UNIVERSITY OF THE WESTERN CAPE

FACULTY OF LAW

THE ADMISSIBILITY AND EVIDENTIAL WEIGHT OF ELECTRONIC EVIDENCE IN SOUTH AFRICAN LEGAL PROCEEDINGS: A COMPARATIVE PERSPECTIVE

A mini-thesis submitted in partial fulfilment of the requirements for the LLM degree in the Faculty of Law of the University of the Western Cape.

By

Gert Petrus van Tonder

Student number: 2715660

Supervisor: Mr Pieter Koornhof

May 2013

KEY WORDS

Electronic Evidence

Data Messages

Admissibility

Exclusionary Rules

Evidential Weight

South Africa

England and Wales

Canada

Electronic Communications and Transactions Act 25 of 2002

LIST OF ACRONYMS

EU	European Union
LRCI	Law Reform Commission of Ireland
SALC	South African Law Commission
SALRC	South African Law Reform Commission
UNCITRAL	United Nations Commission on International Trade Law

DECLARATION

I, **Gert van Tonder**, declare that **The Admissibility and Evidential Weight of Electronic Evidence in South African Legal Proceedings: A Comparative Perspective** is my own work and that it has not been submitted before for any degree or examination in any other university, and that all sources I have used or quoted have been indicated and acknowledged as complete references.

Signed: _____

Gert van Tonder

May 2013

Signed: _____

Mr Pieter Koornhof

May 2013

ACKNOWLEDGEMENTS

I am grateful to Mr Pieter Koornhof for the advice and input provided in the writing of this thesis.

I would like to thank my parents, Mr André van Tonder and Mrs Elna van Tonder, for the love and support.

Additionally, I wish to express my gratitude to my colleagues and classmates, Razyaan Johaardien and Ghislaine Jacobs, and the others who have not been mentioned for the encouragement.

To my special friends, Myra Triegaardt and Handré van Heerden, who motivated me and served as an inspiration, thank you.

DEDICATION

This work is dedicated to my parents Mr and Mrs van Tonder, who continued to support my dream to pursue a career in law.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION

1.1 Introduction

Technology can be used as a medium to communicate, store and transmit information in civil practice and criminal activity.[1] The proliferation of electronic media has caused that more and more legal, commercial and criminal activities are carried out by electronic instruments and the need to regulate this source of evidence has gained momentum.[2]

Once the electronic information is admitted by a court, it becomes electronic evidence,[3] which can often assist to prove or disprove a fact or a point of law.[4] Electronic evidence is a valuable and abundant source of evidence in legal proceedings.[5] This type of evidence has become increasingly prevalent in, for example, commercial litigation, criminal fraud prosecutions and bankruptcy proceedings.

In view of the rapid technological developments, it is common that there is a gap between technology and the law.[6] This is generally the case due to the fact that legal systems do not develop at the same pace that technology does.[7] The law of evidence, like many other fields of law, find it difficult to adapt to a world in which paper is replaced by electronic documents.[8] The courts have struggled with the traditional rules of evidence and adapting those to newer technologies with inconsistent results, an example of this has been how perceptions of the concept of reliability has caused confusion between the principles of admissibility, authentication, hearsay, the best evidence rule and evidential weight.[9] The courts should also distinguish between the different forms of electronic evidence such as, computer-assisted and computer-generated, for different evidentiary rules will apply.

---

[1] South African Law Reform Commission Issue Paper 27 (Project 126) *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* (2010) 7.
[2] Law Reform Commission of Ireland Consultation Paper 57 (Project 7) *Documentary and Electronic Evidence* (2009) 71. In this consultation paper, the Law Commission of Ireland dealt extensively with the law in regard to electronic evidence in the United Kingdom, particularly the law of England and Wales. For comparative purposes, Ireland is not relevant to this research.
[3] 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* 2.
[4] Watney M (2009) 2.
[5] SALRC Issue Paper 27 (2010) 7.
[6] SALRC Issue Paper 27 (2010) 4.
[7] Watney M (2009) 1.
[8] Van der Merwe D et al *Information and Communications Technology Law* (2008) 104.
[9] LRCI Consultation Paper 57 (2009) 72.

Traditionally, documents referred to masses of paper stored in filling cabinets.[10] Notably, space is finite and storage costs money, resulting in documents having to be either destroyed or additional storage being purchased.[11] In order to curb this problem, it has resulted in the increase of electronic document generation and storage methods.[12] In comparison to a paper document, most of the 'guarantees of authenticity' disappear as far as an electronic document is concerned, which highlights a fundamental problem with electronic evidence.[13] There have been developments in the technology, which may help to establish the authenticity, and to maintain the integrity and accuracy of data. However the law has not yet settled on standards in respect of electronic evidence.[14]

As modern technological advances so do computers, networks and any other communication or storage devices, which also have a potential impact on information technology law.[15]

Electronic information can take the form of stored data, but a distinction must be made between digital and analogue data.[16] Digital data is created and stored on an electronic device or the internet.[17] For example, 'cache files on a personal computer, digital photographs or graphics files'.[18] Analogue data is created by an analogue device, which is fixed and permanent.[19] Analogue data is difficult to manipulate, however digital data is problematic since it can be potentially altered without any residual effect, something which should be safeguarded against.[20] Digital data also presents other problems such as hardware failure[21] or defective software.[22] All these concerns highlight a fundamental problem when information is stored digitally.

1.2 Background

[10] LRCI Consultation Paper 57 (2009) 144.
[11] LRCI Consultation Paper 57 (2009) 145.
[12] LRCI Consultation Paper 57 (2009) 145.
[13] Van der Merwe D et al (2008) 104.
[14] Van der Merwe D et al (2008) 104.
[15] SALRC Issue Paper 27 (2010) 7.
[16] Schwikkard PJ & van der Merwe SE *Principles of Evidence* 3 ed (2009) 410.
[17] Schwikkard PJ & van der Merwe SE (2009) 410.
[18] SALRC Issue Paper 27 (2010) 8.
[19] Schwikkard PJ & van der Merwe SE (2009) 410.
[20] Schwikkard PJ & van der Merwe SE (2009) 410-411.
[21] Van der Merwe D *Computers and the law* 2 ed (2000) 226.
[22] Marshall A *Liability of Defective Software in South Africa* (LLM minor dissertation, University of Cape Town, 2005).

Before the Electronic Communications Act 25 of 2002 (hereafter referred to as the 'ECT Act'), computer related evidence was regulated in terms of the Civil Proceedings Evidence Act 25 of 1965 ('CPEA'), the Criminal Procedure Act 51 of 1977 ('CPA') and the Computer Evidence Act 57 of 1983 ('CEA').

Reference will be made to the relevant provisions of the CPEA, CPA, CEA and the ECT Act, which relate to the admissibility of electronic evidence, and case law applicable to those provisions.

Civil Proceedings Evidence Act 25 of 1965

A difficult position regarding documentary evidence was highlighted in the *Vulcan Rubber Works (Pty) Ltd v South African Railways and Harbours*[23] case, where the evidence was given by an official in charge of harbour claims to the effect that they made certain investigations to trace the appellant's bales of rubber.[24] The court excluded the evidence because the official's statements about the reports that he received from other officials were of a hearsay nature.[25]

Thereafter, the CPEA was enacted which was based on the old English Evidence Act of 1938, and was framed long before the Computer Age.[26] At that stage, questions regarding whether the definition of a document was wide enough to include computers came to the fore.[27] Section 33 of the CPEA defined a 'document' to include 'any book, map, plan, drawing or photograph'.

The potential admissibility of computer-related evidence was effectively regulated by section 34 of the CPEA, which introduced a substantial exception to the hearsay rule regarding documentary evidence.[28] Section 34(1)(a) provided that:

> 'In any civil proceedings where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact shall on production of the original document be admissible as evidence of that fact.'

[23] [1958] 3 All SA 241 (A).
[24] [1958] 3 All SA 241 (A) 249.
[25] [1958] 3 All SA 241 (A) 250.
[26] Van der Merwe D et al (2008) 105.
[27] Van der Merwe D et al (2008) 105.
[28] Van der Merwe D et al (2008) 105.

