prosecution v Modise*,[231] Lamont J seemed to indicate that section 15(4) is an intentional step by South Africa's legislature to foster efficiency and properly deploy limited resources:[232]

> [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.[233]

---

[224] See chapter 5, paragraph 5.4.2 above.
[225] See chapter 5, paragraph 5.4.5 above.
[226] Section 15 (4) is discussed above in para 3.5.4 in the context of hearsay evidence where the section appears in full. It is discussed here in the context of data message admissibility in general for the sake of completeness.
[227] M Takombe 'The rise of the machines – understanding electronic evidence' *De Rebus* August 2014 at 153 – 155.
[228] Hofman & de Jager op cit note 4 at 771 – 772.
[229] *LA Consortium* supra note 31 para 12.
[230] Hofman op cit note 25 at 268; D De Villiers 'Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)' (2010) 4 *TSAR* 733 – 734; Hofman & de Jager op cit note 4 at 771 – 772.
[231] *Director of Public Prosecution v Modise* supra note 82. See also *Sublime Technologies (Pty) Ltd v Jonker* 2010 (2) SA 522 (SCA) para 13 where the section is superficially referred to.
[232] See A Duvenhage *An evidential analysis of section 15 (4) of the Electronic Communications and Transactions Act 25 of 2002* (LLM thesis, University of Pretoria, 2016) 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.
[233] *Director of Public Prosecution v Modise* supra note 82 at 557.

Section 15(4)[234] is in addition to the existing statutory exceptions created for business records and hearsay in: Section 34 of the Civil Proceedings Evidence Act 25 of 1965; s 221 – 222 of the Criminal Procedure Act 51 of 1977; and s 3 of the Law of Evidence Amendment Act 45 of 1988.

The current application of s 15(4) is as follows: If a data message is reduced to a print-out (if created during a business context), then if that copy of the data message is certified to be correct by a person in the service of that business, that printout is admissible in evidence, and rebuttable proof of the facts contained therein.[235]

5.8 CONCLUSION

The admissibility and weight of data message evidence does not require drastic overhaul.[236] Common law principles – read together with the ECT Act, and recent case law – are largely adequate for the time being.

Section 15(1) deals with admissibility, while s 15(2) and s 15(3) provide guidance in so far as assessing evidential weight is concerned; finally, s 15(4) creates a further statutory exception to the hearsay rule by introducing an exception for business records. These sections ensure electronically stored and produced information will be admissible in evidence, and that it should be accorded appropriate evidential weight. These provisions are based on the Model Law, 1996 which has been implemented in one hundred and fifty jurisdictions world-wide.[237] South Africa's common law of evidence, read together with the ECT Act is largely consistent with global best practice, and unless there are cogent reasons to repeal and amend s 15, for the short to medium term, the section should remain unamended.

South Africa ought to ensure that new forms of technology remain admissible in evidence, and that when assessing admissibility and weight of evidence – whether electronic or otherwise – the judiciary should retain a discretion, rather than over legislating or adopting a rigid, tick-box approach. Currently, s 15 achieves the desired result and although reform may be required

---

[234] On s 15(4) of the ECT Act, see Duvenhage op cit note 221 9 – 34. See also P Fourie *Using Social Media as Evidence in South African Courts* (LLM thesis, North-West University, 2016) 8 – 14.

[235] See the cases and discussion above in paragraph 3.5.4.

[236] However, as noted above, law reform is desirable in at least the following areas: The definition of data message; definition of document in the statutes applicable to hearsay exceptions; a distinction between types of electronic evidence in so far as computer-generated evidence with human intervention, and without human intervention is concerned; and more cohesion and alignment with the statutory exceptions.

[237] United Nations 'Status: UNCITRAL Model Law on Electronic Commerce (1996)' *http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html*, accessed on 4 August 2018 where the United Nations Secretariat lists member states that comply with the Model Law, 1996.

in the greater scheme of the ECT Act and electronic evidence, s 15 of the ECT Act is adequate to regulate the admissibility and weight of electronic evidence.

ARE THERE DIFFERENT EVIDENTIARY CONSIDERATIONS APPLICABLE TO DATA MESSAGE EVIDENCE IN CIVIL AND CRIMINAL PROCEEDINGS?

CHAPTER 6

6.1 INTRODUCTION

This chapter seeks to determine whether it is appropriate to apply different evidentiary considerations to data messages in civil and criminal proceedings. It may well be trite, but in order to appropriately discuss this issue it is worth repeating the fundamental distinction in South Africa's legal system: in criminal matters, guilt must be proved *beyond reasonable doubt*; and a court will presume an accused person is *innocent* until the state proves otherwise.[1] Conversely, in civil matters, there is no presumption of innocence;[2] and a litigant must satisfy a court of *on a balance of probabilities*. When discussing these concepts, the key terms that arise are: onus of proof, evidentiary burden, and 'shifting' of the onus of proof. These terms will be analysed in the context of data messages, and this chapter will comment on whether different evidentiary considerations should apply to electronic evidence in civil and criminal proceedings.[3]

6.2 ONUS OF PROOF AND EVIDENTIARY BURDEN

The onus of proof (sometimes referred to as the burden of proof) is a legal expression used to describe the duty on a litigant to satisfy a court that he or she is correct[4] – it sets out *who* has the duty to satisfy a court that his or her claim or defence should succeed. This is sometimes also referred to as the 'full' onus,[5] the 'overall' onus,[6] onus 'proper,[7] or 'true' onus.[8] The onus

[1] Section 35 (3)(h) Constitution of the Republic of South Africa, 1996. See also P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) ch 2, ch 31 and ch 32; D Zeffertt & A Paizes *The South African Law of Evidence* 2 ed (2009) ch 3 and ch 5; A Paizes 'The law of evidence: Seven wishes for the next twenty years' (2014) 3 *SACJ* 273 – 278.
[2] *Prinsloo v van der Linde* 1997 (3) SA 1012 (CC). See also Zeffertt & Paizes op cit note 1 at 45 – 48.
[3] For a broader discussion on the state of the law of evidence in South Africa, see Paizes op cit note 1 at 272 – 292.
[4] Zeffertt & Paizes op cit note 1 at 45 – 50, 27 – 128; Schwikkard & van der Merwe op cit note 1 at 34 – 36, 602 – 603; DT Zeffertt and A Paizes *Essential evidence* (2010) 13 – 16.
[5] Zeffertt & Paizes op cit note 1 at 128.
[6] *South Cape Corporation (Pty) Ltd v Engineering Management Services (Pty) Ltd* 1977 (3) SA 534 (A) 548 where the court referred to Ogilvie Thompson JA in *Brand v Minister of Justice* 1959 (4) SA 712 (AD).
[7] *South Cape Corporation (Pty) Ltd* supra note 6 at 548 – 549.
[8] Schwikkard & van der Merwe op cit note 1 at 602.

of proof must be distinguished from an *evidentiary burden*,[9] which is the duty on a litigant to either adduce evidence to combat *prime facie* evidence,[10] or to adduce evidence to call upon the other litigant to answer a case – depending on the context.

For example, in a criminal matter, the state bears the onus of proof: the prosecution must prove guilt beyond reasonable doubt. Conversely, in a civil matter, the onus of proof rests with the party instituting civil proceedings to satisfy a court that they have a valid claim. The onus of proof will never shift in criminal matters, it will always remain on the state to prove guilt beyond reasonable doubt. Similarly, in civil matter,[11] the onus of proof rests on a civil litigant who instituted proceedings to satisfy a court as to the correctness of their propositions.[12] However, the *evidentiary burden* does move or *shift* throughout the course of a trial.[13] To illustrate the shift in evidentiary burden – and the static nature of the onus of proof – consider a civil dispute relating to defamatory comments on social media: the plaintiff will carry the onus of proof to satisfy a court that he or she should, on a balance of probabilities, succeed in a damages claim based on the *actio injuriarum*.[14] The duty to begin typically rests with the party who instituted action[15] – following the maxim *he who alleges must prove*.[16] Consequently, the evidentiary burden will, at first, be on the plaintiff. However, during the trial, if the plaintiff makes out a prima facie case, then the evidentiary burden will shift to the defendant[17] to adduce evidence to avoid liability.

Therefore, in a civil defamation matter, in addition to the onus of proof, an evidentiary burden is on the plaintiff to adduce evidence to call upon the defendant to answer a case. In a case of civil defamation, the evidentiary burden will only shift from the plaintiff to the defendant if the plaintiff establishes a publication that is defamatory and that refers to the plaintiff – however, in the internet age, this is usually straight forward to prove and invariably

---

[9] *Brooks v National Director of Public Prosecutions* 2017 (1) SACR 701 (SCA) para 75. See also *South African Human Rights Commission v Qwelane* 2018 (2) SA 149 (GJ) para 14 where the Appellate Division's approach in *Pillay v Krishna* 1946 AD 946 is endorsed.

[10] In this context prima facie means contrary proof is still possible, see Schwikkard & van der Merwe op cit note 1 at 22.

[11] Zeffertt & Paizes op cit note 1 at 890. Generally, the plaintiff has a duty to begin. If there is a dispute as to which party bears the burden of proof, a court must give a ruling.

[12] Schwikkard & van der Merwe op cit note 1 at 602.

[13] Schwikkard & van der Merwe op cit note 1 at 602 – 603.

[14] *Khumalo v Holomisa* 2002 5 SA 401 (CC) para 17 – 18.

[15] Zeffertt & Paizes op cit note 4 at 51 – 53 for an overview of the duty to begin in civil and criminal proceedings.

[16] *Cecilia Goliath v Member of the Executive Council for Health, Eastern Cape* 2015 (2) SA 97 (SCA) para 8 where the court notes: 'The general rule is that she who asserts must prove'. However, see Paizes op cit note 1 at 282 – 284 for a critique of this position.

[17] Social media defamation cases in civil law are instituted by way of summons (as opposed to an application), therefore the party accused of making defamatory statements is known as the defendant and not the respondent (as would be the case in application proceedings).

in civil defamation matters in the context of social media and data messages, the evidentiary burden typically shifts from the plaintiff to defendant.

Once a defamatory publication is established, it is presumed to be both intentional and unlawful.[18] As a result, a defendant will be required to adduce evidence to show a lack of fault, or that the publication was not in the circumstances unlawful. Typically, a defendant in a defamation case has several defences open to her. Briefly, these defences are: 1) truth for the public benefit (the published material must be true and in the publics' interest to receive); 2) fair comment (editorial comment or satirical piece); and 3) privilege (where there is a moral or social duty to publish the defamatory matter, and the recipient has a similar interest or duty in receiving it).[19]

The overall or true onus, however, will always remain on the plaintiff to satisfy a court that her version, on a balance of probabilities, is correct and that she should obtain the relief she seeks.

To continue the defamation analogy,[20] in a *criminal* defamation case,[21] the onus of proof rests on the prosecution to prove the defendant's guilt beyond reasonable doubt. The state will bear the evidentiary burden at the start of the trial, and the prosecution must prove every element of the crime *beyond reasonable doubt*: 1) unlawful; 2) intentional; 3) publication 4) defamatory statement concerning another person.[22] As pointed out by the Supreme Court of Appeal:

> A criminal sanction is indeed a more drastic remedy than the civil remedy but that disparity is counterbalanced by the fact that the requirements for succeeding in a criminal defamation matter are much more onerous than in a civil matter. In a civil action for defamation unlawfulness and animus injuriandi are presumed once the publication of defamatory material is admitted or proved and the onus is on the defendant to prove whatever he relies upon in justification. In the case of criminal defamation not only is there no presumption of

[18] *Khumalo v Holomisa* 2002 5 SA 401 (CC) para 18.
[19] Ibid.
[20] D Milo 'The Timely demise of criminal defamation law' available at *http://www.polity.org.za/article/the-timely-demise-of-criminal-defamation-law-2015-10-05*, accessed on 24 April 2018. The author cogently argues that criminal defamation is unconstitutional in that it amounts to an unjustifiable limitation on the right to freedom of the media. However, in *Motsepe v S* 2015 (5) SA 126 (GP) at para 50 the North Gauteng High Court Pretoria confirmed that in its view, the 'crime of defamation is not inconsistent with the constitution' and that 'even though the defamation crime undoubtedly limits the right to freedom of expression, such limitation is reasonable and justified in an open and democratic society and consistent with the criteria laid down in Section 36 of the Constitution'. See also *S v Hoho* 2009 (1) SACR 276 (SCA).
[21] *S v Hoho* 2009 (1) SACR 276 (SCA) para 33 where the court notes: 'the requirements for succeeding in a criminal defamation matter are much more onerous than in a civil matter.' See also *Motsepe v S* 2015 (5) SA 126 (GP). In a civil law context, see *Khumalo v Holomisa* 2002 5 SA 401 (CC) para 18.
[22] *S v Hoho* 2009 (1) SACR 279 SCA at para 23; *Motsepe v S* 2015 (5) SA 126 (GP) para 46.

unlawfulness or animus injuriandi, the state has to prove both elements and has to do so beyond reasonable doubt.

The *evidentiary burden* can shift[23] from one party to another during the course of a trial, but the *onus of proof* remains on the same party from start to end – regardless of whether the matter is criminal or civil.[24]

In *South Cape Corporation (Pty) Ltd v Engineering Management Services (Pty) Ltd*[25] the Appellate Division confirmed the nature of the onus of proof and its distinction with the evidentiary burden; the court held: "the [true] onus can never shift from the party upon whom it originally rested… the burden of adducing evidence in rebuttal…may shift or be transferred in the course of the case, depending upon the measure of proof furnished by the one party or the other." More recently, in *Mohunram v National Director of Public Prosecutions*,[26] the Constitutional Court approved the distinction made in *South Cape Corporation*.

In civil matters the allocation of the onus of proof is determined by substantive law.[27] Given the plethora of potential legal sources it is 'quite impossible for anyone to present an exhaustive litany of all the rules of substantive law that lay down who bears the onus on every given issue'.[28]

In what is often referred as one of the seminal judgments in this area of law,[29] in *Tregea v Godart*,[30] the Appellate Division – in a judgment questioned by some academics[31] – held that substantive law lays down what must be proved, and who must prove it;[32] and that the rules of evidence relate to the manner of proof.[33] In *Pillay v Krishna*,[34] the Appellate Division (confirming *Tregea*) had occasion to deal with the onus of proof in civil cases in a matter relating to non-payment of a promissory note – this case is often referred to as the locus classicus in judgments.[35] The court confirmed the basic proposition: if one person institutes

[23] Zeffertt & Paizes op cit note 4 at 13 – 16.
[24] Zeffertt & Paizes op cit note 1 at 127 – 130; Schwikkard & van der Merwe op cit note 1 at 602 – 603.
[25] 1977 (3) SA 534 (A). See also Zefferttt & Paizes op cit note 1 at 45 – 46.
[26] 2007 (2) SACR 145 (CC) para 75.
[27] *Tregea v Godart* 1939 AD 16; Zeffertt & Paizes op cit note 4 at 14.
[28] Zeffertt & Paizes op cit note 4 at 14.
[29] Schwikkard & van der Merwe op cit note 1 at 35 where this case is referred to as the 'leading' but 'doubtful' authority. See also Zeffertt & Paizes op cit note 4 at 35 – 55.
[30] 1939 AD 16. See also Schwikkard & van der Merwe op cit note 1 at 35 – 36.
[31] Schwikkard & van der Merwe op cit note 1 at 36; Zeffertt & Paizes op cit note 4 at 13 – 21.
[32] Ibid.
[33] Schwikkard & van der Merwe op cit note 1 at 36.
[34] 1946 AD 946.
[35] See *Brooks v National Director of Public Prosecutions* 2017 (1) SACR 701 (SCA) para 75; *South African Human Rights Commission v Qwelane* 2018 (2) SA 149 (GJ) para 14; *Strydom v Engen Petroleum Ltd* 2013 (2) SA 187 (SCA) para 46 where the Appellate Division's approach in *Pillay v Krishna* 1946 AD 946 is endorsed.

action against another, that person must satisfy a court that they are entitled to the relief they seek. The court referred to *Corpus Juris*, and in particular: *'*semper necessitas probandi incumbit illi qui agit*'* (if one person claims something from another in a court of law, then he has to satisfy the court that he is entitled to it). Further, the court confirmed that the principle must be read together with the following proviso: 'agere etiam is videtur, qui exceptione utitur: nam reus in exceptione actor est' (where the person against whom the claim is made is not content with a mere denial of that claim, but sets up a special defence, then for his defence to be upheld he must satisfy the Court that he is entitled to succeed on it).[36]

Although criticized by some authors for conceptual ambiguity,[37] the position set out in *Tregea*, confirmed in *Pillay* and *South Cape Corporation*, amongst others, has also been confirmed by the Constitutional Court and is the current leading authority in this area of law.

6.3 DOES THE ECT ACT REQUIRE DIFFERENT CONSIDERATIONS OF DATA MESSAGES IN CIVIL AND CRIMINAL CONTEXTS?

Do different considerations exist in so far as data message evidence is concerned in civil and criminal matters? In principle, in terms of the ECT Act,[38] no. Data messages are functional equivalents of paper, and considered in terms of the same provisions of the ECT Act, with the same considerations.[39] Consider this brief analogy: would it be appropriate to apply different considerations in criminal proceedings (as opposed to civil proceedings) when considering the admissibility of a traditional paper document? No. The considerations would be the same – this applies equally to data messages as it does to *all* forms of evidence.