The exception was subject to one of two conditions, namely the person who made the statement either- had personal knowledge of the matters dealt with in the statement; or where the document in question is or forms part of a record purporting to be a continuous record, made the statement (in so far as the matters dealt with therein are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had or might reasonably have been supposed to have personal knowledge of those matters.'[29]

In addition, the person making the statement must be called as a witness, unless he is dead or unfit due to a bodily or mental condition, or he is outside the Republic and it is not reasonably practical to secure his attendance or all reasonable efforts to find him were unsuccessful.[30]

The first case illustrating the need for legislative intervention in the field of information technology law was twenty-five years before the ECT Act was passed.[31] In *Narlis v South African Bank of Athens,* the bank sought to use the evidence of entries in banker's book to indicate an overdraft facility. The court examined the validity of the ledger cards and statements in terms of section 34 of the CPEA.[32] Holmes JA stated that 'a computer, perhaps, fortunately, is not a person' as contemplated by the section.[33] The court held that a computerised bank statement is not admissible, since it is not a statement in a document made by a *person* in a document.[34]

In *Ex parte Rosch* the electronic evidence consisted of a telephone company's records which were automatically generated for all phone calls made by its subscribers.[35] The court found the telephone records were documents generated by a computer without the assistance of a human agency.[36] Section 34(1) did not apply, as a statement made by a computer is not a statement by a person, thus no 'person' could give evidence in regard to the contents of the document.[37] Nor did the evidence amount to hearsay as a computer is not a 'person' as

[29] Section 34(1)(a)(i)-(ii).
[30] Section 34(1)(b).
[31] Watney M (2009) 3; SALRC Issue Paper 27 (2010) 7; *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A).
[32] 1976 (2) SA 573 (A) 577.
[33] 1976 (2) SA 573 (A) 577.
[34] 1976 (2) SA 573 (A) 577-578.
[35] [1998] 1 All SA 319 (W) 326.
[36] [1998] 1 All SA 319 (W) 327.
[37] [1998] 1 All SA 319 (W) 327.

contemplated by section 3(1) of the Law of Evidence Amendment Act.[38] The court also considered whether it was excluded in terms of the Computer Evidence Act and stated:

> 'In our view a reading of the statute makes it plain that the statute does not require that whatever is retrieved from a computer can only be used if the statute's requirements have been met. It is a facilitating act not a restricting one.'[39]

The court stated that 'the common law position prevails, ie evidence tending to prove or disprove an allegation which is in issue is admissible unless a specific ground for exclusion exists.'[40] The court held that the computer printout was held to be admissible as real evidence.[41]

Criminal Procedure Act 51 of 1977

In criminal proceedings, the admissibility of computer printouts was regulated by the CPA in terms of section 221,[42] section 222,[43] and section 236.[44] The CPA also incorporated section 38 of the CPEA, which has been made applicable to criminal matters.[45] However, the CPA was not amended to incorporate any provisions of the CEA. Although, the CPA was also based on English law it managed to avoid many of the computer-related pitfalls in comparison to the CPEA.[46]

Notably, the definition of a 'document' was much wider in the CPA than the civil equivalent.[47] Section 221(5) provided for 'any device by means of which information is recorded or stored'. Additionally, the Act merely speaks of 'any statement contained in a document'[48] as opposed to 'any statement made by a person in a document'[49] as stated in the

[38] [1998] 1 All SA 319 (W) 328.
[39] [1998] 1 All SA 319 (W) 327.
[40] [1998] 1 All SA 319 (W) 327.
[41] [1998] 1 All SA 319 (W) 327.
[42] Dealt with the admissibility of certain trade or business records.
[43] Made sections 33 to 38 of the Civil Proceedings Evidence Act, which dealt with documentary evidence, apply *mutatis mutandis* to criminal proceedings.
[44] Dealt with the proof of entries in accounting records and documentation of banks.
[45] Van der Merwe D et al (2008) 106.
[46] Van der Merwe D et al (2008) 106.
[47] Van der Merwe D et al (2008) 106.
[48] Section 221 of the Criminal Procedure Act.
[49] Section 34(1) of the Civil Proceedings Evidence Act.

CPEA.[50] The CPA also stated that nothing in Part VII of the CPEA shall prejudice the admissibility of any evidence that would otherwise be admissible.[51]

In *S v Harper* it was considered whether a computer printout of stored information or recorded on a computer, as a business record, is a 'document' as stipulated in section 221(5) of the CPEA.[52] Milne J held:

> 'The computer print-outs consist of typed words and figures and would, *prima facie*, clearly fall within the ordinary meaning of the word "document". …
>
> It seems to me necessarily envisaged that, because of the development of modern commerce and the necessity to store records relating to large sums of money and large numbers of people, special provisions would have to be made making evidence admissible that would not be able to be subject to the ordinary rigorous test of cross-examination. In so doing the Legislature has, in addition to stipulating compliance with the above pre-requisites [in terms of s 221], also enjoined the matters which are to be taken into account in estimating the weight to be attached to the statements, and I refer to the provisions of ss (3).
>
> It seems to me, therefore, that it is correct to interpret the word "document" in its ordinary grammatical sense, and that once one does so the computer print-outs themselves are admissible in terms of s 221.'[53]

On the question whether a computer, itself, would fall under the definition Milne J stated:

> 'The extended definition of "document" is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than mere storage or recording of information. … Even if the section could be interpreted to mean that what must be produced is that part of the computer on which information is recorded or stored, that would mean the tape or disc on which it was stored, and this would be meaningless unless the electronic impulses on that tape or disc were to be translated or transcribed into a representation or statement intelligible to the ordinary human eye – or perhaps ear. The section does not refer to the product of the device,

[50] Van der Merwe D et al (2008) 106.
[51] Section 38(1) of the Criminal Procedure Act.
[52] 1981(1) SA 88 (D).
[53] 1981(1) SA 88 (D) 96-97.

> nor does it refer to any document produced by the device, it refers to the document itself being produced.'[54]

Several commentators and courts have misinterpreted the dictum to mean that if the computer performed functions over and above 'the mere recording or storage of information', then the product of those functions, eg a computer printout would be inadmissible.[55] The court was concerned with whether or not a computer is included 'as any device by means of which information is recorded or stored' under subsection (5).[56] In *S v De Villiers*, O'Linn J pointed out that the authors misread that *dictum*.[57] *In casu*, the court applied the approach in *Harper* to the computer printouts and its production, and held that the bank statements are certified duplicate originals and admissible in terms of section 221. [58]

In *S v Mashiyi*,[59] the erroneous interpretation of *Harper* was applied in the case.[60] Miller J excluded computer printouts that contained information 'obtained after treatment by arrangement, sorting, synthesis and calculation by a computer' and that 'is not only information that has been retrieved and stored from other documents or any other source'.[61]

In conclusion Miller J remarked:

> 'I am therefore unable, in terms of the prevailing law, to admit as evidence the disputed documents which contain information that has been processed and generated by a computer. All that I can do is add my voice to the call that this *lacunae* in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered.'[62]

As the *Harper* decision, in regard to the non-admissibility of computer printouts in terms of section 221, had the effect that there was no legislation dealing specifically with computer evidence in criminal cases.[63]

[54] 1981(1) SA 88 (D) 95.
[55] SALRC Issue Paper 27 (2010) 24; Hoffmann LH & Zeffert DT *South African Law of Evidence* 4 ed (1988) 142.
[56] SALRC Issue Paper 27 (2010) 24.
[57] 1993 (1) SACR 574 (Nm) 577.
[58] 1993 (1) SACR 574 (Nm) 579.
[59] 2002 (2) SACR 387 (Tk).
[60] SALRC Issue Paper 27 (2010) 26.
[61] 2002 (2) SACR 387 (Tk) 390.
[62] 2002 (2) SACR 387 (Tk) 392.
[63] SALRC Issue Paper 27 (2010) 27.

Computer Evidence Act 57 of 1983

As a result of the *Narlis* decision, the South African Clearing Bankers' Association requested the South African Law Commission to investigate the need for dedicated legislation regulating the admissibility computer generated evidence.[64] Following a report made to the Minister of Justice by the Law Commission,[65] the Computer Evidence Act was passed by Parliament.[66]

The CEA was the first piece of information technology legislation, although it was only applicable to civil proceedings.[67] However in a subsequent report, the Law Commission did consider whether to extend the application of the Act to criminal proceedings, but any decisions were deferred pending further investigations.[68] The Law Commission argued that a criminal matter is more serious and that an unrepresented accused would not be able to effectively oppose any computer evidence put against him.[69]

The CEA provided that an authenticated computer printout was admissible as evidence of any fact recorded in it where direct oral evidence of the fact would be admissible.[70] 'Authenticated' meant that the printout must be accompanied with an authenticating affidavit and any other supplementary affidavits as may be required to prove reliability thereof.[71] The Act required that the deponent to the authenticating affidavit had to be qualified by reason of his knowledge and experience of computers and the particular system; and in respect of his examination of all relevant records and facts concerning the operation of the computer and the data and instructions supplied to it.[72] The evidential weight attached to the printout will depend on the circumstances of case.[73] Van der Merwe submitted that:

> 'It is likely that the evidential weight of such an "in-house" declaration would have been so low that banking (and similar) institutions would not have considered it worthwhile to take a chance on the affidavit's effectively settling the status of a disputed computer document. Instead, these institutions simply insert a clause in the

[64] Schwikkard PJ & van der Merwe SE (2009) 412; SALRC Issue Paper 27 (2010) 19.
[65] South African Law Commission (Project 6) *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers* (1982).
[66] Watney M (2009) 3.
[67] Watney M (2009) 3.
[68] South African Law Commission Report (Project 6) *Review of the Law Evidence* (1986).
[69] SALC Report (1986).
[70] Section 3(1) of the Computer Evidence Act.
[71] Section 1 read with section 2 of the Computer Evidence Act.
[72] Section 2(3) of the Computer Evidence Act.
[73] Section 4(1) of the Computer Evidence Act.

fine print of the contracts with their customers in terms of which the customers undertook not to query the authenticity of any computer-based documents should any dispute arise in that regard'.[74]