However, the standard of proof usually dictates that in criminal matters further and more conclusive evidence is required than in civil matters. Data message evidence should be treated the same as all other forms of evidence (subject to legislation), and no different considerations should apply across civil and criminal matters: other than the inherent differences already apparent in civil and criminal proceedings.

---

[36] 1946 AD 946 at 951 – 952.
[37] Zeffertt & Paizes op cit note 4 at 13 – 20; Schwikkard & van der Merwe op cit note 1 at 36.
[38] See Part 1 of the ECT Act *Legal requirements for data messages*, sections 11 – 20, read together with section 1 of the ECT Act.
[39] *S v Miller* 2016 (1) SACR 251 (WCC) para 52; *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ) para 12 – 13.

Interestingly, the ECT Act is based on the Model Law, 1996 which *applies to civil law only*.[40] However, as noted by the SALRC,[41] and other academics,[42] the ECT Act clearly applies to civil and criminal law.[43] Furthermore, a variety of criminal[44] and civil[45] cases have interpreted the provisions of the ECT Act in a similar manner. Hofman,[46] points out that the ECT Act does not contain a provision limiting it to commercial matters – as the Model Law clearly does in article 1..[47] Moreover, if the ECT Act did not apply to criminal law, it would leave a ludicrous lacuna in the regulation of electronic evidence for criminal matters – an absurd result that would never be intended.

Data messages, subject to concessions[48] or directives in legislation, should be treated the same as traditional evidence as far as possible: the *functional equivalent*. Consequently, it would not be appropriate to apply different evidentiary considerations to data messages in civil and criminal proceedings: the onus of proof and applicable standard of proof must dictate what considerations are applicable with data message evidence. If one has regard to recent criminal cases – for example *S v Meyer,* and *S v Brown* from a criminal perspective, and *LA Consortium & Vending CC t/a LA Enterprises* from a civil perspective, it appears the same considerations apply. The same can be said for earlier cases – such as in *S v Ndiki*, and *Ndlovu v Minister of Correctional Services*, where regardless of whether the matter was civil or criminal, the relevant sections of the ECT Act were applied in similar manner – in summary: the cases reflect no clear difference in treatment of data messages across civil and criminal law.

---

[40] United Nations 1996 Model Law on Electronic Commerce with Guide to Enactment 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, article 1. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 31 – 32; J Faria 'E-commerce and international legal harmonization: Time to go beyond functional equivalence?' (2004) *SA MERC LJ* 529-555.

[41] Section 4 of the ECT Act states that it applies in respect of *any* electronic transaction or data message. See also South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 27 – 30 where the South African Law Reform Commission also conclude that the ECT Act applies to both civil and criminal proceedings.

[42] D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) 77 – 82; C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461; J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 260 – 261.

[43] This interpretation is given irresistible flavour when one considers that the ECT Act specifically regulates cyber-crime – although, as noted by the court in *S v Miller* 2016 (1) SACR 251 (WCC) para 56, a cyber-inspector has yet to be appointed. See also van der Merwe et al op cit note 43 at 85 – 86.

[44] *S v Ndiki* 2007 2 All SA 185 (Ck); *S v Meyer* 2017 JDR 1728 (GJ); *S v Brown* 2016 (1) SACR 206 (WCC).

[45] *Ndlovu v Minister of Correctional Services* 2006 4 All SA 165 (W); *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).

[46] Hofman op cit note 43 at 260 – 261.

[47] United Nations 1996 Model Law on Electronic Commerce with Guide to Enactment 1996 *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf* at article 1.

[48] Such as in the ECT Act, the Civil Proceedings Evidence Act 25 of 1965, the Criminal Procedure Act 51 of 1977, and the Law of Evidence Amendment Act 45 of 1988.

6.4 IN A CRIMINAL MATTER, MUST ALL DATA MESSAGE EVIDENCE BE PROVED BEYOND REASONABLE DOUBT?

It has been said that all evidence requires a court to engage in inferential reasoning.[49] Where a court must consider a 'second tier of inferential reasoning in addition to the first', this is referred to as circumstantial evidence.[50] As discussed above in the context of admissibility and weight of data message evidence,[51] a court will likely have to rely on circumstantial evidence and inferential reasoning when assessing weight (cogency) of data message evidence, amongst others.[52]

Do all facts in a murder trial need to be proved beyond reasonable doubt? For example, must the existence or reliability of *all* data message evidence be proved beyond reasonable doubt? In short: it depends on the facts of the case and evidence available, but most likely no. An analogy from Paizes is useful in this regard: Some facts can be likened to links in a chain – without proof thereof beyond reasonable doubt there can be no conviction. Conversely, some facts can be likened to strands in a cable; the more facts that are relied upon to support the inference, the less likely it is that each must be proved beyond reasonable doubt.[53] Put differently,[54] as set out by the Appellate Division in *R v De Villiers*,[55] a court should consider the *cumulative* effect of the evidence.

However, it should be noted that when evaluating circumstantial evidence, there are different standards applied in civil and criminal trials.[56] These 'rules' are referred to as the cardinal rules of logic, and were set out by the Appellate Division in *R v Blom*,[57] where the court held:

> In reasoning by inference there are two cardinal rules of logic which cannot be ignored:

---

[49] Zeffertt & Paizes op cit note 1 at 99.
[50] Zeffertt & Paizes op cit note 4 at 23; Schwikkard & van der Merwe op cit note 1 at 23.
[51] See ch 4 para 2; ch 3 para 3.
[52] Also, for example, when considering whether a document is an original in terms of ECT Act.
[53] Paizes op cit note 1 at 281 – 282 where reference is made to the Australian case of *Shepherd v The Queen* (1990) 170 CLR 573 where the court notes at 2-510: 'Generally, no particular fact or circumstance relied upon in a circumstantial case needs to be proved beyond reasonable doubt. There may, however, be a circumstantial case where one or more of the facts relied upon by the Crown is, or are, so fundamental to the process of reasoning to the guilt of the accused that the fact or facts must be proved beyond reasonable doubt'. See also *Davidson v R* (2009) 75 NSWLR 150; *Burrell v R* (2009) 196 A Crim R 199.
[54] Schwikkard & van der Merwe op cit note 1 at 578.
[55] 1944 AD 493 508 – 509.
[56] Schwikkard & van der Merwe op cit note 1 at 578 – 579.
[57] 1939 AD 188 202 – 203. This case is often referred to as the *locus classicus*, for example, see *Malebo v S* [2015] ZAFSHC 61 para 6 and *Jantjies v S* [2014] ZASCA 153 para 14.

(1) The inference sought to be drawn must be consistent with all the proved facts. If it is not, the inference cannot be drawn.

(2) The proved facts should be such that they exclude every reasonable inference from them save the one sought to be drawn. If they do not exclude other reasonable inferences, then there must be a doubt whether the inference sought to be drawn is correct.'

In civil cases, the second consideration set out in *Blom* does not apply.[58] This takes account of the differing standards of proof, namely, a balance of probabilities will not require a court to be sure that all other reasonable inferences are excluded, rather, in a civil matter, a court must determine that the inference which is drawn is the most acceptable or probable inference from all the available inferences.[59]

6.5 CONCLUSION

The ECT Act applies to both civil and criminal proceedings.[60] Other than the difference in the standard of proof, data message evidence should be considered similarly whether in civil or criminal proceedings: in my view, it is not appropriate to apply different considerations; the ECT Act makes no distinction, and the case law suggests that the same considerations should apply.

[58] Schwikkard & van der Merwe op cit note 1 at 579.
[59] *AA Onderling Assuransie Bpk v De Beer* 1982 (2) SA 603 (A); Schwikkard & van der Merwe op cit note 1 at 578 – 579.
[60] Section 15 (1) which states that it applies in *any* legal proceedings.

CHAPTER 7: AN ANALYSIS OF THE MOST RECENT SOUTH AFRICAN LAW REFORM COMMISSION RECOMMENDATIONS IN THE CONTEXT OF ELECTRONIC EVIDENCE

7.1 INTRODUCTION

In its most recent investigation into the law of evidence, the SALRC suggest three options for law reform in the context of electronic evidence.[1] The three options are: retention of the current regulatory landscape with minor reform; alternatively, electronic evidence specific legislation, regulations or guidelines; alternatively, complete reform of the current regulatory environment.[2] The suggested approaches to law reform are intended to resolve areas of confusion[3] which have been exacerbated by swift technological development; a relative lack of authoritative precedent in this area; and deliberate, unrushed regulation in the information, communication and technology environment. In this context – importantly – it is an undeniable fact that technology is becoming more pervasive,[4] and smarter;[5] consequently, electronic evidence will be an unavoidable part of legal proceedings and areas of confusion must be resolved as soon as possible.

The SALRC recommend implementing the most aggressive of the three options,[6] and proposes drastic reform in the form of a *Law of Evidence Bill* which seeks to regulate, inter alia: the admissibility of evidence in the context of hearsay evidence; the admissibility and proof of business records; and evidence produced by machines in all legal proceedings.[7] This recommendation follows a lengthy review and investigation into the state of evidence in civil and criminal proceedings in South Africa – which began soon after the SALRC's establishment in 1973 following the promulgation of the South African Law Reform Commission Act 19 of

[1] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 86 – 88 for a summary of the three proposed options for law reform. For further context into this investigation, see also South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010).
[2] Ibid.
[3] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 22.
[4] *Van Breda v Media 24 Limited* 2017 (5) SA 533 (SCA) para 2.
[5] W Erlank & L Ramokanate 'Allocating the risk of software failures in automated message systems (autonomous electronic agents)' 2016 *SAMLJ LJ* 201 – 202.
[6] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 87 where the SALRC are aware that the third option for law reform – the most aggressive – may be controversial, and state: '[T]his option does, however, present a fairly extensive departure from the status quo and would therefore require further reflection and feedback from the various stakeholders.'
[7] See Annexure A *Draft Law of Evidence Bill* B2014 South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 89.

1973.[8] Ultimately, the decades-long research and discussion has culminated in the recommendations discussed in this chapter.[9] Consequently, this chapter will critically analyse the eleven issues identified by the SALRC, and conclude with comments on each relevant section of the proposed *Law of Evidence Bill*.

7.2 BACKGROUND TO SOUTH AFRICAN LAW REFORM IN THE CONTEXT OF ELECTRONIC EVIDENCE

The original intention of the SALRC in relation to the law of evidence was to suggest the enormous task of complete codification in one piece of legislation.[10] However, once it commenced its work, the SALRC realised that such a task would probably take years to complete, and entail resources outside of its reach – consequently, it decided against the complete codification approach, and rather elected to ascertain which aspects of the law of evidence were unsatisfactory; and to formulate suggestions for reform.[11]

As discussed above,[12] soon after the 1976 matter of *Narlis v South African Bank of Athens*,[13] the Clearing Bankers Association of South Africa instructed Judge Didcott[14] to prepare a report and draft legislation regulating the admissibility of electronic evidence.[15] The report and draft legislation[16] was presented to the SALRC, who in turn produced the first research report into electronic evidence: the 1982 *Admissibility in Civil Proceedings of Evidence Generated by Computers (Project 6) Review of the Law of Evidence.* As a result of the SALRC's recommendations in this first report on the issue, the Computer Evidence Act 57 of 1983 commenced operation on 1 October 1983.

---

[8] This legislation was originally known as the South African Law Commission Act 19 of 1973. It changed names to the South African Law Reform Commission Act 19 of 1973 in terms of section 5 of the Judicial Matters Amendment Act 55 of 2002 on 17 January 2003. For more on the SALRC see *http://www.justice.gov.za/salrc/objects.htm#sthash.OIkeTaHM.dpbs*, accessed on 3 June 2018.

[9] I was advised in June 2018 by a South African State Law Advisor that these recommendations are currently pending before the Minister of Justice and Constitutional Development.

[10] 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 (2010) para 1.6 at 3.

[11] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 1.2 at 12.

[12] See chapter 2 para 2.3.1 above.

[13] 1976 (2) SA 573 (A).

[14] D van der Merwe et al *Information and Communications Technology Law* 2 ed (2016) at 111.

[15] 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 (2010) para 4.3 at 19.

[16] Van der Merwe et al op cit note 14 at 111.

As noted by many,[17] the Computer Evidence Act was a failure.[18] The SALRC recommended its repeal in 1995[19] after first expressing satisfaction with its enactment in 1987.[20] In the interim, further research papers explored cybercrime,[21] and despite first recommending the Computer Evidence Act's repeal in 1995, new legislation in the form of the ECT Act only commenced operation in 2002; section 92 of the ECT repealed the Computer Evidence Act entirely.[22]

It is worth mentioning that in 1996, instead of preparing and releasing what were known as *working papers*, the SALRC opted to start exploring law reform with *issue papers*, and *discussion papers*. The purpose of an *issue paper* is to 'announce an investigation, or to clarify the aim and extent of the investigation, and to suggest the options available for solving existing problems.' These research papers 'involve the community actively at an earlier stage, the [SALRC] publishes issue papers for appropriate investigations as the first step in the consultation process.'[23] Conversely, *discussion papers* are: 'documents in which the [SALRC]'s preliminary research results are contained. In most cases discussion papers also contain draft legislation. The main purpose of these documents is to test public opinion on solutions identified by the [SALRC].'

The promulgation of the ECT Act in 2002 notwithstanding, the SALRC in 2010 felt that an *issue* paper dealing with the use of electronic evidence in criminal and civil proceedings was necessary.[24] Following the 2010 issue paper, which suggested eleven main areas of concern,[25] the SALRC released in 2014 a *discussion* paper which ultimately recommended the

---

[17] P Schwikkard & S van der Merwe *Principles of Evidence* 4 ed (2016) at 440; D van der Merwe et al op cit note 14 at 111-112; 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 (2010) para 4.5 at 19; J Hofman & J de Jager 'South Africa' in Mason (ed) *Electronic Evidence* 3 ed (2012) para 18.06 at 763; D Zeffertt and A Paizes *The South African Law of Evidence* 2 ed (2009) at 431 – 432.

[18] *S v Brown* 2016 (1) SACR 206 (WCC) para 16 where the court noted: 'the Computer Evidence Act 57 of 1983, was generally considered to have failed to achieve its purpose… and, in any event, [did not] regulate criminal proceedings'. See also S Mapoma *A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM thesis, University of South Africa, 1997) 3 – 32.

[19] South African Law Commission Working Paper 60 (Project 95) *Investigation into the Computer Evidence Act 57 of 1983* (1995) at iv.

[20] South African Law Commission Report (Project 6) *Review of the Law of Evidence* (1987) 28. See also J Hofman 'Electronic evidence in criminal cases' (2006) 3 *SACJ* 257.

[21] South African Law Commission Issue Paper 14 (Project 108) *Computer related crime* (1998) para 19; South African Law Commission Discussion Paper 99 (Project 108) *Computer related crime* (2001) at para 2.5.

[22] Hofman op cit note 20 at 258.

[23] South African Law Reform Commission 'Issue Papers' available at *http://www.justice.gov.za/salrc/ipapers.htm*, accessed 5 May 2018.

[24] 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 (2010) at iii.

[25] 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 (2010) at 28 – 49 where eleven areas for comment are identified.

overhaul of the current regulatory framework governing electronic evidence.[26] The period for public comment on the recommendations contained in the 2014 discussion paper was extended into 2015, and the discussion paper findings finalised in November 2016; the final recommendations are pending before the Minister of Justice and Constitutional Development in 2018.[27]

7.3 THE ADEQUACY OF THE ECT ACT: QUESTIONS RAISED IN THE SALRC'S ISSUE PAPER 27; AND RECOMMENDATIONS MADE IN DISCUSSION PAPER 131 (PROJECT 126) REVIEW OF THE LAW OF EVIDENCE

7.3.1 Should the ECT Act be reviewed regularly?

The SALRC start with the most obvious question: 'Should the ECT Act be reviewed on a regular basis to take account of advances in technology?'[28] In response, the SALRC note:

> By and large, there seems to be consensus on the need for regular review of the provisions of the ECT Act. The SALRC invites further suggestions on the appropriate technical forum (which must be in a position to facilitate the engagement of multiple stakeholders) for such review.

The LSSA propose a multidisciplinary panel comprising of, inter alia, the SALRC, applicable government representation from the department of Justice and Constitutional Development, the Department of Communications, the Information Regulator,[29] and ICT experts. In addition, in my view, any review panel *must* also include diverse legal skills in the form of: an experienced practicing attorney, an experienced practicing advocate of a recognised Bar Council in South Africa, and an academic professor. Clearly, the review panel should ensure foreign developments are monitored and that where possible (and desirable) South Africa is consistent therewith.[30] The recommendations made by the LSSA – or something similar – should be implemented as soon as possible. In summary, a multidisciplinary team should be

[26] See a summary of the SALRC's findings in South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 1.27 – 1.38 at 20 – 25.
[27] Based on my own discussions with the SALRC, a State Law Advisor, and staff members of the Department of Justice and Constitutional Development.
[28] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.2 – 4.11 at 46 – 48.
[29] The *Information Regulator* created by the Protection of Personal Information Act 4 of 2013 – this regulator also regulates freedom of information disputes in terms of the Promotion of Access to Information Act 2 of 2000.
[30] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 1 – 3, accessed on 8 May 2017.

appointed with a mandate to review the ECT Act, and to report to Parliament periodically to monitor the dynamic, business-critical ICT landscape.