Initially, the South African Law Commission was satisfied with the legislation.[75] However, the response to the CEA was mostly negative.[76] Consequently, the South African Law Commission headed a project entitled the 'Investigation into the Computer Evidence Act'[77] to ascertain the cause of the Act's problematic nature.[78] A view is that the Act failed to make reference to respected international standards and it did not determine how the archival requirements of others statutes is affected by a computer medium.[79]

The SALRC endeavoured to provide more updated legislation to regulate electronic commerce, which led to a discussion paper for legislation dealing with computer crime and related procedural aspects, including evidence.[80] This discussion paper had a significant role in the adoption of standards in regard to the admissibility and evidential weight of electronic evidence.[81] Concomitantly, a private initiative was led for a 'Green paper on e-commerce'.[82] Both of these initiatives merged into a task team under the auspices of the Department of Communication which led to the ECT Act.[83] Hofman stated that although the Department of Justice took part in the consultations that preceded the ECT Act, not much was contributed to what the Act says about the law of evidence.[84]

Electronic Communications and Transactions Act 25 of 2002

In 2002 the ECT Act was enacted and, amongst other things, repealed the CEA.[85] The repeal was welcomed, due to the onerous technical requirements found in the CEA.[86] The ECT Act is largely based on the United Nations Commission on International Trade Law

[74] Van der Merwe D et al (2008) 108.
[75] South African Law Commission (Project 6) Report *Review of the Law of Evidence* (1987).
[76] Van der Merwe D et al (2008) 108.
[77] South African Law Commission Working Paper 60 (Project 95) *Investigation into the Computer Evidence Act 57 of 1983* (1995).
[78] Van der Merwe D et al (2008) 108.
[79] Van der Merwe D 'Computer law'at para 14.
[80] South African Law Commission Discussion Paper 99 (Project 108) *Computer-related Crime* (2001); South African Law Commission Issue Paper 14 (Project 108) *Computer-related crime* (1998).
[81] Van der Merwe D et al (2008) 109.
[82] Van der Merwe D et al (2008) 109.
[83] Van der Merwe D et al (2008) 109.
[84] Hofman J 'South Africa' in Mason (ed) *Electronic Evidence* 2 ed (2010) 677.
[85] Section 92 of the ECT Act; SALRC Issue Paper 27 (2010) 21.
[86] Schwikkard PJ & van der Merwe SE (2009) 412.

('UNICTRAL')[87] Model Law on Electronic Commerce with Guide to Enactment 1996 ('Model Law').[88]

The ECT Act is an omnibus act that deals with many different provisions regarding transactions and communications that are concluded electronically.[89] The Act accommodates developments in technology by creating a new type of evidence that is related to information represented in any electronic form.[90] The Act has done away with concepts such as computer printouts,[91] and provides for the legal recognition of 'data'[92] and 'data messages'[93] as electronic evidence.[94]

The ECT Act excludes the validity of certain types of electronic transactions, such as a bill of exchange, will or codicil, long-term lease or alienation of immovable property agreement.[95] The Act also does not limit the operation of any law that regulates, authorises or prohibits the use of data messages.[96] The Model Law did not specify exclusions, but contemplated that countries would like to exclude some laws from its rules.[97]

1.3 The Research Question

The traditional law of evidence originates from the physical medium, and it is dubious whether it has developed sufficiently to regulate the problems that pertain to electronic evidence.[98]

The law has regularly faced questions such as, when information that was stored electronically should be admitted as evidence, and how should the evidential value be assessed.[99]

---

[87] UNCITRAL is a subsidiary of the United Nations General Assembly.
[88] Hofman J (2010) 677.
[89] Van der Merwe D et al (2008) 110.
[90] Schwikkard PJ & van der Merwe SE (2009) 404.
[91] Schwikkard PJ & van der Merwe SE (2009) 412, 404-405.
[92] Defined in section 1 as electronic representations of information in any form.
[93] Defined in section 1 as data generated, sent received, or stored and includes (a) voice, where the voice is used in an automated transactions; and (b) a stored record.
[94] SALRC Issue Paper 27 (2010) 21.
[95] Section 4(4) read with Schedule 2 of the Electronic Communications and Transactions Act.
[96] Section 4(5) of the Electronic Communications and Transactions Act.
[97] UNICTRAL *Model Law on Electronic Commerce with Guide to Enactment* 1996 36-37.
[98] Watney M (2009) 3.
[99] Van der Merwe D et al (2008) 104.

The research question of this study:

(a) Is the South African law of evidence sufficient to regulate the admissibility and evidential weight of electronic evidence?

The aims of this research are:

(a) To propose recommendations that address *lacunae* in current legislation by the introduction of an amendment, the enactment of other legislation or the adoption of universal standards in regard to electronic evidence, if necessary.
(b) To build on further research in the area of electronic evidence in South Africa.

1.4 Methodology and Overview

The most suitable research methods to conduct the above are a combination of a literature review and a comparative analysis. This research will analyse legislation, case law, law commission papers and reports, as well as academic commentary on electronic evidence in South Africa, Canada and England. A comparative analysis will be conducted in order to determine whether South Africa is adequately regulating electronic evidence in light of international and foreign law.

South Africa has effectively adopted the UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with the enactment of the Electronic Communications Act 25 of 2002. For the purpose of comparative analysis, a country that has also ratified or adopted the relevant provision of the Model Law on Electronic Commerce will be used to conduct this research. Canada has ratified the Model Law on Electronic Commerce in terms of the Uniform Electronic Evidence Act of 1998.

Countries that follow the European Union's *Electronic Commerce Directives* are also relevant in order to sufficiently draw a comparison between the regulation of electronic evidence within South Africa and the international community. England, which follows the *Electronic Commerce Directives*, will be used to broaden the comparative research

This is a brief overview and outline of the following chapters:

- Chapter 2: Electronic Evidence within the South African Legal Framework

This chapter provides an overview of the South African legal framework regarding electronic evidence. The chapter identifies the legal principles found in the common law, case law and

legislation that govern the admissibility and evidential weight of electronic evidence in South Africa. The chapter also surveys the South African academic opinion on the treatment of evidence in electronic format.

- Chapter 3: Electronic Evidence within the English Legal Framework

This chapter provides a background to electronic evidence in England and Wales. The chapter also discusses the rules that regulate the admissibility and evidential weight of electronic evidence in terms of English law.

- Chapter 4: Electronic Evidence within the Canadian Legal Framework

This chapter sets out the background and history regarding electronic evidence in Canada. The chapter also examines the current Canadian legal framework and academic opinion in regard to electronic evidence.

- Chapter 5: Recommendations and Conclusion

This chapter provides a summary of the different legal positions regarding electronic evidence in South Africa, England and Canada. The chapter then compares and discusses recommendations in terms of the regulation of electronic evidence in South Africa.

1.5 Conclusion

The historical background of electronic evidence provides for much insight on the importance of electronic evidence, how electronic evidence was treated, and the issues in that regard. A further discussion is necessary on the current approach to electronic evidence in South Africa. The next chapter discusses the admissibility and evidential weight of electronic evidence in the current South African legal framework.

CHAPTER 2: ELECTRONIC EVIDENCE WITHIN THE SOUTH AFRICAN LEGAL FRAMEWORK

2.1 Introduction

This chapter will deal with the legal rules that govern the admissibility and evidential weight of electronic evidence in South Africa.

Section 15 of the ECT Act primarily deals with the law of evidence. The purpose of the section is two-fold, namely to establish the admissibility and the evidential value of data messages in legal proceedings.[100] It has been questioned whether section 15 applies to non-commercial matters because the Act contains no expression provision in that regard, however it would not be consistent with the purpose of the Act as stated in the long title 'to provide for the facilitation and regulation of electronic communications and transactions'.[101]

2.2 The Rules of Admissibility for Evidence

The admissibility of evidence is foundationally based on the principle that '[a]ll facts relevant to the issue in the legal proceedings may be proved.'[102] Section 210 of the CPA stipulates that '[n]o evidence as to any fact, matter or thing shall be admissible which is irrelevant or immaterial and which cannot conduce to prove or disprove any point or fact in criminal proceedings.'[103]

Relevance is a matter of common sense,[104] according to the every-day standards of reason prevailing at the time of a particular case (and much of that depends on the judicial officer).[105] Based on the facts of a case not all evidence that is logically relevant is legally relevant, for example evidence that is excluded by an exclusionary rule[106] or a binding precedent.[107] Therefore, any evidence which is relevant is admissible unless there is some other rule of evidence which excludes it.[108]

---

[100] SALRC Issue Paper 27 (2010) 41.
[101] Hofman J (2010) 680.
[102] *R v Trupedo* 1920 AD 58 at 62; *S v Gokool* 1965 3 SA 461 (N) at 475.
[103] Act 51 of 1977.
[104] *R v Matthews* 1960 (1) SA 752 (A) 758.
[105] Zeffert DT, Paizes A and Skeen A St Q (2003) 220; *DPP v Boardman* [1975] AC 421 (HL) 444.
[106] Schwikkard PJ & van der Merwe SE (2009) 45.
[107] Zeffert DT, Paizes A and Skeen A St Q (2003) 221.
[108] *R v Schaube-Kuffler* 1969 2 SA 40 (RA) at 50.