Despite the recommendations of the SALRC, a review of recent (and all relevant) case law suggests there is no urgent need to adopt new legislation;[31] however, there is certainly a need for an on-going review of the ECT Act and the surrounding regulatory landscape. Moreover, there is definitely a pressing need for reform in certain areas, and given the explosion of internet connectivity in the last 5 to 10 years,[32] and the likely importance electronic evidence will have in all forms of legal proceedings going forward, this review project should receive urgent attention.

7.3.2 Are the provisions in the ECT Act adequate to regulate the admissibility[33] of electronic evidence in criminal and civil proceedings?

The SALRC points out that the ECT Act, including s 15 which specifically regulates evidence, is based on the UNCITRAL Model Law, 1996 that only applies to commercial activities, and poses the following question: are the provisions of the ECT Act adequate for both civil and criminal law? By proposing an aggressive overhaul of the current regulatory environment, the SALRC appears to believe the current provisions of the ECT are not adequate. However, in discussing this issue the following pertinent observation is made:[34]

> The fact that the admissibility of electronic evidence is regulated by not only the provisions of the ECT Act, but also by common law principles and by provisions in the CPA and CPEA, may take the pressure off the ECT Act to accommodate nuanced differences in criminal and civil proceedings.

In addition to the provisions mentioned by the SALRC directly above – the Law of Evidence Amendment Act[35] is also relevant and applicable,[36] and the ECT Act certainly does not stand

[31] *S v Meyer* 2017 JDR 1728 (GJ), *S v Miller* 2016 (1) SACR 251 (WCC), and *S v Brown* supra note 18 for three recent criminal law examples. See also *Trustees for the time being of the Delsheray Trust* v *ABSA Bank Ltd* [2014] 4 All SA 748 (WCC), and *LA Consortium & Vending CC t/a LA Enterprises v MTN Service Provider (Pty) Ltd* 2011 (4) SA 577 (GSJ) for two recent civil law examples.
[32] Internet World Stats 2018 *http://www.internetworldstats.com/africa.htm#za*, roughly 53.7% of South Africa's population had Internet access as at December 2017. In 2008, the South African internet penetration rate was roughly 9%: This is remarkable growth in one decade.
[33] Admissibility and weight of electronic evidence is discussed above in chapter 5.
[34] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.17 at 50.
[35] Act 45 of 1988, particularly s 3 thereof.
[36] See the discussion above in chapter 2 and 3.

alone. That being the case, the LSSA[37] believe the current position is adequate, and that the standard of proof[38] will accommodate any differences in civil and criminal matters, and state:

> evidence submitted in criminal or civil proceedings is essentially the same, but that ―the onus of proof … in criminal and civil matters … will differ. The yardstick is proof beyond reasonable doubt in criminal matters and a lower one in civil matters namely, a balance of probabilities.

Accordingly, the LSSA believe it is not necessary to regulate the use and admissibility of electronic evidence outside the ECT Act.[39] Similarly, the NPA are of the view that the current position is adequate and state: 'There is no real reason why there should be a separate piece of legislation to provide for the admissibility of electronic evidence in criminal and civil proceedings outside the provisions of the ECT Act 25 of 2002.'[40]

Conversely, Legal Aid South Africa[41] believe that the current approach is fragmented and the common law inadequate, and that law 'dealing with [electronic evidence] in a single piece of legislation is eminently desirable.' It may well be desirable, but at this stage of South Africa's jurisprudence relating to e-commerce and technology, it is probably not practical without further, more comprehensive review.

Be that as it may, Advocate Eiselen, arguing on behalf of Nedbank and what the SALRC refer to as the banking industry[42] in my view cogently summarises some of the key issues that require urgent attention:

> [T]here are good grounds for streamlining this part of the law of evidence by aligning the provisions of section 26-32 of the CPEA , section 221 of the CPA and section 15(4) of the ECT Act. We further submit that the approach contained in section 221 of the CPA and section 15(4) of the ECT Act is preferable to that contained in the CPEA.

The current position – although slightly fragmented, and in need of amendment in certain areas is adequate for the time being. For example, from *S v Ndiki*,[43] the early seminal criminal case

---

[37] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.18 at 51. Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 1 – 3, accessed on 8 May 2017.

[38] See the discussion above in chapter 6 para 6.2.

[39] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 3 – 4, accessed on 8 May 2017.

[40] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.21 at 51.

[41] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.19 at 51.

[42] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.119 at 75.

[43] [2007] 2 All SA 185 (Ck). Also reported as *S v Ndiki* 2008 (2) SACR 252 (Ck).

dealing with electronic evidence to the more recent cases of *S v Brown*,[44] *S v Meyer*,[45] and *S v Miller*,[46] the current legislation has been no obstacle to courts receiving electronic evidence, and courts have adequately dealt with differing forms of electronic evidence. Similarly, in civil courts, from *Ndlovu v Minister of Correctional Services*[47] to the more recent *LA Consortium & Vending CC v MTN Service Provider (Pty) Ltd,*[48] courts have adequately dealt with and received electronic evidence (although sometimes superficially, inconsistently, and often without sufficient detail in so far as its admissibility and weight are concerned).

Since the promulgation of the ECT Act in 2002, there are no reported cases – civil or criminal – where the ECT Act (or related legislation) posed a specific impediment to the reception of electronic evidence. Consequently, although the ECT Act is not perfect, it can certainly be said that is has achieved its goal of facilitating the admissibility of electronic evidence in civil and criminal proceedings. Consequently, before introducing new concepts and legislation, a further review is necessary – and more time should elapse to allow the medium to develop and mature. This would also allow the SALRC or any ECT review team to consider new cases and further international developments.

The LSSA and NPA view should be supported – the ECT Act is adequate in the short-term, but minor reform is required, including reform to related legislation, particularly: consistency with the term 'document' in the Civil Proceedings Evidence Act, and the Criminal Procedure Act.[49] In addition, consideration must be given to the express inclusion of the term 'data message' in appropriate legislation, such as: the Law of Evidence Amendment Act, the Civil Proceedings Evidence Act, the Criminal Procedure Act, the Uniform Rules of Court, and the Magistrates Court Act Rules. Further, and as will be discussed further below,[50] consideration must be given to an amendment of court rules to specifically incorporate electronic discovery[51] and discovery of meta data.[52]

---

[44] Supra note 18.
[45] Supra note 31.
[46] Supra note 31.
[47] [2006] 4 All SA 165 (W).
[48] Supra note 31.
[49] The Civil Proceedings Evidence Act 25 of 1965 defines *document* as: 'includes any book, map, plan, drawing or photograph.' Conversely, s 221 of the Criminal Procedure Act 51 of 1977 defines *document* as: 'includes any device by means of which information is recorded or stored.' It is not sustainable that the civil definition of document is narrower than the criminal definition – this anomaly should be rectified.
[50] See para 7.3.11 below.
[51] B Hughes 'The rise of electronic discovery' *De Rebus* January/February 2012 at 24 – 26.
[52] F Cassim 'The use of electronic discovery and cloud-computing technology by lawyers in practice: Lessons from abroad' *Journal for Juridical Science* (2017) 42 (1) 21 – 23.

7.3.3 Should the current definition of "data message" in the Act be revised? Should the ECT Act include definitions of "electronic", "copy", and "original"?

The current definition in the ECT Act reads as follows:

> 'data message' means data generated, sent, received or stored by electronic means and includes-
>
> (a) voice, where the voice is used in an automated transaction; and
> (b) a stored record

Conversely, the *Cybercrimes Bill*[53] will define the term as:

> 'data message' means data generated, sent, received or stored by electronic means, where any output of the data is in an intelligible form

As discussed in chapter 2,[54] according to s 58 of the Cybercrimes Bill, the term data message in the ECT Act will have a different meaning to that in the Bill – this will therefore lead to a situation where data message has two different definitions. Granted, this could potentially have very little practical effect, but is it clearly not desirable, and either the Cybercrimes Bill should repeal the term 'data message' in section 1 of the ECT Act, or when Bill is promulgated, the final version should not include a definition for data message.

Some point out that the term data *record* may be preferable to data *message*[55] – and although there is certainly merit in that argument, my view is that South Africa ought to exercise caution when moving away from internationally accepted terminology,[56] and at the very least complete a review of the ECT Act before amending key definitions. That notwithstanding, the SALRC (referring to the ECT Act definition of 'data message') state:

> There is clearly concern around the inclusion of the term ―voice, where the voice is used in an automated transactionin the definition of data message, and there do not appear to be compelling reasons to retain the term in the definition. The SALRC therefore proposes that the term be deleted or amended.

In relation to the proposed Cybercrimes Bill definition of 'data message', there is a potential concern in so far as the final part of the definition is concerned (the relevant portion reads: *where any output of the data is in an intelligible form*). One should ask, when considering the admissibility of traditional evidence, is it necessary for that evidence to be in

---

[53] Bill B6B – 2017.
[54] Para 2.2.
[55] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.23 – para 4.33 at 52- 53.
[56] Ibid at 53.

an *intelligible* form? As long as a document is relevant, it does not need to be intelligible as a condition to being admissible. in light of functional equivalence, I would argue that a preferred definition of *data message* must exclude the additional requirement of the data being intelligible. Granted, some may argue that this may mean a court has a proliferation of issues to deal with when potentially considering unintelligible data. However, even if data message evidence is unintelligible, its admission may provide context or add a strand of cable to the narrative.[57] Holistically, any definition should be neutral, concise and comply with functional equivalence where possible. My suggestion is: 'data message' means data generated, sent, received or stored by electronic means.

Consequently, my view is that the definition proposed by the Cybercrimes Bill is superior to the current ECT Act definition (even with the extra condition of intelligibility as it stands). Accordingly, s 58 of the Cybercrimes Bill should be amended to include the repeal of the definition of *data message* in s 1 of the ECT Act to avoid conflicting definitions. Ideally, the promulgated version of the Bill will also remove the condition of *intelligibility* from the definition of *data message*.

In so far as further clarity on the meaning of 'original', 'electronic' and 'copy' – the ECT Act already deals comprehensively with an original.[58] The section reads as follows:

> 14. Original
> (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if –
> (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
> (b) that information is capable of being displayed or produced to the person to whom it is to be presented.
>
> (2) For the purposes of subsection 1(a), the integrity must be assessed-
> (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
> (b) in the light of the purpose for which the information was generated; and
> (c) having regard to all other relevant circumstances.

However, in *S v Koralev*,[59] a matter in the Natal Provisional Division relating to child pornography, and offences in terms of the Films and Publications Act 65 of 1996, and the Sexual Offences Act 23 of 1957, the court found that digital images were not original images:

[57] A Paizes 'The law of evidence: Seven wishes for the next twenty years' (2014) 3 *SACJ* 281.
[58] Section 14 of the ECT Act. See also, C Theophilopoulos 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 468 – 470; Hofman op cit note 20 at 263 – 264.
[59] 2006 2 SACR 298 (N).

'we are also not in agreement with the finding by the learned magistrate that the images were 'original' since [it was] common cause that they had been either downloaded from [the] Internet or transferred from a digital camera…' and that 'original images would be those contained in camera or in original source from which they had been loaded onto an Internet site.'[60] This position is *clearly* incorrect. This interpretation[61] does not take account of s 14 of the ECT Act – a digital image, in terms of s 14, will be regarded as an *original* if: a) the image's integrity has been assessed;[62] and b) the information is capable of being displayed. A digital image is usually capable of being displayed. The key issue in determining whether an image will be original is to ascertain whether: 'the integrity of the information from the time when it was first generated… has passed assessment.' *Assessment*, according to s 14 (2) requires considering all relevant factors, but specifically in s 14(2)(a): 'considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display.' As noted by *S v Meyer*[63] when passing judgment in August 2017:

> Section 14 requires that the integrity of the information contained in the data message be assessed: has it remained complete and unaltered except for the addition or endorsements or changes which arise in the normal course of communication, storage or display… also … the information [must] be capable of being displayed or produced to the person to whom it is to be presented.

In many instances a digital image should properly be considered original without it having to be on the original device. As pointed out by Zeffertt and Paizes,[64] the decision in *Koralev* is 'difficult to reconcile' with the Supreme Court of Appeal decision in *Botha v S*[65] (and even more difficult to reconcile with recent cases, including *Meyer* discussed above). In *Botha*, in the context of an attorney being convicted of fraud, forgery and uttering, the court found:

> For each charge, the State adduced documentary proof, sometimes the original documents and sometimes copies. Botha's legal representative in the trial argued at length that no reliance

[60] 2006 2 SACR 298 (N) 307 – 308.
[61] *S v Koralev* 2006 (2) SACR 298 (N) was heard on 18 May 2006 – the judgment was delivered on 6 June 2006. The ECT Act was assented to on 31 July 2002 and commenced operation on 30 August 2002.
[62] Section 14 (1). See also *Meyer* supra note 31 para 302.
[63] *S v Meyer* supra note 31 para 302.
[64] D Zeffertt and A Paizes *Essential evidence* (2010) 128. As an aside, the reference used by the authors in this text at footnote 11 on page 128 contains a small anomaly. It reads [2010] 2 All SA 116 (SCA) which refers to a Supreme Court of Appeal case – also *Botha v S* – but a matter that deals section 20 (1) of the Arbitration Act 42 of 1965. The editors of electronic law library LexisNexis appear to have made the same mistake (as have a number of other authors). The correct neutral reference is *Botha v S* [2009] ZASCA 125 (29 September 2009) – it is available at *http://www.justice.gov.za/sca/judgments/sca_2009/sca09-125.pdf*, accessed 21 June 2018.
[65] *Botha v S* [2009] ZASCA 125 (29 September 2009) para 27.

> could be placed on copies. But no evidence was adduced by him to show that they were not authentic copies. *And since many of the documents were computer-generated it cannot be said that the documents were not the originals*. While clearly it is preferable for original documents to be produced as evidence, where this is not possible or practicable, there is no reason, in the absence of countervailing evidence as to its lack of authenticity, not to accept it as the best evidence available... [my emphasis]

This view is preferable as it allows a data message to be considered an original in terms of s 14 of the ECT Act even where it is not the initial data message created. For example, on the interpretation in *Koralev*, a data message can only be original if it is on the device (camera, phone etc.) – this view is clearly incompatible with s 14 of the ECT Act and an evolving digital environment. However, in *Botha v S*,[66] even though – surprisingly – the ECT Act was not expressly referred to, the court's opinion expressed above *is* compatible with s 14 of the ECT Act.

In the more recent *S v Brown*,[67] the Western Cape Division of the High Court found that the 'potential mutability and transient nature of images' means it is better to treat digital images as documentary evidence rather than real evidence. Be that as it may, the court applied section14 of the ECT Act and found:

> As regards the images being in their original form, s 14 of ECTA provides that a data message satisfies the requirements of original form if it meets the conditions in that section. These are, in short, that the integrity of the information, from the time when it was first generated in its final form as a data message , has passed assessment in terms of s 14(2) and, secondly, that information is capable of being displayed or produced to the person to whom it is to be presented.[68]

> In my view, on a conspectus of this evidence, the requirements of original form and of s 14 of ECTA have been met. In any event, s 15(1)(b) of ECTA gives data messages a further exemption from the requirement of original form 'if it is the best evidence that the person adducing it could reasonably be expected to obtain'.[69]

The more recent decisions in *Meyer, Botha,* and *Brown*,[70] read together with the ECT Act, certainly mean that the term *original* is adequately dealt with at present. The SALRC appears to agree,[71] and states: 'given the existing provisions of the ECT Act regarding an 'original' and the 'best evidence rule', no further reform is proposed at this stage.

---

[66] Ibid.
[67] *S v Brown* supra note 18 paras 19 – 22.
[68] Ibid at para 22.
[69] Ibid para 24.
[70] Supra note 31 above.
[71] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.39 at 55.

On *copy* and *electronic*, most agree a definition for 'electronic' is not required, but some[72] propose the introduction of a definition for 'copy' in order to foster greater clarity and conceptual certainty. What further conceptual clarity is required? It appears courts and attorneys must first familiarise themselves with the ECT Act, together with information communication technology in general, before introducing definitions that may well be superfluous. As noted by the LSSA, there is no pressing need for the introduction of new definitions at this stage;[73] particularly in light of the fact there are no reported decisions (or any published South African litreture) suggesting that such a distinction is necessary, or even whether it is feasible. As a result, before the introduction of new terms, some of which may conflict with internationally accepted terminology, the ECT Act and related legislation should first be comprehensively reviewed as outlined above in paragraph 7.3.1 and suggested by the SALRC.

7.3.4 Should the ECT Act be amended to extend its sphere of application?

Currently, s 4(3) and s 4(4) of the ECT Act provide certain exclusions from the operation of the ECT Act – these relate to four specific pieces of legislation: The Wills Act 7 of 1953; the Alienation of Land Act 68 of 1981; the Bills of Exchange Act 34 of 1964; and the Stamp Duties Act 77 of 1968. These exclusions, found in Schedule 2, relate to four items: i) the execution of wills; ii) the sale of immoveable property; iii) an agreement for the long-term lease of immovable property in excess of 20 years; and iv) the execution of a bill of exchange.