Section 35(5) of the Constitutions states that '[e]vidence obtained in a manner that violates any right in the Bill of Rights must be excluded if the administration of that evidence would render the trial unfair or otherwise be detrimental to the administration of justice.'[109] The threshold of section 35(5) is the violation of a constitutional right.[110] Thereafter, a court will determine whether the admission would render the trial unfair or be detrimental to the administration of justice.[111] In *S v Tandwa* it was held that the following factors are relevant in determining trial unfairness:

> '[t]he severity of the rights violation and the degree of prejudice, weighed against the public policy interest in bringing criminals to book. Rights violations are severe when they stem from deliberate conduct of the police or are flagrant in nature. There is a high degree of prejudice when there is a close causal connection between the rights violation and the subsequent self-incriminating acts of the accused.'[112]

In regard to the second leg of section 35(5), Cloete J stated the following in *S v Mphala*:

> 'So far as the administration of justice is concerned, there must be a balance between, on the one hand, respect (particularly by law enforcement agencies) for the Bill of Rights, and, on the other, respect (particularly by the man in the street) for the judicial process.'[113]

In determining whether or not the admission would be detrimental to the administration of just the following factors are considered namely, the absence of good faith by the police,[114] the public safety and urgency,[115] the nature and seriousness of violation,[116] the availability of lawful means to secure evidence,[117] and the inevitable discovery of the evidence.[118] Electronic evidence which is relevant may be excluded by the operation of section 35(5) if it was unconstitutionally obtained.

In respect of electronic evidence, the admissibility of data messages is provided for in section 15(1) of the ECT Act which states that:

> '15(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

[109] Act 108 of 1996.
[110] Schwikkard PJ & van der Merwe SE (2009) 216.
[111] Schwikkard PJ & van der Merwe SE (2009) 215.
[112] *S v Tandwa* 2008 (1) SACR 613 (SCA) at [117].
[113] 1998 1 SACR 654 (W) at 657.
[114] *S v Naidoo* 1998 1 SACR 479 (N).
[115] *S v Madiba* 1998 1 BLCR 38 (D).
[116] *S v Mark* 2001 1 SACR 572 (C).
[117] Schwikkard PJ & van der Merwe SE (2009) 257.
[118] Schwikkard PJ & van der Merwe SE (2009) 258.

(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.'

This section does not make every data message admissible.[119] The wording of the section assumes it may be denied on other grounds not found in the ECT Act (since the Act does not contain any such grounds).[120] Therefore, except where the Act changes it, the ordinary South African law on the admissibility of evidence applies to data messages.[121] The wording also indicates that the form in which certain information is presented cannot be used as the only ground to deny admissibility.[122] If the section was phrased in the positive, it would go against the functional equivalence created between the data messages and other evidence by treating them differently.[123]

Section 15 has been interpreted to distinguish between the computerised equivalent of real evidence and that of hearsay evidence.[124] In *Ndlovu v Minister of Correctional Services and another*,[125] Gautschi AJ states:

> '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" to be admitted, and due evidential weight to be given thereto according to an assessment having regard to certain factors.'[126]

In the case, the Minister of Correctional Services relied on a two-page computer printout from the Department's computer system which recorded entries from various authors relating to Ndlovu's parole violations. The court held that the computer printout is treated as documentary evidence, which must be relevant, authentic and the original unless it satisfies

[119] Hofman J 'South Africa' in Mason S (ed) *Electronic Evidence* (2010) 681.
[120] Hofman J (2010) 681.
[121] Hofman J (2010) 682.
[122] Hofman J (2010) 681-682.
[123] Hofman J (2010) 681.
[124] SALRC Issue Paper 27 (2010) 42.
[125] [2006] 4 All SA 165 (W).
[126] [2006] 4 All SA 165 (W) 172.

the best evidence rule.[127] Where the authors did not testify the remaining entries were treated as hearsay evidence.[128]

S v Ndiki and Others,[129] was another case that found section 15 distinguishes between two types of electronic evidence, Van Zyl J states:

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

According to this common sense approach, the first port of call is to 'closely examine the evidence in issue and to determine what kind of evidence it is and what the requirements for admissibility are'.[130] In the case, the accused were charged with fraud and theft in connection with the delivery of medical supplies to the Department of Health and Welfare. The state relied on a series of computer printouts to prove the fraud. The court found that certain computer printouts contained documentary statements which were dependent upon the credibility of the signatories, and the computer was merely used as a tool to make typed hearsay statements.[131] The other computer printouts were treated as real evidence because it was created without any human intervention.[132]

The approach in *Ndiki* case signifies a shift to a protocol approach, which classifies products of technology as real evidence, whereas a paper approach tends to view such products of as documentary evidence.[133]

2.2.1 Real Evidence

[127] [2006] 4 All SA 165 (W) 173.
[128] [2006] 4 All SA 165 (W) 173.
[129] [2007] 2 All SA 185 (Ck).
[130] [2007] 2 All SA 185 (Ck) para 53.
[131] [2007] 2 All SA 185 (Ck) para 35.
[132] [2007] 2 All SA 185 (Ck) para 37.
[133] Van der Merwe D et al (2008) 123.

Real evidence consists of things which are examined by the court as means of proof upon proper identification and, it becomes, of itself evidence.[134] Upon proper identification, real evidence must only be relevant for it to be admitted.[135]

The traditional view is that graphics, audio and video are real evidence.[136] This view does not take into account the way graphics, audio and video can be stored, recorded, and distributed in digital form, which becomes susceptible to error or falsification in the same way as documents.[137] It has been argued that graphics, audio or video in the form of a data message should be produced, be original in form and be authenticated to guard against these alterations.[138] This academic view is also supported by case law.[139]

There is no hearsay involved with regard to real evidence; the only persons that are likely to be cross-examined are the computer experts explaining the appropriate standards of accuracy and whether the computer conformed to them.[140] In the *Ndiki* case, a relevant factor would also be the reliability of operating system of the computer.[141]

Other real evidence could be a computer program, which is in the form of data message.[142] A computer program has at some point a human author and, thus, could be treated as a document.[143] However, a computer program can also produce data without human intervention, which is the functional equivalent to a piece of equipment and should be treated as real evidence.[144] For example, a computer programme that captures traffic data.[145] A

[134] *S v M* 2002 (2) SACR 411 (SCA) para 31; Schwikkard PJ & van der Merwe SE (2009) 395; Zeffert DT, Paizes A and Skeen A St Q (2003) 703.
[135] Schwikkard PJ & van der Merwe SE (2009) 395; Hofman J (2010) 689.
[136] Watney M (2009) 9; Hofman J (2010) 690.
[137] Hofman J (2010) 690.
[138] Zeffert DT, Paizes A and Skeen A St Q (2003) 704-706; Zeffert relied on *S v Ramgobin* 1986 (4) SA 117 (N).
[139] Watney M (2009) 9; In *S v Motata* (Johannesburg District Court) unreported case no 63/968/07 at 622, the complaint made certain audio recordings on his mobile phone after the accused allegedly crashed into the boundary wall of his residential property. The audio recordings were later transferred from the mobile phone and stored on a laptop. The original audio recordings were not available at the time of the trial, and the court found that the audio recordings were documentary evidence and ruled it as admissible.
[140] Van der Merwe D et al (2008) 123.
[141] [2007] 2 All SA 185 (Ck) para 54.
[142] Hofman J (2010) 690.
[143] Hofman J (2010) 690.
[144] Hofman J (2010) 690.
[145] Watney M (2009) 10.

logical approach would be to ask what the computer program is being used for and to treat it accordingly.[146]

2.2.2 Documentary Evidence

The word document is widely defined and includes 'everything that contains written or pictorial proof of something [and] it does not matter of what material it is made'.[147] A document will be admitted into evidence if original document was produced and authenticated.[148]

A document may include electronic information or in other words a data message.[149] Data messages that are the functional equivalent,[150] to documents must meet the ordinary requirements in the South African law of evidence for the admissibility of documents (except where the ECT Act exempts them).[151]

In addition, documentary evidence from a computer may involve hearsay, and it is necessary to determine whether the value of the statements depend on the credibility of anyone other than the person giving the evidence.[152] As illustrated by the *Ndlovu* case, the truth of the contents of such statements must be tested against the author.

Original

A general rule is that 'no evidence is ordinarily admissible to prove the contents of a document except the original document itself'.[153] Originality is a requirement in South African law and, consequently, secondary evidence cannot prove the contents of a document.[154] However, secondary evidence may be used if it is the only means of proving the

[146] Hofman J (2010) 690.
[147] *Seccombe v Attorney-General* 2002 (2) All SA 185 (Ck) 277; Schwikkard PJ & van der Merwe SE (2009) 404; Zeffert DT, Paizes A and Skeen A St Q (2003) 685.
[148] Watney M (2009) 6; Schwikkard PJ & van der Merwe SE (2009) 405; Zeffert DT, Paizes A and Skeen A St Q (2003) 685.
[149] Watney M (2009) 5.
[150] The doctrine of functional equivalence (as used in the Model Law) means electronic evidence should be treated as the functional equivalent of paper.
[151] Hofman J (2010) 682.
[152] Van der Merwe D et al (2008) 123.
[153] *Standard Merchant Bank v Creaser* 1982 (4) SA 671 (W) 674; Zeffert DT, Paizes A and Skeen A St Q (2003) 686; Hofman J (2010) 682.
[154] *R v Pelunsky* 1914 AD 360; Schwikkard PJ & van der Merwe SE (2009) 405.

document.[155] Other exceptional cases include: if the document is lost or destroyed; or the document is in the possession of the opposing party; or a third party; or it is impossible or inconvenient to produce the original; or it is permitted by statute.[156]

Section 14 of the ECT Act provides that a data message will met the requirement of originality:

> '14(1) Where a law requires the information to be presented or retained in its original form, that requirement is met 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);
>
> b) That information is capable of being displayed or produced to the person to whom it is to be presented.
>
> (2) For 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.'

When a data message is used as evidence, it must be shown that the computer system has maintained the integrity of the original,[157] because alterations are much less apparent on a digital document when compared to its paper equivalent.[158]

Authenticity

Any party who tenders a document as evidence is required to satisfy the court of its authenticity.[159] This is generally done by adducing evidence of authorship or possession, depending on the purpose for which the evidence was tendered.[160] In *Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa*, Human J stated several ways to do so:

---

[155] *Welz v Hall* 1996 4 SA 1073 (C); Schwikkard PJ & van der Merwe SE (2009) 405.
[156] Schwikkard PJ & van der Merwe SE (2009) 406.
[157] Watney M (2009) 7.
[158] Van der Merwe D et al (2008) 115.
[159] Zeffert DT, Paizes A and Skeen A St Q (2003) 694; Watney M (2009) 8; Hofman J (2010) 683.
[160] Schwikkard PJ & van der Merwe SE (2009) 407.

> 'The law in relation to the proof of private documents is that the document must be identified by a witness who is either (i) writer or signatory thereof, or (ii) the attesting witness, or (iii) the person in whose lawful custody the document is, or (iv) the person who found it in possession of the opposite party, or (v) handwriting expert …' [161]

In terms of the ECT Act the person responsible for the data message must establish its authenticity.[162] An advanced electronic signature[163] may be used to warrant the authorship and authenticity of an electronic document.[164] Notably, there are also two presumptions regarding the correctness of the data message in terms of section 15(4) and section 13 of the Act.[165]

2.3 The Exclusionary Rules of Evidence

2.3.1 The Best Evidence Rule

Conradie J in *Welz v Hall* stated that:

> 'As far as the best evidence rule is concerned, it is a rule which applies nowadays only in the context of documents, and then only when the content of a document is directly in issue. … It provides that the original of a document is the best evidence of its contents. This rule is a very ancient one. It goes back to the Dark Ages, well perhaps the twilight days, before faxes and photocopying machine, when making copies was difficult and such copies as were made often inaccurate.'[166]

The best evidence rule is still in operation and also applies in the context of electronic documents, in other words data messages which are the functional equivalent to a paper document. The rational of the best evidence rule is to exclude inaccurate copies and to ensure that the most reliable evidence is produced. As copying technology develops the need for this ancient rule should be questioned. However, Zeffert commented that the compliance with the rule might be warranted since it is easy to tamper with electronic copies, and that courts should apply a more restrictive approach.[167]

---

[161] 1971 (3) SA 937 (T) 940.
[162] Watney M (2009) 8.
[163] Section 1 defines an 'advanced electronic signature' as an electronic signature which results from a process which has been accredited by an Authority as provided for in section 37.
[164] Van der Merwe D et al (2008) 115 and 123.
[165] Discussed respectively in 2.3.2.1 and 2.4 below.
[166] 1996 (4) SA 1073 (C) 1079.
[167] Zeffert DT, Paizes A and Skeen A St Q (2003) 358.

In terms of the ECT Act, if the data message is the best evidence that the person adducing it could reasonably be expected to obtain, then the original form requirement is exempted in terms of section 15(1)(b) of the Act. Thus, the data message cannot be refused merely because it is not seen as an original.

2.3.2 The Hearsay Evidence Rule

The Law of Evidence Amendment Act 45 of 1988 brought about significant changes to the South African law of evidence, such as a new definition of hearsay.[168] Hearsay evidence is defined as 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'.[169]

The ordinary rules regarding the admissibility of hearsay evidence should also apply to electronic evidence.[170] The reference to writing in the definition means that the rule applies to data messages.[171] When a data message is used merely to establish the fact that information was sent, received or stored it is not excluded.[172] Where a data message is used to show the truth of its contents, the common law requires the one responsible for the data message should be available for cross-examination about its contents.[173]

It has been argued that the definition of a data message is wide enough to make all data messages admissible whether they constitute hearsay or not.[174] Hofman submits that this argument confuses form with content and that 'the law excludes a document as hearsay, because of the doubts about the reliability of its content, not because about the reliability of the technology used to record that content'.[175] Therefore, a data message being used to show the truth of its content should be treated in the same as a document and can only be admitted if the author of the data message testifies about the content.[176] In *MTN Service Provider (Pty) Limited v L A Consortium & Vending CC t/a L A Enterprises and Others*, the plaintiff

[168] Van der Merwe D et al (2008) 109.
[169] Section 3(4) of the Law of Evidence Amendment Act; Schwikkard PJ & van der Merwe SE (2009) 275-276; Zeffert DT, Paizes A and Skeen A St Q *The South African Law of Evidence* (2003) 366-368.
[170] Zeffert DT, Paizes A and Skeen A St Q (2003) 393-395; Van der Merwe D et al (2008) 125.
[171] Hofman J (2010) 684.
[172] Watney M (2009) 8; Hofman J (2010) 684.
[173] Watney M (2009) 8; Hofman J (2010) 684.
[174] Collier D 'Criminal law and the Internet' 385.
[175] Hofman J (2010) 684; Van der Merwe D et al (2008) 125.
[176] Hofman J (2010) 684.

claimed payment from the defendant in respect of, *inter alia*, electronic signal facilities sold and delivered.[177] The plaintiff relied on computer generated statements indicating activations on the plaintiff's computer system to prove the delivery of the network services.[178] The defendant argued that the evidence amounts to inadmissible hearsay.[179] The court held, although the orders were captured by his staff, the head of the department was responsible for the correct capturing of orders onto a computer system, and his evidence in regard to the transactions recorded in the statements and the summary of the transactions constituted direct evidence of its correctness.[180]

2.3.2.1 The Exceptions to the Hearsay Evidence Rule

If the probative value depends on any other person than the person giving such evidence, the evidence will be inadmissible unless it falls under the exceptions to the hearsay rule.[181]

If a data message satisfies any of the following conditions it is admissible as evidence. Section 3 of the Law of Evidence Amendment Act provides for the following exceptions:

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

[177] 2011 (4) SA 562 (W) 566-567.
[178] 2011 (4) SA 562 (W) 560-562.
[179] 2011 (4) SA 562 (W) 578.
[180] 2011 (4) SA 562 (W) 579.
[181] Section 3(1)(a)-(c) of the Law of Evidence Amendment; Schwikkard PJ & van der Merwe SE (2009) 276-283; Zeffert DT, Paizes A and Skeen A St Q (2003) 369-380.

(vi) any other factor which should in the opinion of the court be taken into account, is of the opinion that such evidence should be admitted in the interest of justice.'

The main impact of the Law of Evidence Amendment Act was to provide new statutory grounds for allowing hearsay evidence at the discretion of the court.[182] The Act treats together the admissibility and evidential weight of hearsay evidence and computer-generated evidence.[183] Collier submits that all computer printouts occur with human intervention because the computer is driven by a program written by a human author.[184] However, the focus should rather be on whether the program requires a human input during its operation of computer in order to produce the printout.

The business record rule is another exception in terms of the hearsay evidence rule. Section 15(4) of the ECT Act creates a rebuttable presumption in favour of data made in the ordinary course of business. In *Ndlovu*, Gautschi AJ takes the view that section 15(4) provides for two situations in which data messages may be admissible on its mere production:

> 'The first is a "data message made by a person in the ordinary course of business", which is 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 a data message which is certified to be correct by an officer in the service of such person (being the 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 contents contained therein.'[185]

In the *MTN* case the data message was part of the second situation. Claassen J stated:

> 'Their evidence [referring to the senior financial manager and the product manager] is uncontroverted that the capturing of the transaction was in the ordinary course of the business of the plaintiff. To the extent that the documents are copies or printouts or extracts from the data messages, their certifications as officers in the employ of the

[182] Section 3(1)(c) of the Law of Evidence Amendment Act; Van der Merwe D et al (2008) 109.
[183] Van der Merwe D et al (2008) 110.
[184] Collier D 'Evidently not so simple: Producing computer print-outs in court' 2005 (1) *JBL* 6.
[185] *Ndlovu v Minister of Correctional Services and another* [2006] 4 All SA 165 (W); SALRC Issue Paper 27 (2010) 42.

plaintiff, make the documents on mere production admissible and therefore the documents constitute rebuttable proof of the facts contained therein.'[186]

This section is not based on the Model Law and the current wording of the section is seen as problematic.[187] Hofman argues by creating such a broad exception, the section goes against the functional equivalence approach that should apply between data messages and written documents in terms of the Model Law.[188] Hofman questions the constitutionality of the section 15(4) and highlights six main difficulties with the way the section is worded:

(i) 'First, an exception for communications made 'in the ordinary course of business' is much wider than the previous business record exceptions. Taken at face value, this exception could apply to any email or even a recorded voice message made in the course of business.