Although this particular issue has largely fallen outside the scope of this research, for the sake of completeness, the SALRC questions whether the ECT Act should be amended to include the previously excluded pieces of legislation (although the Stamp Duties Act was mentioned as a possible area for extension, this legislation was repealed with effect from 1 April 2009 and therefore cannot be included in the operation of the ECT Act).[74]

---

[72] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.34 – 4.38 at 54 where the National Prosecuting Authority, Nedbank, and the South African Police Services argue that a definition for *copy* is required. However, the Law Society of South Africa, and Legal Aid South Africa do not believe copy or electronic should be defined.

[73] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.36 at 54; Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 1 – 5, accessed on 8 May 2017.

[74] Section 103 of the Revenue Laws Amendment Act 60 of 2008.

Certain submissions to the SALRC on this issue suggest a large amount of scepticism concerning electronic commerce in general, with the tone being that given the 'high risks involved'[75] the 'excluded transactions mentioned in Schedule 2 should not be included in the ECT Act, at this stage of electronic commerce development.'[76] However, other submissions – such as from the LSSA and Legal Aid South Africa – are more progressive and suggest that technological advances dictate that there should no longer be exclusions. However, there is a cogent argument that wills should remain excluded from execution via data messages[77] because of the fast-paced nature of ICT development; the LSSA note:

> Wills also have a potentially very long 'shelf-life'. In this regard, the LSSA has also noted the reservations of some practitioners regarding the potential for even advanced security methods of signing documents to be exploited in the future. For example, where a document is signed with an advanced electronic signature today, practitioners have questioned whether that technology would still be relatively tamper proof in 30 to 40 years' time (or would a future grandchild with a degree in Computer Science be able to easily decrypt the technology of 2015 and alter the contents of his or her grandparent's electronic will)?

That objection notwithstanding, provided a data message is properly authenticated,[78] then a person should be able to execute a will, enter in an agreement for a long-lease, enter into an agreement for the sale of immoveable property, and to execute a bill of exchange, as the case may be, with a data message. Consequently, in order to ensure equal treatment of mediums, the scope of the ECT Act should be extended.[79]

---

[75] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.41 at 55.

[76] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.42 at 56.

[77] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 5 – 7, accessed on 8 May 2017.

[78] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 5.14 at 84 where the SALRC state key concerns 'revolve around issues of authentication and reliability'.

[79] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.42 at 56 where the Law Society of South Africa also believe the ECT Act's application should be extended.

7.3.5 *Should the distinction between "advanced electronic signature" and "electronic signature" be abolished in the ECT Act?*

Although this issue has fallen outside the scope of this research, it has been explored three[80] times in recent peer-reviewed publications in South Africa. Some 16 years after the promulgation of the ECT Act, the *advanced* electronic signature remains a white elephant: *rare and cumbersome*.[81] Its high barrier to entry – together with prohibitive accreditation processes – means that all but a few elite corporate entities will ever use an advanced electronic signatures. A pilot project in 2014 to 2015 which saw the roll-out of advanced electronic signatures to certain attorneys in Gauteng and KwaZulu-Natal also appears to have failed spectacularly.[82] A number of responses to the SALRC recommend the abolition of the distinction between *advanced* electronic signature and *electronic signature*.[83]

In *Spring Forest Trading v Wilberry (Pty) Ltd*,[84] the Supreme Court of Appeal had occasion to deal with the distinction between electronic signatures and advanced electronic signatures, and described an electronic signature as follows:

> The Act describes an electronic signature – which is not to be confused with an advanced electronic signature – as 'data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature'. Put simply, so long as the 'data' in an email is intended by the user to serve as a signature and is logically connected with other data in the email the requirement for an electronic signature is satisfied. This description accords with the practical and non-formalistic way the courts have treated the signature requirement at common law.

Ultimately, the Supreme Court of Appeal found that a person's name, typed at the end of an e-mail (such as, for example: *Sincerely, Bob Marley*) will constitute a *signature* for purposes of s 13(3) of the ECT Act.[85]

---

[80] S Eiselen 'Fiddling with the ECT Act – Electronic Signatures' (2014) 17(6) *Potchefstroom Electronic Law Journal* 2805-2820; Y Mupangavanhu 'Electronic signatures and non-variation clauses in the modern digital world: The case of South Africa' (2016) *SALJ* 133 (4) 853-873; L Swales 'The Regulation of Electronic Signatures: Time for Review and Amendment' (2015) 132 (2) *SALJ* 257-270. See also *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA) para 27 – 29.

[81] Eiselen op cit note 80 at 2814.

[82] These views are my own and based on participation in this project as a consultant attorney for a Durban law firm in 2014 – 2015. I was also a member of the Law Society of South Africa e-law committee from 2012 to 2015 which managed this project.

[83] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.46 – 4.65 at 57 – 60.

[84] 2015 (2) SA 118 (SCA).

[85] Ibid para 28.

The SALRC recommends that the ECT Act review panel discussed above review this issue, together with biometric technology. Electronic signatures have received extensive attention by the LSSA,[86] who are scathing in their criticism of the manner in which the ECT Act regulates the issue by stating:

> when dealing with electronic signatures and the concept of advanced electronic signatures, the drafters of the ECT Act misunderstood the issues.

Be that as it may, as I stated elsewhere in 2015,[87] the distinction in the ECT Act ought to be abolished, and if necessary, certification and authentication to be dealt with in secondary law such as regulations to the ECT Act.

7.3.6 *Should section 15 of the ECT Act prescribe that a data message is automatically admissible as evidence in terms of section 15(2) and a court's discretion merely relates to an assessment of evidential weight based on the factors enumerated in section 15(3)?*

Should a "data message" constitute hearsay[88] within the meaning of section 3 of the Law of Evidence Amendment Act?

As discussed above,[89] in terms of the ECT Act a data message is certainly not automatically admissible – nor should it be. This approach would destroy any semblance of functional equivalence.[90] Our courts have accepted – universally – that s 15 of the ECT Act correctly interpreted does not exempt data messages from the rules regulating hearsay.[91]

As to the question of whether a data message should constitute hearsay in terms of the Law of Evidence Amendment Act,[92] in *LA Consortium*,[93] a full bench of the South Gauteng

---

[86] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 8 – 16, accessed on 8 May 2017.
[87] Swales *SALJ* op cit note 80 at 269 – 270.
[88] See the discussion in chapter 2 above.
[89] Chapter 5 para 5.4.
[90] *Ndlovu v Minister of Correctional Services* supra note 47 at 173 – 174; *LA Consortium* supra note 31 para 11 – 15; *S v Brown* supra note 31 at para 18; *S v Meyer* supra note 31 at para 299; South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.68 at 63.
[91] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.69 at 63 where the seminal *Ndlovu v Minister of Correctional Services* is cited as authority.
[92] Act 45 of 1988.
[93] *LA Consortium* supra note 31 para 13.

High Court answered conclusively: '[A]ny hearsay contained in a data message must pass the criteria set out in section 3 of the Law of Evidence Amendment Act 45 of 1988.' As noted above,[94] if data messages were to be exempt from the rules regulating hearsay this would clearly elevate electronic forms of evidence over other traditional forms of evidence.[95] All courts and commentators are ad idem that if a data message depends upon the credibility of a person, it must be considered hearsay. This follows from the definition in the Law of Evidence Amendment Act,[96] which defines hearsay as: '[E]vidence, whether oral or in writing, the probative value of which depends upon the *credibility* of any person other than the person giving such evidence' [my emphasis].

Consequently, where the *credibility* of data message evidence does not depend on a person – for example in automated telephone records[97]– it cannot be subject to hearsay considerations. Theophilopolous points out[98] that these distinctions created in *Ndiki*[99] and *Ndlovu*[100] (using terminology derived from the Law of Evidence Amendment Act) are problematic because they are ambiguous.[101] Ambiguity and the precise choice of terms notwithstanding, a survey of the international position[102] suggests that a distinction between automated computer output (akin to real evidence) and computer output subject to hearsay (akin to documentary hearsay) is necessary.

[94] See the discussion in chapter 3 para 3.4.
[95] *S v Brown* supra note 31 para 16 – 18; *Ndlovu v Minister of Correctional Services* supra note 47 at 172.
[96] Section 3 of Act 45 of 1988.
[97] *Ex parte Rosch* [1998] 1 All SA 319 (W) 328 where telephone records were admitted as real evidence. The court notes: 'The printout is real evidence in the sense that it came about automatically and not as result of any input of information by a human being. There is therefore no room for dishonesty or human error. The printout in the present case is similar to the radar diagram produced in the English case of *The Statue of Liberty: Owners of* the *Motorship Sapporo Maro v Owner of Steam Tanker, Statue of Liberty* [1968] 2 All ER 195 (PDA) where such a document was admitted as evidence'. In a South African context, see *S v Ndiki* supra note 43 para 7; *S v Brown* supra note 31 at para 18.
[98] Theophilopolous op cit note 58 at 474.
[99] *S v Ndiki* supra note 43.
[100] *Ndlovu v Minister of Correctional Services* supra note 47.
[101] Theophilopolous op cit note 58 at 474.
[102] Discussed above in chapter 3.

7.3.7 *Should the ECT Act (or other relevant legislation) make a clear distinction between mechanically produced evidence without the intervention of the human mind (akin to real evidence) and mechanically produced evidence with the intervention of the human mind (hearsay)?*[103]

There is no clear consensus on how to treat data produced by a largely automated process; as pointed out by the SALRC: 'There is less consensus… on the approach to be followed when the probative value of a statement in a printout is dependent upon the "credibility" of the computer itself.'

As recently pointed out in the Western Cape High Court by Bozalek J in *S v Brown*:[104] 'the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document.' Crucially, when considering the distinction between real and documentary electronic evidence, the court in *Ndiki*[105] referred to a 1998 academic article by Bilchitz[106] and suggested *obiter,* that because it may be difficult to make the distinction between real and documentary electronic evidence at times, all computer output should be regarded hearsay. The court noted that if all electronic evidence were hearsay, then:

> It does away with the necessity to distinguish in each case between what would constitute hearsay evidence and what real evidence, a task that is not always without its difficulties. I do not, however, find it necessary for purposes of this judgment to make any finding in this regard.

This *obiter* statement notwithstanding, it must be borne in mind that *Ndiki* is also clear authority for the proposition that automated data message evidence should be classified as real evidence.[107]

In *LA Consortium*,[108] the court was faced with what will probably be the norm in many civil and criminal trials involving data message evidence: a combination of automated data messages with no human input, and hearsay data messages where the credibility of the data depends on a person. The court noted: 'The data messages relied upon in this case are not only

[103] See the discussion in chapter 2 and 3 above.
[104] *S v Brown* supra note 18 para 18.
[105] *S v Ndiki* supra note 43.
[106] D Bilchitz 'Law of Evidence' in C Lewis et al (eds) *Annual Survey of South African Law* (1998) 735-821. See also Hofman & de Jager op cit note 17 at 776 – 777; Theophilopoulos op cit note 58 at 464.
[107] *S v Ndiki* supra note 43 para 7.
[108] *LA Consortium* supra note 31 para 12.

real evidence but includes hearsay' and that '[t]he definition of 'data message' in s 1 [of the ECT Act] is sufficiently wide to include not only real, but also hearsay evidence.'[109]

As discussed above in chapter 3, the position that all computer-generated evidence is hearsay is not consistent with South African case law,[110] and international best practice[111] where data messages are routinely categorised as real evidence *if* the data message is automated and requires substantially no human input. Ultimately, in a South African context, although it is clear that a distinction should be made between automated data messages and data messages subject to human input, the question as to how to best achieve this remains unanswered. For the short term, it is prudent for the ECT Review committee referred to above to consider this issue with a mandate to determine how best to achieve this distinction. As I see it, there are no alarming issues present at the moment, and the distinction can be achieved within the current legal framework (leaving a measure of interpretation to the judiciary when a particular court determines whether evidence is admissible or not).

Moreover, the SALRC[112] notes that a handbook on obtaining and producing electronic evidence will provide clarity for practitioners and judicial officers. This recommendation is sensible, and the ECT Review committee ought to delegate this task to the appropriate persons or group.

7.3.8 *In view of the fragmented nature of case law focusing on authentication of specific types of evidence, is a review of the principle of authentication necessary in view of the nature and characteristics of electronic evidence that raise legitimate concerns about its accuracy and authenticity?*

The SALRC is of the view that the ECT Act is somewhat 'laconic' on best practice and international standards.[113] It should be stressed that both the LSSA[114] and the NPA[115] assert

[109] Ibid.
[110] For example, see the cases cited in note 31 above. See also *S v Ndiki* supra note 43 para 7 where the ratio finds that computer generated evidence can be real in nature if it 'depends solely upon the reliability and accuracy of the computer itself.'
[111] Chapter 3 para 3.7 above.
[112] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.104 at 70.
[113] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.109 at 72.
[114] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 19 – 21, accessed on 8 May 2017.
[115] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.21 at 51 where the NPA states: 'There is no real reason why there should be a separate piece

that a new Law of Evidence Bill is not necessary at present. The LSSA points out: 'The granularity that may be desirable should rather be dealt with in secondary law, for instance regulations or rules of court.' The LSSA argues that courts should develop and test authenticity further as required.[116] The position of the LSSA and NPA is far more desirable in the short term while electronic evidence (and the manner in which local and international courts deal with the various issues) matures further. Additional case law and academic opinion will point out lacunas or issues that require urgent attention. In the short term, the current position is satisfactory in that a court will be seized with determining whether a data message is authentic (using its discretion to determine authorship). For example, in *S v Meyer*,[117] the court noted:

> The ECT Act does not attempt to enumerate any specific criteria that should be applied, this is due to the fact that there are different types of data messages so it would be difficult to formulate prerequisites for authentication which would apply to all types.

As discussed above,[118] in *Ndlovu v Minister of Correctional Services*,[119] when dealing with data messages, the court interpreted the requirement of authenticity to mean 'proof that a document was written or executed by the person who purports to have done so'.[120] Most academic opinion suggests that authenticity relates to tendering evidence relating to authorship.[121] As a result, in *S v Meyer*,[122] the court again confirmed that authenticity relates to evidence as to the authorship of the particular data message. Further, it is submitted that a party ought to also adduce evidence that identifies the use of software and/or manual methodologies that prevented the data from being altered prior to its presentation to court.[123] The fragmented case law notwithstanding, there is no reported decision (post the promulgation of the ECT Act) in which authentication has proved a particular issue for courts who will often rely on expert evidence. Consequently, for the short-term, other than guidelines for

---

of legislation to provide for the admissibility of electronic evidence in criminal and civil proceedings outside the provisions of the ECT Act'.

[116] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 19 – 21, accessed on 8 May 2017.

[117] *S v Meyer* supra note 31 para 306.

[118] See chapter 5 above.

[119] Supra note 31 at 174.

[120] *S v Brown* supra note 18 para 19 - 22.

[121] Schwikkard & van der Merwe op cit note 17 at 434 – 435; Zeffertt and Paizes op cit note 17 at 837 – 838; R Davey & L Dahms-Jansen *Social Media in the Workplace* (2017) at 290.

[122] *S v Meyer* op cit note 31 para 306.

[123] *S v Meyer* op cit note 31 para 305. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.105 – 4.115 at 70 – 74 for *issue 8*, a discussion of authentication. See further, Ireland Law Reform Commission Consultation Paper 57 *Documentary and Electronic Evidence* (2009) at 141 – 146 for a discussion of authentication in the context of electronic evidence.

practitioners and judicial officers (and amendment to existing legislation as noted above) the position is adequate.

7.3.9 *Should section 15(4) be reviewed to give a restrictive interpretation to the words "in the ordinary course of business"?*

Should section 15(4) as applicable in criminal cases be reviewed in view of the current law on reverse onus provisions?

As discussed above,[124] section 15(4) has been described by a full bench of the South Gauteng High Court as 'controversial'.[125] In the court a quo, in *MTN Service Provider (Pty) Limited v LA Consoritum & Vending CC,*[126] print-outs from accounting software were declared admissible in terms of section 15(4) of the ECT Act. However, on appeal, in *LA Consortium*[127] the South Gauteng High Court took a different view. Although the print-outs were ultimately admissible, the appeal court in Johannesburg held that any hearsay contained in a data message must be admitted to court via an exception contained in s 3 of the Law of Evidence Amendment Act. In my view, this interpretation does not take account of the literal wording of section 15(4) which appears to be an intentional step by South Africa's legislature to subjugate the hearsay rule with an internationally acceptable (and common-place) *business records* exception.

In so far as the SALRC proposals are concerned, the recommendation is the repeal of section 15(4) and the introduction of a new piece of legislation. Regarding a *restrictive interpretation*[128] on the phrase 'ordinary course of business', both the LSSA and the NPA adopt a pragmatic and common-sense approach with their suggestions. The LSSA are of the view that a restrictive interpretation is not necessary, and that it may 'hamper electronic commerce'. Further, it is clear that the onus or proof[129] (read together with our flexible common law approach) will accommodate the inherent differences between civil and criminal proceedings – as noted by the SALRC, 'the NPA expresses a similar view to that of the LSSA.'[130] In

[124] See chapter 3 para 3.5.4 above.
[125] *LA Consortium* op cit note 31 para 18.
[126] 2011 (4) SA 562 (W).
[127] *LA Consortium* op cit note 31. See also Hofman & de Jager op cit note 17 at para 18.26 at 772 – 774.
[128] This would keep s 15(4) intact, but enjoin courts to interpret the provisions in a *restrictive* manner.
[129] Discussed above in detail in chapter 6 para 6.2.
[130] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.118 at 75.

addition, on behalf of Nedbank, it is suggested that s 15(4) should not be given a restrictive interpretation, nor should it be reviewed.[131]

Conversely, Legal Aid and the South African Police Services believe s 15(4) may be unconstitutional as it creates a 'reverse onus'.[132] A *reverse-onus* provision is one where, according to the Constitutional Court in *S v Zuma*,[133] a 'presumption with the legal burden of rebuttal on the accused' is created. Are all reverse-onus provisions unconstitutional? The Constitutional Court[134] in *S v Bhulwana*[135] rejected the notion that a reverse-onus provision could be 'read down' to an evidential presumption. However, the Constitutional Court when considering this issue for the first time in the seminal case of *Zuma*[136] noted that reverse-onus provisions are not automatically unconstitutional,[137] and noted:

> [This judgment] does not decide that all statutory provisions which create presumptions in criminal cases are invalid. This Court recognises the pressing social need for the effective prosecution of crime, and that in some cases the prosecution may require reasonable presumptions to assist it in this task. Presumptions are of different types. Some are no more than evidential presumptions, which give certain prosecution evidence the status of prima facie proof, requiring the accused to do no more than produce credible evidence which casts doubt on the prima facie proof.

Although a reverse-onus clause may survive constitutional scrutiny in certain limited instances, for the most part, the Constitutional Court has been consistent[138] in its finding that these types of clauses offend the presumption of innocence. Paizes suggests[139] that in criminal matters, these types of reverse onus clauses should never operate and opines as follows:

> It is my wish, in short, that the courts recognise the foundational nature of the proposition that the onus should rest on the state and, moreover, treat it as an absolute rule permitting of no exceptions. Absolute rules are out of fashion in our post-constitutional culture. But there is a place, in my view, for at least this one.

---

[131] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.119 at 75.
[132] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.120 – 4.121 at 76.
[133] 1995 (2) SA 642 (CC) para 19.
[134] I Currie & J de Waal *The Bill of Rights Handbook* 6 ed (2013) 189 – 190.
[135] 1996 (1) SA 388 (CC) para 25–29.
[136] Supra note 133.
[137] Supra note 133 para 40.
[138] 1996 (2) SA 464 (CC) para 10. See also Currie & de Waal op cit note 159 at 758.
[139] Paizes op cit note 57 at 278.

However, the question remains whether s 15(4), in criminal matters, is a justifiable limitation of the presumption of innocence.[140] For example, in *S v Meaker*[141] a reverse onus provision in the Road Traffic Act 29 of 1989 was found to be a permissible departure – in terms of s 36 of the Bill of Rights – from the presumption of innocence.[142] However, holistically, given the Constitutional Court's jealous protection of the presumption of innocence, jurisprudence since the first reverse onus case of *Zuma* in 1995 suggests that a provision of the nature of s15(4) in criminal cases is unlikely to be justifiable in terms of s 36 of the Bill of Rights. Academic opinion appears to favour an approach that s 15(4) should not apply to criminal matters.[143]

In summary, in so far as s 15(4) of the ECT is concerned, holistically, the hearsay exceptions should be better aligned and the Law of Evidence Amendment Act, the Civil Proceedings Evidence Act, and the Criminal Procedure Act must be amended to make specific reference to data messages: consequently, amendment is certainly required in some areas,[144] but as pointed out above, a review of recent case law and foreign developments suggest that the current regulatory regime is satisfactory, and the drastic reform suggested by the SALRC is not required at this time; the approach put forward by the LSSA, the NPA, and the banking industry should be preferred.

7.3.10 Should the law of evidence prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breath-testing devices)?

As discussed above,[145] in *Trustees for the time Being of the Delsheray Trust v ABSA Bank Limited*[146] the Western Cape High Court found: a 'presumption [of reliability] is not generally applied in South African case law … but the underlying principles … are indeed established.' It based this decision on an Appellate Division case in relation to judicial notice.[147] Rather than a flexible common law approach, the SALRC suggest a statutory presumption of

[140] Paizes op cit note 57 at 275; Currie & de Waal op cit note 159 at 756.
[141] 1998 (2) SACR 73 (W).
[142] See also *S v Manamela* 2000 (1) SACR 414 (CC) where a divided Constitutional Court bench considered reverse onus provisions.
[143] Hofman op cit note 20 at 267 – 268; Theophilopolous op cit note 58 at 476; Hofman & De Jager op cit note 17 at 780 – 781; Paizes op cit note 57 at 273 – 278.
[144] My findings are summarised below in chapter 8 para 8.2.
[145] See chapter 4 para 4.5.
[146] [2014] 4 All SA 748 (WCC).
[147] *S v Mthimkulu* 1975 (4) SA 759 (A).

reliability applicable to *only* civil law.[148] The current legal position, reading in the common law should be preferred over these proposed amendments. South Africa ought to only implement law reform that applies to both civil and criminal proceedings. In the short term, the ECT Act, read together with the common law, is far superior to the proposed SALRC reforms which will leave a lacuna in relation to the regulation of criminal law in this context, and potentially introduce confusion to civil proceedings.

7.3.11 In general, are the provisions in the ECT Act sufficient to regulate the admissibility of computer generated evidence?

In general, the banking industry appear satisfied with ECT Act. Advocate Eiselen, on behalf of Nedbank, [149] concludes:

> We submit that in general the provisions of the ECT Act have proven to be effective and sufficient to regulate the admissibility of electronic evidence. We submit that there may be a need for some smaller amendments to the Act, especially in regard to section 13 dealing with electronic signatures.

Holistically, the LSSA also appear satisfied with the ECT Act,[150] but insist on minor amendment and further amendment to the rules of court (to be discussed below):

> The LSSA is of the view that the ECT Act is sufficient to regulate the admissibility of computer generated evidence. However, the LSSA also supports the recommendation that the Rules Board consider amendments to the rules of court to provide for the discovery and inspection of electronic documents and submits that such revisions would greatly promote the administration of justice.

A private company Infology[151] further raises a valid issue relating to discovery by noting an issue in relation to metadata:[152]

---

[148] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.125 – 4.133 at 78 – 79. The provisions of the proposed *Law of Evidence Bill* are discussed below at para 7.4.

[149] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.135 at 80.

[150] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 26, accessed on 8 May 2017.

[151] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.139 at 81.

[152] According to an Internet version of the Oxford English Dictionary, *metadata* is defined as: 'A set of data that describes and gives information about other data.' *https://en.oxforddictionaries.com/definition/metadata*, accessed on 12 May 2018. For example, metadata on a word document will reveal when it was created (which may reveal whether it was used on a Macintosh or Windows machine), when it was last modified, when it was

> A printed copy of a data message —would lack the embedded information [metadata] normally retained in an electronic copy that evidences 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

Consequently, when assessing data messages, it can be said that metadata must be analysed to reach a credible result. Although the ECT Act makes provision for an original, and creates a statutory best-evidence rule, the rules relating to discovery require amendment, and in this context, the SALRC state:

> Infology refers to legislation and rules regulating the discovery and production of evidence, in particular Rule 35 of the Uniform Rules applicable to the High Court. Rule 35 regulates such discovery and inspection, but does not expressly address the manner or format in which discovered documents must be produced, except at the hearing of a matter where the original may be required by a party to the proceedings. The production of an original data message is further circumscribed by section 14 of the ECT Act, read with section 4(2)(a). Infology argues that there are significant shortcomings in the procedural rules regulating the discovery and production of electronically stored evidence.

The South Gauteng High Court in Johannesburg[153] notes:

> The purpose of discovery is to enable the parties to become aware of documentary evidence that is available and to identify factual issues. In addition, discovery results in the production of documents that can be used in the course of interrogation of witnesses.

Cassim[154] further points out that the purpose of discovery is to ensure that parties to proceedings are aware of all *relevant* information or documentation that exists prior to any trial so that parties can prepare properly.[155] It is undeniable that information communication technologies have changed the way society interacts and the law must adapt.[156] Part of this adaption must entail the appropriate and adequate discovery of information stored electronically. However, currently, the rules relating to discovery require further and direct amendment to accommodate full and proper discovery; and for the production of metadata where appropriate. Many lawyers *still* – in 2018 – 'drown unnecessarily in seas of paper'.[157]

---

last opened, where it was stored, its size, access permissions, and potentially, a host of other useful information (the document I am typing in, for example, was created on 3 April 2018 on a Macintosh machine – one can also determine the date it was last modified and various other critical pieces of information. Furthermore, on a PDF (portable document format), one is able to determine the total number of pages in the file, whether it is encrypted, encoding software, and when the document was last opened.

[153] *STT Sales (Pty) Ltd v Fourie* 2010 BIP 298 (GSJ) para 14.

[154] Cassim op cit note 52 at 20.

[155] Ibid.

[156] R Susskind *The End of Lawyers? Rethinking the Nature of Legal Services* (2010) at 1.

[157] Hughes op cit note 51.

The advantages and efficiencies of electronic discovery are numerous, and as Hughes correctly notes:

> Ask a lawyer a meaningless factual question like what the weight of the largest pumpkin ever grown is and he would probably be able to turn to the internet to produce the correct answer within 60 seconds. Why then should a lawyer take any longer to determine more important facts, like whether a potentially relevant document exists within his client's documentary records? Electronic information management rewards practitioners with significant efficiency benefits that clients have come to appreciate and are now beginning to expect.

However, as noted by Cassim, there are many perceived problems with electronic discovery, including: '[T]he huge volume and number of data messages; the problem of metadata; the changing status of electronic contents; the impact of technological changes on data; the use of different locations of electronic data, and the expenses involved'.[158]

Be that as it may, Rule 35 of the Uniform Rules of Court still refers to 'tape recordings'. This should be replaced with *data messages*. Moreover, Rule 35 should include provision for the mandatory production of metadata as part of the discovery process. If a party to proceedings is of the reasonable view that full and proper metadata has not been disclosed, courts should be able to direct the other party to properly discover. Although recent cases interpret 'tape recordings' and documents widely,[159] direct reference should be made to data messages.

In *Makate v Vodacom (Pty) Ltd*[160] the court found that electronic documents fell within the scope of discovery of Rule 35 of the Uniform Rules of Court, and this finding illustrates how courts have adapted legislation designed in a time before computer technology to fit the needs of society today. As a result of outdated terminology in the court rules, Infology makes the following recommendation in the context of electronic discovery:[161]

> [Substitute] the phrase "documents and tape recordings" with the phrase "documents and tape recordings including electronically stored information and related metadata";
>
> inserting the following words at the end of section 35(2)(a): —…and the manner in which such documents and tape recordings are retained including, in the case of electronically stored information, the electronic file formats in which they are retained"; and

[158] Cassim op cit note 52 at 22 – 23.
[159] Cassim op cit note 52 at at 26.
[160] 2014 (1) SA 191 (GSJ).
[161] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 4.139 at 81.

> inserting the words — "in a format reasonably specified by such party or, if not so specified, in the form in which they are ordinarily retained or another reasonably usable form" after the words "make available for inspection" in Rule 35(6).

Rule 35(1) currently reads:

> (1) Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within twenty days of all documents and tape recordings relating to any matter in question in such action …

In these critical court rules, 'documents and tape recordings' should be replaced with *documents and data messages*. As discussed above[162] the definition of data messages is wide enough to include all electronically stored information. Moreover, all instances of 'tape recordings' should be replaced with 'data message', and as Infology suggests above, the mandatory production of metadata (although I suggest different terms – the use of the term tape recordings is archaic and should be removed). Finally, provision must be made for parties to inspect data messages, and data message systems that may potentially hold metadata.

In respect of the magistrates' courts, Rule 23 of the Magistrates Court Act 32 of 1944 reads as follows:

> (1) *(a)* Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within 20 days of all documents and tape, *electronic, digital* or other forms of recordings relating to any matter in question in such action... [my emphasis].

It together with the High Court Rule 23 ought to be amended to remove reference to 'tape recordings', and to include 'data messages'. Moreover, once data messages is inserted in Rule 23 the superfluous phrase 'electronic, digital or other forms of recordings' may also be removed.

As with the High Court Rules, two further amendments are crucial: 1) the mandatory provision of metadata in discovery; and 2) provision for parties to inspect data messages (and/or data message systems where appropriate).

The SALRC recommend that the Rules Board for Courts of Law[163] assisted by a standing committee or working group assess amendments to the rules of court that may be required. This proposal should be supported and implemented as soon as possible.

[162] See chapter 2 para 2.1 above.
[163] A statutory body established in terms of Rules Board for Courts of Law Act 107 of 1985.

7.3.12 Overview of law reform

The SALRC is correct that law reform is desirable in this environment – but my view is that instead of reform in the guise of a new Law of Evidence Bill, South Africa ought to rather adopt a more pragmatic approach and retain the current regime with reform of current legislation to foster greater clarity and consistency. These issues are immensely complicated, carry great importance for commerce and evidence in general, and there are no straight forward answers. Before implementing drastic reform, South Africa ought to adopt a 'wait-and-see' approach: the current position is adequate (with minor reform of the current relevant legislation), and a more comprehensive review is ideally required before implementing drastic law reform. This approach will allow South Africa a further period of two to five years to monitor international trends,[164] and follow the development of emerging jurisprudence in this rapidly-developing area.

As noted by the Law Society of South Africa in its scathing criticism of *Discussion Paper 131: Review of the Law of Evidence*, an 'abundance of caution'[165] is required before drastic reform. The LSSA support the retention of the current regulatory landscape, with minor reform. Moreover, that a *further* comprehensive review of the ECT Act be conducted.

South Africa should be cautious when deviating from the Model Law, 1996 and must have cogent reasons to do so, particularly where such change does not appear to be supported by the majority. Electronic evidence covers 'every nook and cranny of our daily lives' and South Africa must ensure 'harmonisation of our law with developments in other countries'.[166] Moreover:

> there are vast tracts of the ECT Act, not based on the Model Law, which were ill-conceived at the time of inception, have never been implemented and should be dealt with by other entities within government.[167]

---

[164] For example, see the discussion in paragraph 5.4.2 above where it is concluded that South Africa should: reject the notion that all electronic evidence is hearsay; confirm that electronic evidence is not automatically admissible; and confirm that all electronic evidence (real or documentary) should be subject to authentication (prima facie proof that the evidence is what it purports to be).

[165] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 34, accessed on 8 May 2017.

[166] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 2 - 3, accessed on 8 May 2017.

[167] Ibid 2 – 3.

Simply put: to answer the overall question posed by the SALRC in terms of the adequacy of the ECT Act and its ability to *regulate the admissibility of computer generated evidence*, in general, the ECT Act is sufficient in the short term. However, there are several areas that require amendment to foster greater consistency, clarity, and certainty.

7.4 AN ANALYSIS OF THE PROPOSED LAW OF EVIDENCE BILL

It is necessary to consider the Law of Evidence Bill proposed by the SALRC,[168] which is intended to clarify, consolidate and align the rules for the admissibility of business records and electronic evidence, while leaving certain other existing legislation in tact. For example, the admissibility of official and public documents. It is express that the common law applies where appropriate. Contrary to the stated aim of the Law of Evidence Bill, for reasons set out below, the intended legislation requires further consideration, and should be held in abeyance until at least a comprehensive review of the ECT Act as envisioned in issue 1 of the SALRC Discussion Paper 131 has been completed by a diverse, multi-skilled group including experienced *practicing* legal professionals, and academics, with experience in this environment.

7.4.1 Section 1: Definitions

On a review of the SALRC 2010 *Issue Paper* 27,[169] and the SALRC's 2014 *Discussion Paper* on the review of the law of evidence,[170] it is not entirely clear why a definition is required for the word *copy* in an ever-evolving digital context. What clarity is required? Whether a data message is original, or a copy, should make very little difference to authentication. Originals can be infinite with digital data, and an original is no guarantee that the data can be trusted. These terms are no longer so relevant as they once were (with paper). Authentication of evidence is key; South Africa ought to move away from definitions configured for a traditional, paper-based world. Importantly, one must bear in mind that our courts have, thus far,

[168] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) 89 – 95.
[169] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) para 6.13 at 33.
[170] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) at 54 – 55.

satisfactorily dealt with the reception of electronic evidence since the promulgation of the ECT Act. The SALRC[171] itself states:

> Electronic evidence arguably requires a shift in emphasis away from the exclusion from admissibility based on hearsay and the best evidence rule, to the question of reliability. For reliability, the concepts of authentication and integrity become important. This is particularly so given the concern that electronic records may be more susceptible to undetected modification than are traditional paper-based records

In addition, some further issues to consider with the proposed definitions:

i) The proposed Law of Evidence Bill only mentions an electronic signature once in the entire Bill [at s 4 (2)(i)(b)] Why define *Electronic Signature* when it is comprehensively dealt with in s 13 of ECT Act and already defined therein?

ii) The Law of Evidence Amendment Act[172] adequately deals with hearsay evidence and the Law of Evidence Bill repeats, verbatim, the definition of hearsay evidence. Although this issue does require alignment, and consistency, there are less disruptive and far easier methods to achieve clarity in so far as electronic hearsay evidence is concerned – amendment to existing legislation, for example. Further, there is no need to introduce a definition for hearsay evidence in this Bill (it already exists), nor is there a need for this Law of Evidence Bill to regulate the giving of notice for hearsay or documentary evidence. These issues, assuming they even need to be regulated in the first place, should be dealt with by amendments to existing legislation or procedural rules of court.

iii) Why define *writing* when it is adequately dealt with in the ECT Act? What basis exists to define the term *statement* and *records*? How will these definitions align themselves with the ECT Act *data message* definition? How will these definitions foster or hamper international trade? What rationale exists to deviate from the Model Law, 1996?