(ii) Second, s 15(4) is not only wider in scope than the previous business record exceptions. It differs from all of them (although not the exceptions for banking records) in making data messages not only admissible as evidence but also rebuttable proof of facts they contain. Attaching a probative value to bank records is acceptable because banks are regulated and supposedly responsible institutions whose records can be assumed to be reliable in much the way as the records of a public body. However, s 15(4) applies to records of any business is no guarantee that the records of that business are kept accurately or honestly.

(iii) Third, s 15(4) requires a certificate 'by an officer in the service of such person' for the data message to be admissible. This imposes less responsibility than the affidavit previously required for banking exceptions. There is also no need for the certificate to assert, as required in affidavit, that the records have been under the control of the business.

(iv) Fourth, if the person wanting to submit this form of evidence does not control the computer system which contains it, it may be difficult to get the certificate required to make the evidence admissible.

(v) Fifth, the wide range of evidence that s 15(4) makes admissible could lead courts to being asked to consider much larger volumes of evidence than at present.

[186] *MTN Service Provider (Pty) Limited v L A Consortium & Vending CC t/a L A Enterprises and Others* 2011 (4) SA 562 (W) 581.
[187] Hofman J (2010) 691.
[188] Hofman J (2010) 689.

(vi) Sixth, when applied in a criminal prosecution, for which s 15(4) explicitly provides, the presumption of truth the section creates is open to constitutional challenge as an unjustified shifting of the onus of proof onto the accused.'[189]

This section treats data messages made in the ordinary course of business differently than its documentary equivalent, which is problematic in that format shopping may be promoted.

2.4 Evidential Weight

Once evidence is admitted, a court must decide what weight to attach when evaluating the evidence.[190]

The evidential weight of a data message must similarly be determined, once admitted into evidence. The ECT Act states that 'information in the form of a data message must be given due evidential weight'.[191] In terms of section 15(3) of the ECT Act when assessing the weight of a data message, the following factors may be taken into account:

'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;

(d) Any other relevant factors.

In the *Ndiki* case, the accuracy of the computer is an important consideration when evaluating (real) evidence from a computer.[192] The computer experts are likely to be cross-examined explaining the required standards of accuracy, and whether that computer met at the time the data generated, stored or communicated.[193] Van Zyl J states that any doubts as to the accuracy of the operating system may affect the reliability of the evidence and the evidential weight given thereto.[194]

[189] Hofman J (2010) 689.
[190] Hofman J (2010) 691; Watney M (2009) 10.
[191] Section 15(2) of the Electronic Communications and Transactions Act.
[192] *S v Ndiki and Others* [2007] 2 All SA 185 (Ck) 196*;* Van der Merwe D et al (2008) 123.
[193] Van der Merwe D et al (2008) 122.
[194] [2007] 2 All SA 185 (Ck) para 32.

Hofman suggests that the court will need an expert to help understand the technical procedures in regard to the accuracy and reliability of a computer.[195] When dealing with electronic documents it is important to find alternative electronic guarantees of reliability.[196] For example, encryption programs may help secure the integrity of a data message.[197] The courts may start to take judicial notice of the less technical features in respect of data messages.[198]

The ECT Act creates two presumptions in favour of the correctness of data messages. These presumptions ultimately affect the evidential weight attached to a data message. Section 13(4) states that 'where an advanced electronic signature has been used, such signature is regarded as being a valid advanced electronic signature and to have been properly applied, unless the contrary is proved'. Section 13(2) provides that electronic signatures that do not qualify as advanced electronic signatures[199] will not any carry evidential weight in respect of the data message. Secondly, the presumption in terms section 15(4) deals with business records has already been discussed.[200]

2.5 Conclusion

It is important to understand the current South African approach to the admissibility and evidential weight of electronic evidence, in order to ascertain whether or not it is adequately regulated in comparison with other countries and international trends.

The next chapter will discuss the legal principles that regulate evidence in electronic format, with regard to the admissibility and evidential weight thereof, in England.

[195] Hofman J (2010) 692; Watney M (2009) 10.
[196] Van der Merwe D et al (2008) 123.
[197] Van der Merwe D et al (2008) 115.
[198] Hofman J (2010) 692; Watney M (2009) 10.
[199] Section 1 read with section 13 and section 37.
[200] Discussed above 2.3.2.

CHAPTER 3: ELECTRONIC EVIDENCE WITHIN THE ENGLISH LEGAL FRAMEWORK

3.1 Introduction

The aim of this chapter is to set out the legal principles that govern electronic evidence in civil and criminal proceedings in England and Wales.

European Union legislation has found application in the United Kingdom. The basis for most of the European Union legislation is the EU Directive on Commerce[201] and the Electronic Signature Directive,[202] which has been adopted in terms of the Electronic Communications Act by the United Kingdom.[203]

In light of electronic evidence, England has adopted the approach of creating a statutory solution drafted specifically with computers in mind.[204] In this regard, the following two pieces of notable legislation shall be examined, the Civil Evidence Act of 1995 and the Criminal Justice Act of 2003.

3.2 The Rules of Admissibility for Evidence

To determine whether evidence is admissible is a matter of law for a judge.[205] The decision of the judge is conclusive in regard to the admissibility of the evidence.[206] In *R v Dove*, the accused appealed against a conviction of conspiracy to rob on the ground that the Beretta gun had no relevance to the issues which the jury had to decide.[207] The court found the Beretta was part of the evidential picture as guns were used in the previous robberies, and replica guns were also found with a robber's kit in a stolen car, which was linked to the accused's DNA.[208] The court held that the judge was correct in ruling on the relevance of the accused being found in possession of the Beretta.[209] As illustrated, evidence is admitted into legal

[201] 1999/93/EC.
[202] 2000/31/EC.
[203] Van der Merwe D et al (2008) 135.
[204] Van der Merwe D et al (2008) 134.
[205] Mason S (ed) *Electronic Evidence* 2 ed (2010) 319.
[206] Pattenden R 'Authenticating "things" in English law: Principles for adducing tangible evidence in common law jury trials' (2008) 12 *E&P* 290 at 277.
[207] [2005] EWCA Crim 1982 para 73.
[208] [2005] EWCA Crim 1982 para 74.
[209] [2005] EWCA Crim 1982 para 74.

proceedings if it is relevant to an issue in dispute, subject to a number of exceptions.[210] However, relevant evidence may be rejected under an exclusionary rule, such as the hearsay rule.[211]

3.2.1 Direct and Indirect Evidence

The existence of a physical object constitutes direct evidence, which can by proven by its production.[212] Evidence in electronic format such as video recordings, photographs and computer printouts are, mostly, admitted as real evidence,[213] although such evidence will be subject to proof of authentication, identity, integrity and accuracy.[214] Another form of direct evidence is the existence of fact; a fact can only be asserted by the testimony of a person,[215] such as the testimony of someone who perceived an object is admissible.[216]

Once a fact is proven, indirect evidence can be introduced, which comprises of facts that can be logically inferred from the initial fact.[217] The most significant inference is that electronic evidence is accurate and can be trusted.[218] However, the authenticity of electronic evidence should not be readily accepted, due to the fact it can be manipulated with relative ease. For example, an unprotected personal computer can be accessed easily without any discernible proof.

3.2.2 Primary and Secondary Evidence

A distinction is made between primary and secondary evidence. The main difference lies in between the production of an original document and the submission of inferior evidence, such as a copy of a document.[219]

In relation to electronic evidence, the primary evidence will compromise the storage media upon which the document resides, and the printing out of the document in human-readable

[210] Mason S (2010) 319.
[211] Pattenden R (2008) 277.
[212] Mason S (2010) 301.
[213] Mason S (2010) 301; *R v Penny* (2002) 163 CCC (3d) 329.
[214] Mason S (2010) 301; Pattenden R (2008) 290.
[215] Mason S (2010) 301.
[216] Mason S (2010) 301.
[217] Mason S (2010) 302.
[218] Mason S (2010) 302.
[219] Mason S (2010) 313.

format will be seen as secondary evidence of the document.[220] In practice, however electronic data is not tendered as evidence, but rather the printout of the data on the storage device.[221] The submission of electronic evidence as secondary evidence is therefore the norm.[222]

When the credibility of the data is in question, foundational testimony must be introduced and tested to determine whether it can be accepted into evidence.[223]

3.2.3 Real Evidence

The term 'real evidence' tends not to be used in practice, and it best described as 'material objects other than documents, produced for inspection of the court'.[224] Real evidence must be relevant to the contested issue for it to be admissible.[225]

If real evidence is considered to be a material object other than a document, the hard drive is the material item and the stored data is the document.[226] The position of electronic evidence as real evidence was cemented in *R v Spiby* where the court of appeal held that the trial judge properly admitted evidence of computer printouts of a machine that monitored hotel guests' phone calls.[227] Taylor LJ confirmed that the evidence 'was not a printout which depended in its contents for anything that had passed through the human mind' and so was admissible as real evidence.[228] This is similar to the South African case of *Ex Parte Rosch* where the court also found that the telephone records were created without the assistance of a human agency.[229] A computer printout that is self-generated does not amount to hearsay.[230] Such a printout contains no input from human thought, such as an automated screen capture.[231] However, if the device is fed information, either directly or indirectly, by a person, the printout is inadmissible until the information is proven to be accurate.[232]

[220] Mason S (2010) 313.
[221] Mason S (2010) 314.
[222] Mason S (2010) 312.
[223] Mason S (2010) 314.
[224] Mason S (2010) 302.
[225] Pattenden R (2008) 279.
[226] Mason S (2010) 304.
[227] (1990) 91 Cr App R 186.
[228] (1990) 91 Cr App R 186 at 191.
[229] [1998] 1 All SA 319 (W) 327.
[230] *R* v *Saward* [2005] EWCA Crim 3183 para 44.
[231] *R* v *Skinner* [2005] EWCA Crim 1439 para 21.
[232] Section 129(1) of the Criminal Justice Act 2003; Pattenden R (2008) 297.