---

[171] Ibid at para 3.49 at 40. Note that the Law Society of South Africa 'wholeheartedly' endorse this position, see Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 34, accessed on 8 May 2017.

[172] Section 3 of Act 45 of 1988.

iv) The definition for *computer system* will conflict with the proposed definition in section 1 of the Cybercrimes Bill. Further, what basis exists to define *electronic documents system*? Before venturing out of the comfort of the Model Law, 1996 with ill-conceived definitions, South Africa ought to adopt a more rigorous review. This further review must consider more recent case law, and international developments first; then to remedy the short-comings in the ECT Act – practicing, experienced legal practitioners must also be involved.[173]

7.4.2 Application of Act

Similar to section 4 (sphere of application) of the ECT Act, or article 1 of the Model Law, 1996, legislation of this nature should simply state it applies to all data messages unless otherwise expressly stated.

The *strict rules of evidence* is a term not defined in South African statute and is open to interpretation. In what context would the *strict rules of evidence* not apply? And, in that case, what rules governing electronic evidence and hearsay would apply?

Moreover, s 2(2) is open to interpretation. It currently states its does not affect any law 'except the rules relating to hearsay, authentication and best evidence in relation to certain types of documentary evidence'. This is too wide and vague. It should be removed.

7.4.3 Admissibility of hearsay evidence[174] and notice of intention to produce

Section 3 (1) of the Law of Evidence Bill, almost verbatim, repeats the contents of s 3 of the Law of Evidence Amendment Act, while s 3(2) closely mirrors s 3(3) of the Law of Evidence Amendment Act. The *primary* difference is that the proposed legislation requires a party to give notice of their intention to produce hearsay evidence.

In terms of s 6 of the Law of Evidence Bill, notice must be given in writing and in 'sufficient' time. Section 6 (3) contains several exceptions where notice may be dispensed

[173] Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf* at 34, accessed on 8 May 2017. See also South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) at para 4.21 at 51.

[174] See chapter 5 above.

with, and s 6 (6) outlines some of the potential consequences for lack of compliance with the proposed section.

The current position, with minor amendment, is far superior to the proposed solution, which requires more in-depth analysis and discussion.

7.4.4 Admissibility of business records and repeal

Section 4 is intended to be a replacement for s 15(4) of the ECT Act. As discussed in detail above,[175] this section has been referred to as 'controversial'.[176] However, it is an internationally accepted legislative mechanism,[177] and as Lamont J points out, is an intentional step by South Africa's legislature to subjugate the hearsay rule[178] (whether in the ECT Act or in this proposed legislation).

That aside, the Law of Evidence Bill recommends the repeal of s 15(4), and it appears the drafters were unsure whether to repeal s 15 entirely. Section 11, 'Repeal of sections of statutes' confirms that the SALRC is unclear as to whether s 15 should be repealed entirely, and if so, whether it should be replaced by an amendment Bill.

As discussed above in chapter 5, a comprehensive review of all existing case law dealing with s 15 of the ECT Act from inception of the act to December 2018 suggests the ECT Act, and s 15 in particular, is no impediment to the reception of electronic evidence, and it would be premature to repeal s 15 before a further review of recent trends and developments.

7.4.5 Evidence produced by electronic means; Authenticity and integrity

Section 5 of the Law of Evidence Bill attempts to distinguish between automated machine generated evidence and evidence which is subject to the credibility of a person. The key question whether electronic evidence is hearsay relates to whether its credibility depends on a person, or a machine. Consequently, and in this context: what does *wholly* generated by a machine mean?

At some point in its development and creation, a human will always be involved in a computer program or electronic device in its design, implementation, maintenance,

[175] See chapter 3 above.
[176] *LA Consortium* supra note 31 above para 12.
[177] See 3 above.
[178] *Director of Public Prosecution v Modise* 2012 (1) SACR 553 (GSJ).

configuration etc. Rather, if a section of this nature is to be implemented, the word *substantially* should be inserted instead of *wholly*, so that it would read: A statement which has been *substantially* generated by a machine, device or technical process does not constitute hearsay evidence.

In so far as integrity and authenticity is concerned, and as discussed in detail above,[179] the ECT Act provides a framework that is adequate for the time being and these issues are best left, for now, to the courts to interpret (which has served South Africa satisfactorily to date), or to create secondary law in the form of regulations to the ECT Act, or amendments to existing law. It is now globally accepted that evidence produced substantially or partly by a machine, device, or technical process is *potentially* admissible. And not since the 1970's and *Narlis*,[180] has South Africa had a situation where evidence is excluded solely on the grounds of it being electronic in nature. The judiciary's interpretation of these issues does not appear, currently, to suggest there are any major problems or lacunas. It may be prudent to allow further time to elapse, a further review to take place, and then to revisit this issue. A number of options could be taken: an amendment Act (similar to the Law of Evidence Amendment Act 45 of 1988) that deals only with these two issues; an amendment to the ECT Act; regulations to the ECT Act; or entirely new legislation. However, the codification approach, as the SALRC has noted, is a route that will require a plethora of further resources: with this in mind, what benefit would such an undertaking achieve? To use a business analogy, the costs and effort far outweigh the potential profit or benefit, and this project should be shelved for the time-being.

7.4.6 *General comment on the Law of Evidence Bill*

Although the aims of the Law of Evidence Bill are laudable, it would be premature to enact the legislation as it currently stands, and if codification and aggressive reform is the route South Africa elects to take, then this legislation requires further thought, consistency, and alignment with existing legislation, and *comprehensive* amendment. Portions of the Bill appear to be a copy and paste of various international laws, brought together to make one inconsistent end-product that creates a cacophony of noise in one's head when reading it. South Africa should not be seeking to codify trite and settled principles. Moreover, one should be wary of over-regulating.

[179] See chapter 5 above.
[180] 1976 2 SA 573 (A).

7.5 CONCLUSION

Although amendment is required in certain areas, aggressive reform is not the prudent option at this stage in the development of e-commerce jurisprudence. A further review is required, analysing more recent case law, and international trends and developments. This will allow South Africa to enact consistent and clear legislation. Consequently, and as pointed out by the LSSA and NPA, the Law of Evidence Bill is not the best option at this stage. Option 1 as suggested by the SALRC (a more cautious amendment of the existing environment) will facilitate a clearer and more certain regulatory framework.

CHAPTER 8

8.1 OVERVIEW

The regulatory environment governing electronic evidence is in need of reform. In addition, given rapid technological development, and the importance of e-commerce to South Africa's economy, it is prudent to establish a working-group comprised of multi-disciplinary experts to ensure periodic and thorough reviews of e-commerce related legislation.

Although reform is required, an overhaul of the current legal position by promulgating legislation similar to the *Law of Evidence Bill* (see Annexure A) may be harmful for South African law. Rather, a more thorough review should be undertaken (including multi-disciplinary experts and practicing legal professionals), more recent case law must be analysed, and international trends should be monitored. In the short term, current legislation ought to be amended to ensure certainty, clarity, and consistency with international best practice.

8.2 SUMMARY OF FINDINGS

8.2.1 Functional equivalence, and the definition of data message[1]

In the context of ICT legislation, South Africa ought to ensure it promulgates law that achieves functional equivalence in a technologically neutral manner. The key definitional concept in the ECT Act is *data message*. The promulgation of the current version of the Cybercrimes Bill will result in South Africa having two definitions for the term. This oversight, although of little practical consequence, should be corrected. In addition, the definition itself should remain concise and simple.

8.2.2 Hearsay electronic evidence[2]

South African courts and academics have been almost entirely ad idem in their view that electronic evidence can constitute hearsay within the meaning of the Law of Evidence Amendment Act. Moreover, electronic evidence is not automatically admissible. The ECT Act does however provide a business records exception (which is common around the world),

[1] Chapter 2 above.
[2] Chapter 3 above.

and evidence will be rebuttably presumed true if the provisions of the relevant section are complied with.

To determine whether electronic evidence is real or documentary in nature, one must consider the nature of the data message, and the requirements of the relevant legislation (or common law requirements). If the electronic evidence is largely automated or relies substantially upon a machine, computer, or mechanical process, it should be classified as real evidence. Conversely, if the data message depends upon human assertions or observations, then it should be documentary evidence.

The issue that remains unclear relates to the admissibility of real evidence in the form of data messages. On the one hand, in cases that follow the logic of *Baleka (3)*, real evidence in the form of a data message need only be relevant in order for it to be admissible. Conversely, on the basis of *Ramgobin's* rationale, real evidence in the form of a data message must be relevant and authentic. As is the case with Canada,[3] and the United States of America,[4] South Africa ought to adopt an approach where real electronic evidence must be authenticated prior to it being admissible. As correctly observed in *Tienda v State*, in the context of electronic data, 'evidence has no relevance if it is not authentically what its proponent claims it to be.'[5]

8.2.3 A presumption of regularity[6]

The ECT Act adequately facilitates the admission of electronic evidence. However, the ECT Act applies in addition to the common law, and as was the case in *Delsheray Trust v ABSA*, a court has the ability to receive electronic evidence via the express mechanism created in the ECT Act, or it can equally rely on the common law.

In the absence of evidence, the presumption that mechanical instruments were working at the relevant time is probably too simplistic. In 2018, the advanced nature of technology means we cannot simply accept 'the machine was working'. If the common law is to be relied upon, a person must show the relevant court, whether on affidavit or via viva voce evidence,

[3] Section 31.1 of the Canada Evidence Act, 1985 which provides: 'Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be.'
[4] *Lorraine v Markel American Insurance Company* 241 FRD 534 (2007) at 541 – 542; *Tienda v State* 358 SW3d 633 Texas Criminal Appeal (2012) at 639.
[5] *Tienda v State* supra note 4 at 638.
[6] Chapter 4 above.

that the evidence is reliable and can be trusted – there must be some basis for a court to confirm its reliability and veracity (as is the case with, for example, Canada).[7]

8.2.4 Authentication and weight of electronic evidence[8]

Relatively speaking, in terms of e-commerce, a decade is a significant period of time. The ECT Act has been in place since 2002, but that notwithstanding, the admissibility and weight of data message evidence does not require drastic overhaul – and it does not require the entire repeal and re-promulgation as suggested by the SALRC in the Law of Evidence Bill (Annexure A). The current provisions are adequate for the short term. In addition, if South Africa is to move away from the Model Law, 1996, it should only do so with cogent reasons.

8.2.5 Is it appropriate to apply different evidentiary considerations to electronic evidence in civil and criminal proceedings?[9]

Other than those existing at common law there is no reason to apply different evidentiary considerations to electronic evidence in civil and criminal proceedings. The ECT Act applies to both civil and criminal proceedings and does not distinguish between civil and criminal proceedings. Further, the case law from inception of the ECT Act to date suggests that no differing evidentiary considerations are applicable to electronic evidence in civil and criminal proceedings.

8.2.6 South African Law Reform Commission recommendations[10]

The SALRC suggest three options for law reform in the context of electronic evidence. Rather than opting to pursue the most aggressive option, law reform in the guise of the Law of Evidence Bill attached as Annexure A, South Africa ought to adopt a more cautious and pragmatic approach. Namely, an amendment to existing legislation rather than a drastic overhaul. A summary of recommendations follows immediately below in para 8.3.

[7] Section 31.3 of the Canada Evidence Act, 1985.
[8] Chapter 5 above.
[9] Chapter 6 above.
[10] Chapter 7 above.

8.3 SUMMARY OF RECOMMENDATIONS IN THE CONTEXT OF THE SOUTH AFRICAN LAW REFORM COMMISSION'S *REVIEW OF THE LAW OF EVIDENCE*

The moderate success of the ECT Act notwithstanding – particularly in comparison to the dismal Computer Evidence Act – the current regulatory environment does require amendment given its age, and by way of summary, at least the following is required:

A. *Regular review of the ECT Act* by a multi-disciplinary panel (as suggested by the SALRC),[11] reporting to the Minister of Justice and Constitutional Development at least every two or three years. The panel should consider:

A1 the *Law of Evidence Bill* and the codification approach suggested by the SALRC.

A2 A1 notwithstanding, an extension of the ECT Act and the ECT Act's adequacy in general.

A3 whether to abolish the distinction between advanced electronic signatures and electronic signatures, and biometric technologies.

A4 whether the legislature should distinguish between automated computer evidence and computer output subject to hearsay – or to leave this to the judiciary.

A5 whether the legislature should provide further direction on authentication (such as in secondary law in the form of regulations to the ECT Act), or whether this should be left to the judiciary.

B. *Definition of data message*

B1. Amendment and alignment of the definition of data message in the current version of the Cybercrimes Bill,[12] and the ECT Act.

B2. Inclusion of the term data message in applicable legislation, such as the Criminal Procedure Act, Civil Proceedings Evidence Act, Law of Evidence

[11] South African Law Reform Commission Discussion Paper 131 (Project 126) *Review of the Law of Evidence* (2014) para 5.10 at 84.
[12] Bill B6B – 2017.

Amendment Act, and legislation relevant to rules of South Africa's various courts.

C. *Amendment and alignment of hearsay exceptions*

C1. Consider whether s 15(4) of the ECT Act should apply to criminal proceedings.

C2. Aligning the hearsay exceptions in the Criminal Procedure Act, Civil Proceedings Evidence Act and ECT Act.

D. *Definition of document in* Civil Proceedings Evidence Act *and Criminal Procedure Act*

D1. Consistency in definitions with the term *document*.

E. *Electronic discovery*

E1. Amendment of various legislation to provide for change to court rules to deal with electronic discovery and disclosure of metadata.

8.4 CONCLUDING REMARKS

There can be no doubt that technology and the internet have changed the way society communicates and interacts. The law has had to adapt. In order to foster certainty and clarity, the SALRC has been reviewing electronic evidence since its inception in 1982 when it first mooted the possibility of a codified law of evidence in the form of a statute.

While electronic evidence is certainly susceptible[13] to manipulation and evolving technology, its use is now commonplace, and a plethora of expertise is readily available to detect and comment on manipulation where that may be at issue. The law must adapt.[14] South Africa cannot sustain a legal position where the exclusion of evidence is justified because it is new or uncertain. The traditional principles of evidence need not be re-written, but in certain instances, some adaptation or amendment is required.

In its latest findings, pending before the responsible Minister, the SALRC again suggested the codification route, in the form of a *Law of Evidence Bill*. The promulgation of

[13] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7 – 13 where apparent difficulties with electronic evidence are discussed in detail.

[14] *CMC Woodworking Machinery (Pty) Ltd v Pieter Odendaal Kitchens* 2012 (5) SA 604 (KZD) para 2 where it was stated: 'it is …not unreasonable to expect the law to recognise such [technological] changes and accommodate [them]'.

this Bill will lead to uncertainty, and will arguably be harmful for South African law. To ensure a clear and accessible legal framework, amendment should be made to existing legislation, and a further expert working-group should further consider the *Law of Evidence Bill* in light of more recent case law, and international trends.

Finally, in terms of our current interpretation regarding the admissibility and weight of electronic evidence, when the occasion arises in the Supreme Court of Appeal, South Africa's judiciary should reject the notion that all electronic evidence is hearsay – this proposition is flawed, and destroys functional equivalence. Moreover, our courts should clearly distinguish between automatically produced electronic evidence (which is not subject to the hearsay rules – real evidence), and documentary electronic evidence (which is subject to the hearsay rules). Equally, to the extent that any doubt still exists, our courts should confirm that electronic evidence is not automatically admissible, and that in order to be admissible, the evidence must be authentic (whether classified as real or documentary evidence).

9. BIBLIOGRAPHY

9.1 *Primary Sources*

Constitution

Constitution of the Republic of South Africa, 1996.

Statutes – South Africa

Alienation of Land Act 68 of 1981

Bills of Exchange Act 34 of 1964

Child Justice Act 75 of 2008

Civil Proceedings Evidence Act 25 of 1965

Close Corporation Act 69 of 1984

Computer Evidence Act 57 of 1983

Criminal Procedure Act 51 of 1977

Cybercrimes and Cybersecurity Bill B – 2015

Cybercrimes and Cybersecurity Bill B6 – 2017

Cybercrimes Bill B6B – 2017

Electronic Communications and Transactions Act 25 of 2002

Films and Publications Act 65 of 1996

Judicial Matters Amendment Act 55 of 2002

Law of Evidence Amendment Act 45 of 1988

Legal Aid South Africa Act 39 of 2014

Magistrates Court Act 32 of 1944

Prevention of Organised Crime Act 121 of 1998

Protection from Harassment Act 17 of 2011

Protection of Personal Information Act 4 of 2013

Revenue Laws Amendment Act 60 of 2008

Rules Board for Courts of Law Act 107 of 1985

Sexual Offences Act 23 of 1957

South African Law Commission Act 19 of 1973

Stamp Duties Act 77 of 1968

Supreme Court Act 59 of 1959

Wills Act 7 of 1953

Statutes – international

Police and Criminal Evidence Act, 1984

Canada Evidence Act, 1985

Criminal Justice Act, 2003

Civil Evidence Act, 1995

Federal Rules of Evidence, United States

Cases – South Africa

AA Onderling Assuransie Bpk v De Beer 1982 (2) SA 603 (A)

ABSA Bank Ltd v Expectra 423 (Pty) Ltd 2017 (1) SA 81 (WCC)

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

ABSA Bank Limited v Smith [2016] ZAWCHC 147

ABSA Bank Limited v Future Indefinite lnvestments 201 (Pty) Ltd [2016] ZAWCHC 118

Arthur v Bezuidenhout and Mieny 1962 (2) SA 566 (A)

Botha v S [2009] ZASCA 125

Brooks v National Director of Public Prosecutions 2017 (1) SACR 701 (SCA)

Cecilia Goliath v Member of the Executive Council for Health, Eastern Cape 2015 (2) SA 97 (SCA)

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)

Dutch Reformed Church v Sooknunan 2012 (6) SA 201 (GSJ)

Ex parte Rosch [1998] 1 All SA 319 (W)

Firstrand Bank Limited v Venter [2012] JOL 29436 (SCA)

Gaxa and Kaiser Chiefs Football Club (2017) 38 ILJ 1221 (ARB)

General Council of the Bar of South Africa v Jiba 2017 (2) SA 122 (GP)

Golden Fried Chicken (Proprietary) Limited v Yum Restaurants International (Proprietary) Limited [2005] ZAGPHC 311

Gumede v S 2017 (1) SACR 253 (SCA)

Harvey v Niland 2016 (2) SA 436 (ECG)

Heroldt v Wills 2013 (2) SA 530 (GSJ)

Isparta v Richter 2013 (6) SA 529 (GNP)

Jafta v Ezemvelo KZN Wildlife (2009) 30 ILJ 131 (LC)

Jaftha v Schoeman and Van Rooyen v Stoltz 2005 (2) SA 140 (CC)

Jantjies v S [2014] ZASCA 153

Ketler Investments CC t/a Ketler Presentations v Internet Service Providers Association 2014 (2) SA 569 (GSJ)

Khumalo v Holomisa 2002 5 SA 401 (CC)

Key v Attorney-General, Cape Provincial Division 1996 (4) SA 187 (CC)

LA Consortium & Vending CC v MTN Service Provider (Pty) Ltd 2011 (4) SA 577 (GSJ)
Liberty Group Limited v K & D Telemarketing CC 2015 JDR 1846 (GP)

MTN Service Provider (Pty) Ltd v LA Consortium & Vending CC t/a LA Enterprises 2011 (4) SA 562 (WLD)

Maharaj v Barclays National Bank Ltd 1976 (1) SA 418 (A)

Malebo v S [2015] ZAFSHC 61

Makate v Vodacom (Pty) Ltd 2014 (1) SA 191 (GSJ)

Maseti v S [2014] 1 All SA 420 (SCA)

Motsepe v S 2015 (5) SA 126 (GP)

Mnyandu v Padayachi 2017 (1) SA 151 (KZP)

Motata v Nair NO 2009 (1) SACR 263 (T)

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

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

Nedbank v Fraser 2011 (4) SA 363 GSJ

Pillay v Krishna 1946 AD 946

Prinsloo v van der Linde 1997 (3) SA 1012 (CC)

RM v RB 2015 (1) SA 270 (KZP) 1976 (2) SA 573 (A)

Rees v Investec Bank Limited 2014 (4) SA 220 (SCA)

R v Blom 1939 AD 188

R v Fourie 1937 AD 31

R v Matthews 1960 (1) SA 572 (A)

R v Trupedo 1920 AD 58

S v Baleka (1) 1986 (4) SA 192 (T)

S v Baleka (3) 1986 (4) SA 1005 (T)

S v BM 2014 (2) SACR 23 (SCA)

S v Brown 2016 (1) SACR 206 (WCC)

S v De Villiers 1993 (1) SACR 574 (Nm)

S v Fuhri 1994 (2) SACR 829 (A)

S v Gumede 2017 (1) SACR 253 (SCA)

S v Harper 1981 (1) SA 88 (D)

S v Helm 2015 (1) SACR 550 (WCC)

S v Hoho 2009 (1) SACR 276 (SCA)

S v Koralev 2006 (2) SACR 298 (N)

S v Manamela 2000 (1) SACR 414 (CC)

S v Meaker 1998 (2) SACR 73 (W)

S v Mthimkulu 1975 (4) SA 759 (A)

S v M 2002 (2) SACR 411 (SCA)

S v Mashiyi 2002 (2) SACR 387 (Tk) 393

S v Meyer 2017 JDR 1728 (GJ)

S v Miller 2016 (1) SACR 251 (WCC)

S v Mpumlo 1986 4 All SA 197 (E)

S v Ndiki 2008 (2) SACR 252 (Ck) – also reported as *S v Ndiki* [2007] 2 All SA 185 (Ck)

S v Nieuwoudt 1990 (4) SA 217 (A)

S v Panayiotou [2018] 1 All SA 224 (ECP)

S v Steyn 1963 (1) SA 797 (W)

S v Ramgobin 1986 (4) SA 117 (N)

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

S v Zuma 1995 (2) SA 642 (CC)

S v Zuma 2006 (2) SACR 191 (W)

Savoi v National Director of Public Prosecutions 2014 (5) SA 317 (CC)

Scagell v Attorney-General, Western Cape 1997 (2) SA 368

Shackleton Credit Management (Pty) Ltd v Microzone Trading 88 CC 2010 (5) SA 112 (KZP)

Shaik v S [2007] 2 All SA 9 (SCA)

Sihlali v South African Broadcasting Corporation Ltd

South African Human Rights Commission v Qwelane 2018 (2) SA 149 (GJ)

South Cape Corporation (Pty) Ltd v Engineering Management Services (Pty) Ltd 1977 (3) SA 534 (A)

Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash 2015 (2) SA 118 (SCA)

Stamford Sales & Distribution (Pty) Limited v Metraclark (Pty) Limited [2014] ZASCA 79

Standard Bank of South Africa v Han-Rit Boerdery CC [2011] ZAGPPHC 120

STT Sales (Pty) Ltd v Fourie 2010 BIP 298 (GSJ)

Strydom v Engen Petroleum Ltd 2013 (2) SA 187 (SCA)

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

Tregea v Godart 1939 AD 16

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

Trustees for the time being of the Delsheray Trust v ABSA Bank Limited [2014] 4 All SA 748 (WCC)

Uramin Incorporated v Perie 2017 (1) SA 236 (GJ)

Van Breda v Media 24 Limited 2017 (5) SA 533 (SCA)

Cases – international

Burns v R [2017] EWCA Crim 1466.

Castle v Cross [1985] 1 All ER 87

Dell Computer Corporation v Union des consommateurs [2007] 2 S.C.R. 801

Edwards v The Queen (1993) 178 CLR 193

Jonathan Dixon v R [2015] NZSC 147

Khan v R [2015] EWCA Crim 1816

Lorraine v Markel American Insurance Company 241 F.R.D. 534

McDonald v R 2011] EWCA Crim 2933

Nobel Resources SA v Gross 2009] EWHC 1435 (Comm)

O'Shea v City of Coventry Magistrates' Court [2004] EWHC 905

Perfect 10 Inc v Cybernet Ventures Inc 213 F. Supp. 2d 1146 (C.D. Cal. 2002)

R v Coventry Justices [2004] All ER (D) 78

R v D CA287/2010 [2011] NZCA 69

R v Hall 1998] B.C.J. No. 2515

R v Hayes (2006) 23 CRNZ 547 (CA)

R v McCulloch

R v Minors and Harper (1989) 89 Cr App R 102

R v Mondor 2014 ONCJ 135

R v Oland 2018 NBQB 259

R v Sheppard and Whittle [2010] EWCA Crim 65

R v Spiby [1990] 91 Cr App R 186

Saturley v CIBC World Markets Inc. 2012 NSSC 226

Shepherd v The Queen (1990) 170 CLR 573

Tienda v State 358 SW3d 633 Texas Criminal Appeal (2012)

Telewizja Polska USA Inc. v Echostar Satellite Corp 2004 WL 2367740

The Statue of Liberty: Owners of the *Motorship Sapporo Maro v Owner of Steam Tanker, Statue of Liberty* [1968] 2 All ER 195 (PDA)

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

United States v Rollins 2004 WL 26780

United States v Lizarraga-Tirado 2015 WL 3772772

United States v Lamons 532 F.3d 1251, 1263

United States v Moon, 512 F.3d 359, 362

United States v Washington, 498 F.3d 225, 230

United States v Hamilton, 413 F.3d 1138, 1142

United States v Khorozian, 333 F.3d 498, 506

Van Dusen v Alcurt Landings LLC 2011 WL 530834

9.2 *Secondary Sources*

Books

Bainbridge D *Introduction to Information Technology Law* 6 ed (2008) Longman Publishing Company, London.

Bellengère A, Palmer R, Theophilopoulos C, Whitcher B, Roberts L, Melville N, Picarra E, Illsley T, Nkutha M, Naude B, Van der Merwe A & Reddy S *The Law of Evidence in South Africa* (2013) Oxford University Press Southern Africa, Cape Town

Casey E *Digital Evidence and Computer Crime* 3 ed (2011) Elsevier Academic Press, London

Davey R & Dahms-Jansen L *Social Media in the Workplace* (2017) LexisNexis, Johannesburg

Friedman L & Hayden G *American Law: An Introduction* (2017) Oxford University Press, New York

Harvey D *Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age* (2017) Hart Publishing, Oxford.

Holt T, Bossler AM & Siegfried-Spellar KC *Cybercrime and Digital Forensics* (2015) Routledge, London and New York

Kruger A *Hiemstra's Criminal Procedure* (2018) Butterworth Publishers (Pty) Ltd, South Africa

Lulat Y *United States Relations with South Africa: A Critical Overview from the Colonial Period to the Present* 2 ed (2008) Peter Lang Inc.: International Academic Publishers, New York

Malek H (ed) *Phipson on Evidence* 17 ed (2009) Sweet & Maxwell, London

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

Papadopoulos S & Snail S (eds) *Cyberlaw@SA III: the law of the Internet in South Africa* (2012) 3 ed Van Schaik, Pretoria

Schwikkard P & S van der Merwe *Principles of Evidence* 3 ed (2009) Juta, Cape Town

Schwikkard P & S van der Merwe *Principles of Evidence* 4 ed (2016) Juta, Cape Town

Susskind R *The End of Lawyers? Rethinking the Nature of Legal Services* (2010), Oxford University Press, New York

Susskind R *Tomorrow's Lawyers An Introduction to the Future* 2 ed (2017) Oxford University Press, New York

Tapper C *Cross & Tapper on Evidence* 12 ed (2010) Oxford University Press, Oxford

Underwood G & Penner J *Electronic Evidence in Canada* (2010) Carswell, Toronto

Van der Merwe D, Roos A, Pistorius T, Eiselen G & Nel S *Information and Communications Technology* 2 ed (2016) LexisNexis, Durban

Wigmore J *A treatise on the system of evidence in trials at common law* 3 ed (1940) Little, Brown and Company, Boston

Zeffertt D & Paizes A *Essential Evidence* (2010) LexisNexis, Durban

Zeffertt D, Paizes A & Skeen A *The South African Law of Evidence* (2003) LexisNexis Butterworths, Durban.

Zeffertt D & Paizes A *The South African Law of Evidence* 2 ed (2009) Lexisnexis, Durban

Zeffertt D & Paizes A *The South African Law of Evidence* 3 ed (2017) Lexisnexis, Durban

Chapters in Books

Bilchitz D 'Law of Evidence' in Lewis C *et al* (eds) *Annual Survey of South African Law* (1998) Juta, Johannesburg

Currie R & Coughlan S 'Canada' in Mason S (ed) *Electronic Evidence* 2 ed (2010) LexisNexis Butterworths, London

Gallavin C & Mason S 'Hearsay' in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Gallavin C & Mason S 'Hearsay' in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Hofman J & de Jager J 'South Africa' in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Mason S 'Mechanical Instruments: the presumption of being in order' in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Mason S 'The Presumption that Computers are reliable' in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Mason S 'Software code as the witness' in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Mason S, Freedman C & Patel S 'England & Wales' in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Mason S & Stanfield A 'Authenticating electronic evidence' in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Mason S & Seng D 'Real Evidence' in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Mason S & Seng D ‘Real Evidence’ in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Mason S & Seng D ‘Foundations of evidence in electronic form’ in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Schafer B & Mason S ‘The characteristics of electronic evidence’ in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Schwerha J, Bagby J & Esler B ‘United States of America’ in Mason S (ed) *Electronic Evidence* 3 ed (2012) University of London, London

Swales L ‘Electronic and Cyber Evidence’ in A Bellengère et al (eds) *The Law of Evidence in South Africa* 2 ed (2019) Oxford University Press, Cape Town

Van der Merwe C ‘Servitudes’ in *Law of South Africa* (2010) Juta, Johannesburg

Van der Merwe D ‘Evidence’ in *Law of South Africa* (2015) Juta, Johannesburg

Weir G & Mason S ‘The sources of digital evidence’ in Mason S (ed) *Electronic Evidence* 3 ed (2012) LexisNexis Butterworths, London

Weir G & Mason S ‘The sources of electronic evidence’ in Mason S & Seng D (eds) *Electronic Evidence* 4 ed (2017) University of London, London

Journal Articles

Cassim F ‘The use of electronic discovery and cloud computing technology by lawyers in practice: lessons from abroad’ (2017) 42 *Journal for Juridical Science* 19 – 40

Collier D ‘Evidently not so Simple: Producing Computer Print-outs in Court’ 2005 *Juta Business Law* 1 – 9

De Villiers D ‘Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 1)’ (2010) 3 *TSAR* 558 – 575

De Villiers D ‘Old 'Documents', 'Videotapes' and New 'Data Messages' – A Functional Approach to the Law of Evidence (part 2)’ (2010) 4 *TSAR* 720 – 735

Duranti L, Rogers C & Sheppard A ‘Electronic Records and the Law of Evidence in Canada: The Uniform Electronic Evidence Act Twelve Years Later’ (2010) 70 *Archivaria* 95 – 124

Eiselen S ‘Fiddling with the ECT Act – Electronic Signatures’ (2014) 17 *PELJ* 2805 – 2820

Erlank W & Ramokanate L ‘Allocating the risk of software failures in automated message systems (autonomous electronic agents)’ 2016 *SAMLJ* 201 – 202

Esler B ‘Lorraine v Markel: Unnecessarily Raising the Standard for Admissibility of Electronic Evidence’ 2007 *Digital Evidence and Electronic Signature Law Review* 80 – 82

Faria J ‘E-commerce and International Legal Harmonization: Time to Go Beyond Functional Equivalence?’ (2004) 16 *SAMLJ* 531 – 533

Frieden J & Murray L ‘The Admissibility of Electronic Evidence under the Federal Rules of Evidence’ (2011) 17 *Richmond Journal for Law and Technology* 2 – 6

Gregory J ‘Canadian Electronic Commerce Legislation’ (2002) 17 *Banking & Finance Law Review* 276 – 277

Gregory J ‘The UETA and the UECA – Canadian Reflections’ (2001) *Idaho Law Review* 441 – 476

The Harvard Law Review Association ‘Scientific Gadgets in the Law of Evidence’ (1939) 53 *Harvard Law Review* 285 – 296

Hofman J ‘Electronic evidence in criminal cases’ (2006) 3 *SACJ* 257 – 275

Jacobs W ‘The Electronic Communications and Transactions Act: Consumer Protection and Contracts’ (2004) 16 *SAMLJ* 556 – 557

Kemp L ‘Lorraine v. Markel: An Authoritative Opinion Sets the Bar for Admissibility of Electronic Evidence (Except for Computer Animations and Simulations)’ (2007) 9 *North Carolina Journal of Law & Technology* 20 – 21

Leroux O ‘Legal Admissibility of Electronic Evidence’ (2004) 18 *International Review of Law, Computers & Technology* 201 – 202.