Computer printouts are considered a form of real evidence or direct evidence, although computer printouts that are considered for the truth of the content will be a matter of further testimony.[233] In such an instance, computer printouts may be treated as documentary or hearsay evidence.

If authenticity of the evidence is not agreed upon, there must be some admissible evidence of provenance, integrity, identity and originality.[234] Generally, the evidence must be sufficient to sustain a finding of the existence of a fact, in the absence of proof to the contrary, and need not amount to *prima facie* evidence in the sufficiency sense.[235] The accuracy of the evidence normally goes to the evidential weight, however in some cases the quality is too poor to be fairly assessed and has no probative value.[236] In regard to audio and video computer output the courts have applied a *prima facie* test, which is a higher admissibility hurdle than for other tangible evidence.[237] This was due to the fact that the courts viewed audio and video output of a computer as a potentially more susceptible to manipulation.

3.2.4 Documentary Evidence

In terms of English common law, Darling J in *R v Daye* described a document as, 'any written thing capable of being evidence'.[238]

3.2.4.1 Criminal Proceedings

The Criminal Evidence Act of 1965 was the first legislative attempt to define a 'document' as 'any device by means of which information is recorded or stored'.[239] In the *R v Ewing* the issue was whether the computer printouts, which contained the transaction history of a bank account, were included as a 'document'.[240] The court stated a computer is a 'device by means of which information is recorded or stored' and the printout is a part of that device, for there is no other means to discover the information that was recorded or stored by the device.[241]

[233] Mason S (2010) 314.
[234] Pattenden R (2008) 280.
[235] Pattenden R (2008) 280.
[236] Pattenden R (2008) 290-291.
[237] *R* v *Saward* [2005] EWCA Crim 3183 para 42-44; *R v Murphy* [1990] NI 306 at 342.
[238] [1908] 2 KB 333 at 340.
[239] Section 1(4) of the Criminal Evidence Act.
[240] [1983] QB 1039.
[241] [1983] QB 1039 at 1050.

The court held that a computer printout is a 'document' within the meaning of the subsection (4).[242]

The Police and Criminal Evidence Act of 1984 (referred to as the 'PACE Act') repealed the Criminal Evidence Act. Section 69 dealt with the admissibility of evidence from computer records. In terms of the section, it had to be established that the computer was operating properly, for a computer generated document to be admitted as evidence. In *Darby v DPP* the question was whether a printout of data recorded on a speed gun was a 'document' in terms of section 69.[243] However, it was unnecessary to decide that aspect of the case for the prosecution could discharge the burden that the machine was working correctly.[244] In addition to the PACE Act, the Criminal Justice Act of 1988 also regulated documentary evidence to an extent. The Act provided for the admissibility of documentary evidence in regard to hearsay documents.[245]

Section 69 of PACE Act was repealed and replaced by section 60 the Youth and Criminal Justice Act of 1999. In terms of section 60, the proper use and operation of the computer is no longer required. The latter Act established a degree of functional equivalence between evidence obtained from an electronic source and documentary evidence.[246]

The Criminal Justice Act of 2003 consolidated and incorporated many of the provisions of the 1988 Act.[247] The 2003 Act the latest legislative attempt to address the admissibility of documentary evidence. Many of the provisions in the Criminal Justice Act of 1998 A document is widely defined as 'anything in which information of any description is recorded'.[248] This definition also conforms to the current non-prescriptive approach towards evidence in a digital format.[249] Section 133 of the Criminal Justice Act no longer mentions the number of times a copy is removed from the original. It is the content that is important and not the actual document. Accordingly, it is the content that is important and not the actual

[242] [1983] QB 1039 at 1050.
[243] [1995] RTR 294.
[244] [1995] RTR 301.
[245] Section 23, 24 and 27.
[246] Law Reform Commission of Ireland Consultation Paper 57 *Documentary and Electronic Evidence* (2009) 51.
[247] See section 133 of the Criminal Justice Act of 2003.
[248] Section 134 of the Criminal Justice Act of 2003.
[249] LRCI Consultation Paper 57 (2009) 12.

document, which can be compared favourably to the principles and provisions found in the ECT Act (specifically those in section 14, 16 and 17).

3.2.4.2 Civil Proceedings

In terms of civil matters, the meaning of 'document' and 'copy' is stipulated in section 13 of the Civil Evidence Act and Civil Procedure Rules of 1998 part 31.4:

> '"document" means anything in which information of any description is recorded and "copy" , in relation to a document, means anything onto which information is recoded in the document has been copied, by whatever means and whether directly or indirectly;'

The provisions of the Act and the procedural rules ensure that data stored in a digital format, in whatever form, will not prevent its admission into evidence.[250]

Judicial commentary indicates that technology will not prevent the definition of a document being expanded.[251] Buxton LJ in *Victor Chandler International Ltd v Customs and Excise Comrs* stated, 'the word "document" is not constrained by the physical nature that documents took in 1952, so we are entitled, and indeed bound, to consider … a document in the light of current practice and technology'.[252]

The Civil Evidence Act permits the introduction of copies of documents into evidence for the purpose of proving the statement contained in the document.[253] Section 8 deals with the admissibility of statements produced by a computer.[254] It is the statement that is important not the document itself.[255] For example, a printout is admissible as secondary evidence (if identical to the digital text), and it is also considered real evidence.[256] The printout is a copy of the original from the computer and the statement contained in the document can be considered to be authentic.[257]

---

[250] Mason S (2010) 340.
[251] Mason S (2010) 323.
[252] [2000] 2 Akk ER 315 at 329.
[253] Mason S (2010) 314.
[254] LRCI Consultation Paper 57 (2009) 51.
[255] Mason S (2010) 314.
[256] Mason S (2010) 314.
[257] Mason S (2010) 314.

With the development of technology, we are working in a more complex (and paperless) environment, and to determine the original document in digital form has become more difficult.[258] For example, if a party relies on a statement in a contract that was concluded (but not printed and signed) over various emails and attached documents, which version is the original? In such an instance, determining the authenticity of the content of the digital document will be a challenge, and the party relying on the statement will be required to adduce proof.[259] Rather than question whether a document which is in electronic format is an original or copy, the focus should be on the authenticity, provenance or reliability.[260] This approach removes many of the difficulties in regard to the admissibility of documentary evidence due to its electronic form.

Authentication

When a document is tendered, evidence of its authenticity must also be provided, unless a statutory exception applies or the authenticity is agreed upon.[261]

In the days when computers were relatively novel, section 69 of the PACE Act stipulated that a document produced by a computer is inadmissible, unless a judge was satisfied the computer was operating properly.[262] Electronic documentary evidence would only pass muster if it was shown:

> '(a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer;
>
> (b) That at all material times the computer was operating properly, or if not, that any respect which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of its contents.'

In *DPP v McKeown*, Lord Hoffman commented on section 69:

> 'But section 69 is not in the least concerned with the accuracy of the information supplied to the computer. … All that section 69 requires as a condition of the admissibility of a computer-generated statement is positive evidence that the

[258] See Mason S (2010) 314 for other examples.
[259] Mason S (2010) 316.
[260] Mason S (2010) 318.
[261] Pattenden R (2008) 293.
[262] Pattenden R (2008) 283.

computer has properly processed, stored and reproduced whatever information it received.'[263]

The case concerned readings the reliability of an intoximeter because the clock was slower than the time it should have displayed. Although the time was not in contention, the court a quo held that the machine was compromised and that the convictions must be set aside. On Appeal, a director of the laboratory testified that the breath analyser system was independent from the clock. The court held that the statements in regard to the breath readings were accurate and admissible.