Mupangavanhu Y ‘Electronic signatures and nonvariation clauses in the modern digital world: The case of South Africa’ (2016) 133 *SALJ* 853 – 873

Paciocco D ‘Proof and Progress: Coping with the Law of Evidence in a Technological Age’ (2013) 11 *CJTL* 181 – 228

Paizes A ‘The law of evidence: Seven wishes for the next twenty years’ (2014) 3 *SACJ* 272 – 292

Pistorius T ‘ “Nobody Knows you're a Dog”: The Attribution of Data Messages’ (2002) 14 *SA Merc LJ* 737–738

Reed C ‘The Admissibility and Authentication of Computer Evidence – A Confusion of issues’ *5th Annual British and Irish Legal Education Technology Association Conference* (1990)

Roth A ‘Trial by Machine’ (2016) 104 *Georgetown Law Journal* 1253

Roth A ‘Machine Testimony’ (2017) 126 *Yale Law Journal* 1972 – 2259

Seng D ‘Computer output as evidence’ (1997) *Singapore Journal of Legal Studies* 161 – 163

Surden H ‘Machine Learning and Law’ (2014) 89 *Washington Law Review* 89 – 95

Swales L 'The regulation of electronic signatures: Time for review and amendment' (2015) 132 *SALJ* 257 – 270

Swales L 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part One' (2018) 21 *PELJ* 2 – 24

Swales L 'An Analysis of the Regulatory Environment Governing Hearsay Electronic Evidence in South Africa: Suggestions for Reform – Part Two' (2018) 21 *PELJ* 1 – 25

Swales L 'Electronic instruments – a presumption of reliability, a presumption of regularity, judicial notice, or none of the above?' *SACJ* 2018 (2) 189 – 211s

Teppler S 'Testable Reliability: A Modernized Approach to ESI Admissibility' (2014) 12 *Ave Maria Law Rev* 213

Theophilopoulos C 'The admissibility of data, data messages, and electronic documents at trial' (2015) 3 *TSAR* 461 – 481

Watney M 'Admissibility of Electronic Evidence in Criminal Proceedings: An Outline of the South African Legal Position' (2009) 1 *Journal of Information, Law and Technology* 1 – 13

Whitear-Nel N 'Admissibility of hearsay evidence' (2007) 20 *SACJ* 116 – 117

Theses

Kulehile M *An analysis of the regulatory principles of functional equivalence and technology neutrality in the context of electronic signatures in the formation of electronic transactions in Lesotho and the SADC region* (PhD thesis, University of Cape Town, 2017)

Duvenhage A *An evidential analysis of section 15 (4) of the Electronic Communications and Transactions Act 25 of 2002* (LLM thesis, University of Pretoria, 2016)

Fourie F *Using Social Media as Evidence in South African Courts* (LLM thesis, North-West University, 2016)

Mapoma S *A critical study of the authentication requirements of Section 2 of the Computer Evidence Act No 57 of 1983* (LLM thesis, University of South Africa, 1997)

Stanfield A *The Authentication of Electronic Evidence* (PhD thesis, Queensland University of Technology, 2016) 95 – 120

Van Tonder G *The admissibility and evidential weight of electronic evidence in South African legal proceedings: a comparative perspective* (LLM thesis, University of the Western Cape, 2013)

Periodicals

Hughes B 'The rise of electronic discovery' *De Rebus* January/February 2012 at 24 – 26

Mason S ‘Electronic Evidence, The Presumption of Reliability and Hearsay – a Proposal’ *Criminal Law & Justice Weekly* 28 September 2013

Takombe M ‘The rise of the machines – understanding electronic evidence’ *De Rebus* August 2014 153 – 155

9.3 *Internet Sources*

Beazley M ‘Social Media and the Courts: Service of Process’ Fourth Judicial Seminar on Commercial Litigation available at *http://www.supremecourt.justice.nsw.gov.au/Documents/Publications/Speeches/Pre-2015%20Speeches/Beazley/beazley_160513.pdf,* accessed 17 April 2016

Commonwealth Secretariat ‘Model Law on Electronic Evidence’ available at *http://thecommonwealth.org/sites/default/files/key_reform_pdfs/P15370_7_ROL_Model_Bill_Electronic_Evidence_0.pdf*, accessed on 30 April 2018

Department of Justice and Constitutional Development ‘Memorandum on the objects of the Cybercrimes and Cybersecurity Bill 2017’ available at *http://www.justice.gov.za/legislation/bills/CyberCrimesDiscussionDocument2017.pdf*, accessed on 12 April 2018

Groulx, Rothman & Zawidzki ‘Admissibility: Understanding types and sources of electronic evidence’ available at https://www.dentons.com/~/media/FMC%20Import/publications/pdf/a/Admissibility%20Understanding%20Types%20and%20Sources%20of%20Electronic%20Evidence.ashx, accessed 25 June 2017

Joseph G ‘A Simplified Approach to Computer-Generated Evidence and Animations’ available at *http://www.jha.com/us/articles/viewarticle.php?8*, accessed 5 June 2017

Milo D ‘The Timely demise of criminal defamation law’ available at *http://www.polity.org.za/article/the-timely-demise-of-criminal-defamation-law-2015-10-05*, accessed on 24 April 2018

Mybroadband ‘South Africa’s first computers’ available at *https://mybroadband.co.za/news/hardware/132408-south-africas-first-computers.html*, accessed 25 July 2018

Internet World Stats ‘Usage and Population Statistics’ available at *http://www.internetworldstats.com/africa.htm#za*, accessed on 17 April 2016 and 31 July 2018

Ireland Law Reform Commission Consultation Paper *Documentary and Electronic Evidence* LRC CP 57 – 2009 available at *http://www.lawreform.ie/_fileupload/consultation%20papers/cpDocumentaryandElectronicEvidence.pdf*, accessed on 25 August 2017

Law Commission for England and Wales 'Electronic Commerce: Formal Requirements in Commercial Transactions' available at *http://www.lawcom.gov.uk/wp-content/uploads/2015/09/electronic_commerce_advice.pdf*, accessed on 25 July 2017

Law Society of South Africa 'Comments to the South African Law Reform Commission in relation to issues raised in Discussion Paper 131: *Review of the Law of Evidence*', available at *http://lssa.org.za/upload/LSSA%20comments%20on%20SALRC%20Discussion%20Paper%20131%20LAw%20of%20Evidence%2029%20July%202015.pdf*, accessed on 8 May 2017

Parliament of the Republic of South Africa 'Several Bills get the nod from parliament this afternoon' available at *https://www.parliament.gov.za/press-releases/several-bills-get-nod-parliament-afternoon*, accessed on 29 November 2018

Seng D & Chakravarthi S 'Computer Output as Evidence' available at*https://www.sal.org.sg/Portals/0/PDF%20Files/Law%20Reform/TLDG-2003-09%20-%20Computer%20Output%20as%20Evidence.pdf*, accessed on 25 June 2017

Smith M 'Facilitating Electronic Commerce Through the Development of Laws to Recognize Electronic Documents and Transactions' available at *http://publications.gc.ca/Collection-R/LoPBdP/BP/prb0012-e.htm,* accessed on 10 May 2019

South African Law Reform Commission 'Fortieth Annual Report of the South African Law Commission' available at *http://salawreform.justice.gov.za/anr/2012-2013-anr-salrc.pdf*, accessed on 5 April 2017

South African Law Reform Commission 'Issue Papers' available at *http://www.justice.gov.za/salrc/ipapers.htm*, accessed 5 May 2018

South African Law Reform Commission 'Objects, Constitution and Functioning' available at *http://www.justice.gov.za/salrc/objects.htm#sthash.OIkeTaHM.dpbs*, accessed on 3 June 2018

United Nations 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment' available at *http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf*, accessed on 5 April 2016

9.4 *Reports, Discussion Papers, Issue Papers & Guidelines*

South African Law Commission (Project 6) *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers* (1982)

South African Law Commission Report (Project 6) *Review of the Law Evidence* (1986)

South African Law Commission Working Paper 60 (Project 95) *Investigation into the Computer Evidence Act 57 of 1983* (1995)

South African Law Commission Issue Paper 14 (Project 108) *Computer-related crime* (1998)

South African Law Commission Discussion Paper 99 (Project 108) *Computer-related Crime* (2001)

South African Law Commission (Project 126) *Report on the Preliminary Investigation into the Review of the Rules of Evidence* (2002)

South African Law Reform Commission (Project 113) *The Use Of Electronic Equipment In Court Proceedings Postponement Of Criminal Cases Via Audiovisual Link* (2003)

South African Law Reform Commission Discussion Paper 113 (Project 126) *Review of the Law of Evidence Hearsay and Relevance* (2008)

South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010)

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

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

10. ANNEXURE A

DRAFT LAW OF EVIDENCE BILL
REPUBLIC OF SOUTH AFRICA

_____

LAW OF EVIDENCE BILL

_____

(As introduced)

_____

(MINISTER FOR JUSTICE AND CONSTITUTIONAL DEVELOPMENT)

[B B2014]

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

_____ Words underlined with a solid line indicate insertions in existing enactments.

BILL

To regulate the admissibility of evidence so as to provide for the admissibility of hearsay evidence, and for the admissibility and proof of business records and evidence produced by processes, machines and other devices in all legal proceedings; and to provide for matters connected therewith.

_____

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:

Preamble[15]

1. Definitions

"Business" includes any activity regularly carried on, whether for profit or not, by any organ of state or any organisation or person;

"Business records" includes those records created or received in the ordinary course of business by any organ of state or any trade, profession or other organisation or person;

"Computer system" means a device or a group of interconnected or related devices, which perform functions pursuant to computer programs;

---

204 The Act is intended to clarify, consolidate and align the rules for the admissibility of business records and evidence produced by processes, machines and other devices, while leaving intact existing legislation on (for example) the admissibility of official and public documents

"Copy" in relation to a document means anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly, and regardless of how many removes from the original;
"Document" means anything in which information of any description is recorded, and includes a copy;
"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;
"Electronic documents system" includes a computer system or other similar device by or in which data are recorded or stored, and any procedures related to such recording or storage or electronic document;
"Electronic signature" means electronic representations of information attached to, incorporated in, or logically associated with other information and which are intended by the user to serve as a signature;
"Hearsay evidence" means evidence, whether oral or in writing, the probative value of which depends upon the credibility of a person other than the person giving such evidence;
"Records" means anything in which information of any description is recorded;
"Officer" includes any person occupying a responsible position in relation to the relevant activities of a business or public authority, or in relation to its records;
"Public authority" includes any public or statutory undertaking, or any government department;
"Statement" means any representation of fact or opinion, however made;
"writing" means information contained in a document.

2. Application

2.1 This Act applies to all criminal and civil proceedings or the legal proceedings before any tribunal in which the strict rules of evidence apply, whether as a matter of law or by agreement of the parties.
2.2 The provisions of this Act do not affect any rule of law relating to the admissibility of evidence, except the rules relating to hearsay, authentication and best evidence in relation to certain types of documentary evidence.

3. Admissibility of hearsay evidence

3.1 Subject to the provisions of this Act or any other law, hearsay evidence, whether oral or in writing, shall not be admissible 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; or

(b) the person upon whose credibility the probative value of such evidence depends, 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 probative value of the evidence;

(v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;

(vi) any prejudice to a party which the admission of such evidence mightentail; and

(vii) 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 interests of justice.

3.2 Hearsay evidence admitted in terms of subsection 3.1(b) may be left out of account if the person upon whose credibility the probative value depends subsequently does not testify at the proceedings, unless the hearsay evidence is admitted in terms of paragraph (a) or (c) of subsection 3.1.

3.3 No hearsay evidence shall be admitted in evidence under this section unless the party intending to produce the hearsay evidence has given notice in terms of section 6.

4. Admissibility of business records in legal proceedings

4.1 In any proceedings in which direct evidence of a fact would be admissible, any statement made in the ordinary course of business, whether by a person or wholly or partially by a machine, device or technical process; and contained in a document and tending to establish that fact, shall, upon production of the document, be admissible as evidence of that fact.

4.2 In the absence of a witness or witnesses to produce and give testimony regarding the admissibility of the document produced in terms of this section –

(i) such document must be accompanied by a certificate to the effect that the document forms part of the records of a business or public authority, signed by an officer of the business or public authority to which the records belong.

For this purpose –

(a) a document purporting to be a certificate signed by an officer of a business or public authority shall be deemed to have been duly given by such an officer and signed by him or her; and

(b) a certificate shall be treated as signed by a person if it purports to bear an electronic signature or a facsimile of his or her signature.

(ii) the party intending to produce the document as evidence must give notice in terms of section 6.

4.3 Nothing in this section shall render admissible as evidence in any legal proceedings a record made in the course of obtaining or giving legal advice or in contemplation of a legal proceeding.

4.4 The court may, having regard to the circumstances of the case, require additional evidence, whether oral or in writing, including an affidavit in respect of a document produced in terms of this section; or may direct that all or any of the provisions of this section do not apply in relation to a particular document or record made in the ordinary course of business.

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.

6. Notice of intention to produce hearsay evidence and documentary evidence

6.1 Notice of an intention to produce evidence in terms of subsections 3, 4 or 5 must be given –

(a) in writing to every other party to the proceeding, and must include the contents of the statement and (where applicable) the name of the maker of the statement; and if a document is to be produced, the document including any related metadata must be attached to the notice; and

(b) in sufficient time before the hearing to provide all other parties to the proceeding with a fair opportunity to prepare to meet the statement.

6.2 A party to the proceeding who is given notice in terms of subsection (1) must, if that party objects to the admission of the statement as evidence, give notice of objection as soon as practicable to the party proposing to offer the statement.

6.3 Subsections (1) and (2) may be excluded by agreement of the parties, or by waiver of the party to whom notice is required to be given; or the presiding officer may dispense with the requirement to give notice under subsections (1) or (2) –

(a) if having regard to the nature and contents of the hearsay statement, no party is substantially prejudiced by the failure to give notice under subsection (1); or

(b) if giving notice was not reasonably practicable in the circumstances; or

(c) in the interests of justice.

6.4 In any civil proceedings, where the notice in terms of subsection (1) relates to documentary evidence and no party objects to the notice in terms of subsection (1), or if the court dismisses an objection on the ground that no useful purpose would be served by requiring the party concerned to call a witness to produce the documents, –

(a) the document, if otherwise admissible, may be admitted in evidence; and

(b) it will be presumed, in the absence of evidence to the contrary, that the nature, origin, and contents of the document are as shown on its face.

6.5 Provision may be made by the Rules of Court specifying the manner in which the duties imposed by this section are to be complied with, including the time allowed for such compliance.

6.6 A failure to comply with this section or any Rules of Court provided in terms of subsection (5) does not affect the admissibility of the evidence, but may be taken into account by the court –

(a) in considering the exercise of its powers over the proceedings and in respect of costs; and

(b) as a matter that might adversely affect the weight to be given to the evidence.

7. Authenticity and integrity of documentary evidence

7.1 Subject to the provisions of this Act, a person seeking to admit documentary evidence in terms of the Act has the burden of proving the authenticity and integrity of the document.

7.2 For the purposes of determining whether an electronic document is admissible in terms of this section, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored; having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document, and the nature and purpose of the electronic document.

7.3 The integrity of an electronic documents system may be established by evidence capable of supporting a finding that at all material times the computer system or other similar device used by the electronic documents system was operating properly; or, if it was not, the fact of its not operating properly did not affect the integrity of the electronic document and there are no other reasonable grounds for doubting the integrity of the electronic documents system.

7.4 Evidence in terms of subsections (2) and (3) may be produced orally or by affidavit.

7.5 A party may cross-examine a deponent of an affidavit introduced into evidence in terms of subsection (4) if the deponent is an adverse party or is under the control of an adverse party; or with leave of the court.

7.6 In any civil proceeding where a party is permitted under the Rules of Court relating to discovery to inspect a document –

(a) the requirement to prove the authenticity and integrity of the document may be dispensed with in circumstances described in those Rules; and

(b) the procedure to be adopted by a party seeking to require proof of the authenticity and integrity of the document is that set out in those Rules; and

(c) the production of secondary evidence to prove the authenticity and integrity of the document may be permitted in circumstances described in those Rules.

7.7 The signature, execution, or attestation of a document, whether electronic or otherwise, that is required by law to be attested may be proved by any satisfactory means, provided that an attesting witness need not be called to prove that the document was signed, executed or attested as it purports to have been signed, executed, or attested.

8 Weight to be attached to documentary evidence

In estimating the weight to be attached to documentary evidence admitted in terms of this Act, regard shall be had to all the circumstances from which any inference may reasonably be drawn as to the accuracy or otherwise of the information contained in the document, and in particular –

(d) where the information was directly provided by a person, regard shall be had to whether or not the person who supplied the information did so contemporaneously with the occurrence or existence of the facts stated; and to whether or not that person or any person concerned with making or keeping the record containing the statement had any incentive to conceal or misrepresent the facts.

(e) where the information is contained in an electronic document, regard shall be had to –

(i) the reliability of the manner in which the data message was generated, stored or communicated;
(ii) the reliability of the manner in which the integrity of the data message was maintained;
(iii) the manner in which its originator was identified; and
(iv) any other relevant factor.

9. Discretion to exclude or limit the use of documentary evidence

The court may refuse to admit documentary evidence or may limit the use to be made of such evidence; if a particular use of the evidence might be unfairly prejudicial to a party or might be misleading or confusing.

10. Provisional admission of evidence

If a question arises concerning the admissibility of any evidence, the Judge may admit the evidence in question, subject to further evidence being offered later on to establish its admissibility.

11. Repeal of sections of statutes

Repeals: section 3 of the Law of Evidence Amendment Act
Repeals: section 15(4) of the ECT Act [whole of section 15 and incorporate it in an Amendment Bill?]
Repeals: sections 27 – 38 of the Civil Proceedings Evidence Act
Repeals: sections 221, 222, and 236 of the Criminal Procedure Act