Similarly in *R v Shepard*, the court held that the proper operation of a computer can be proven by evidence of a witness who was reasonably familiar with the operation the computer in question.[264]

As computers became more complex, the section was seen as impractical and costly.[265] Section 69 was repealed and replaced by section 60 of the Youth Justice and Criminal Evidence Act 1999. Subsequently there have been no special rules for the authentication of computer generated documents.[266]

The English courts have adopted an approach against a test for integrity.[267] In *Branagan v Director of Public Prosecutions* the defendant appealed a drink-driving conviction on the basis that it was not shown the intoximeter was working properly.[268] Simon Brown LJ held, 'there is no reason why the prosecution should have to prove one way or the other whether the machine was actually working properly.[269] The defendant is, if anything, better off it is assumed to be working: the option then becomes his as to whether to offer breath or blood sample and he elect which to provide'.[270]

The Youth Justice and Criminal Evidence Act provides for a presumption that the electronic device producing the evidential document is in legible permanent form was working properly

[263] [1997] 1 WLR 295 at 302.
[264] (1991) 93 Cr App Rep 139.
[265] Pattenden R (2008) 283.
[266] Pattenden R (2008) 297.
[267] LRCI Consultation Paper 57 (2009) 165.
[268] [2000] RTR 235.
[269] [2000] RTR 242.
[270] [2000] RTR 242.

at the material time and is admissible as real evidence.[271] The presumption is subject to rebuttal by evidence to the contrary.[272]

In terms of the Criminal Justice Act the best evidence rule is no longer an issue, and the statute leaves it to judicial discretion as to how to best authenticate the impugned document.[273] The Civil Evidence Act has also given the court discretion to determine the appropriate test for authentication of the document in the circumstances of each case.[274]

When dealing with the authenticity Mason states it is uncommon that reference will be made to standards issued by national or international bodies, but rather to the expert evidence of a digital specialist.[275] The nature of evidence available to determine the authenticity, when in question, will differ with each case and it is important to ascertain whether that specific item of electronic evidence is to be trusted or not.[276]

3.3 The Exclusionary Rules of Evidence

3.3.1 The Best Evidence Rule

The best evidence rule can be traced back to *Omychund v Barker*,[277] in which Lord Hardwicke stated the importance to have the 'best [evidence] that [the] nature of the case will admit'.[278] The intention of the rule is to eliminate the possibility of admitting fabricated, erroneous or inaccurate documents.[279] This is considered to be an exclusionary rule, so that anything that is not best evidence is inadmissible.[280] However, this rule can also be considered as an inclusionary rule, under which, whatever is the best evidence is admissible.[281]

[271] Section 60 of the Youth Justice and Criminal Evidence Act; LRCI Consultation Paper 57 (2009) 160.
[272] LRCI Consultation Paper 57 (2009) 160.
[273] Section 133 of the Criminal Justice Act of 2003; LRCI Consultation Paper 57 (2009) 183.
[274] LRCI Consultation Paper 57 (2009) 54.
[275] Mason S (2010) 86.
[276] Mason S (2010) 86.
[277] 1 ATK 21 at 49.
[278] Mason S (2010) 308.
[279] LRCI Consultation Paper 57 (2009) 30.
[280] Mason S (2010) 308.
[281] Mason S (2010) 308.

The best evidence rule is no longer of relevance, in civil cases, as illustrated in *Springsteen v Masquerade Music Ltd*.[282] Parker LJ stated:

> 'In my judgment, the time has now come when it can be said with confidence that the best evidence rule, long on its deathbed, has finally expired. In every case where a party seeks to adduce secondary evidence of the contents of a document, it is a matter for the court to decide, in the light of all the circumstances of the case, what (if any) weight to attach to that evidence. … Thus, the "admissibility" of secondary evidence of the contents of documents is, in my judgment, entirely dependent upon whether or not any weight is to be attached to that evidence.'[283]

The best evidence rule was, effectively, abolished by the Civil Evidence Act, which permit proof of secondary evidence.[284] The Act has removed, *inter alia*, the difficulties associated with the admissibility of scanned documents that were later reproduced.[285] Section 8 outlines the means of proving admissible documents in civil proceedings and generally deals with the proof of computer outputs.[286] The section stipulates that:

> '8(1) where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved -
>
> (a) by the production of that document, or
>
> (b) whether or not the document is still in existence, by the production of a copy of that document or of the material part of it, authenticated in such manner as the court may approve.
>
> (2) It is immaterial for this purpose how many removes there are between a copy and the original.'

Similarly, in criminal proceedings section 133 of the Criminal Justice Act of 2008 provides:

> 'where a statement in a document is admissible as evidence in criminal proceedings, the statement may be proved by producing either-
>
> (a) the document, or
>
> (b) (whether or not the documents exists) a copy of the document or of the material part of it, authenticated in whatever way the court may approve.'

[282] [2001] EMLR 654.
[283] [2001] 654 at para 85.
[284] Section 8 and section 14 of the Civil Evidence Act; LRCI Consultation Paper 57 (2009) 50.
[285] LRCI Consultation Paper 57 (2009) 54.
[286] LRCI Consultation Paper 57 (2009) 50 and 53.

In the context of evidence in electronic format, the ramifications have been significant.[287] The item of real evidence is the physical product that stores the data (if it does so).[288] However, the physical production of the device only proves that the item exists; the data that has been printed on paper or viewed from a screen has further evidential value.[289] The admissibility of secondary evidence depends largely upon its evidential weight. Thus, proving the integrity of the data will be important, especially where authenticity is in issue.[290] The concept of integrity goes to show that the data has not been altered or corrupted.[291]

3.3.2 The Hearsay Evidence Rule

The hearsay rule states that an assertion other than one made by a person while giving oral evidence in the proceedings is inadmissible as evidence of any fact asserted.[292]

Before the hearsay rule was abolished, the admissibility of electronic documentary evidence was problematic. This rule was a longstanding barrier to admitting documentary evidence.[293] In terms of South African law, a similar problem was highlighted in *Narlis* where statement by a *person* did not include a printout generated by a computer.[294]

In *Myers v DPP* assembly line workers compiled a card, which consisted of the chassis, block and engine numbers, when each car was assembled.[295] These cards were destroyed after they were transferred to microfilm, however the workers responsible for the cards were not identified on the microfilm.[296] Lord Reid stated 'the entries on the cards were assertions by the unidentified men who made them that they had entered numbers that they had seen on cars.'[297] Lord Reid held that the records were inadmissible as did not fall within any of the stated exceptions to hearsay.[298]

---

[287] Mason S (2010) 312.
[288] Mason S (2010) 312.
[289] Mason S (2010) 312.
[290] Mason S (2010) 312.
[291] Mason S (2010) 312.
[292] Tapper C (ed) *Cross & Tapper on Evidence* 8 ed (1995) 46.
[293] LRCI Commission 57 (2009) 147.
[294] 1976 (2) SA 573 (A).
[295] [1965] AC 1001 at 1020.
[296] [1965] AC 1001 at 1020.
[297] [1965] AC 1001 at 1022.
[298] [1965] AC 1001 at 1022.

The UK parliament, adopted an inclusive approach in enacting the Criminal Evidence Act of 1965 in order to reverse the effect of the *Myers* decision.[299] This Act represented the first piece of legislation to address the need to define a 'document' for purposes of hearsay.[300]

The PACE Act was another piece of legislation that dealt with documentary evidence. Section 69 imposed a requirement for the admissibility on any statement, which is produced by a computer.[301] However, a hearsay computer document is not rendered admissible by section 69.[302] In *R v Governor of Pentonville ex parte Osman*, the accused argued that the prosecution had not proved that the computers were operating properly before he took up employment, thus the computer printouts were inadmissible.[303] Lloyd held:

> 'Where a lengthy computer output contains no internal evidence of malfunction, and is retained, e.g. by a bank or a stockbroker as a part of its records, it may be legitimate to infer that the computer which made the record was functioning correctly'.[304]

The nature of the electronic record is an important consideration when dealing with the hearsay rule. In *R v Spiby*, Taylor LJ stated that the distinction is whether the content of the printout can be considered a mere recording of a fact, such as when data are processed by a computer without any human input description, and whether the content of the print has been processed in some way by a human being, in which case it is hearsay.[305]

Mason also notes the following with regards to the hybridisation of evidence:

> 'Records comprising a mix of human input and calculations generated and stored by a computer. An example of that is that of a financial spreadsheet and that contains human statements (input to the spreadsheet program), and computer processing (mathematical calculations performed by the spreadsheet program). From the evidential point of view, the issue is whether the person or the computer created the content of the record, and how much of the content was created by the computer and

[299] LRCI Consultation Paper 57 (2009) 58 and 148; *Gillespie* (1967) 51 Cr App R 172.
[300] LRCI Consultation Paper 57 (2009) 157.
[301] *R v Governor of Brixton Prison and Another, Ex Parte Levin* [1997] AC 741.
[302] [1997] AC 741 at 746; *R v Shepard* (1991) 93 Cr App Rep 139.
[303] [1990] 1 WLR 277 at 306.
[304] [1990] 1 WLR 277 at 306.
[305] [1991] Crim LR 199 CA at 192.

how much by the human. It is possible that the input could be hearsay, and the authenticity of the computer processing might be in issue.'[306]

In *R v Harper,*[307] under section 69 of the PACE Act, the entries were of a hybrid nature. The one accused was charged with handling stolen goods, in this case a stolen card.[308] The prosecution relied upon entries in a lost book, which indicated a batch of cards had been stolen; these entries were transferred to several computers.[309] At trial, the entries were presented by an officer of Inland Revenue, who had not been involved in the transfer and who was not a computer technologist, and thus could not from her own knowledge testify as to the reliability of the computer.[310] On appeal, the court held that the computer printouts did not satisfy section 69 and should not have been admitted.[311]

Steyn J made the following comments:

'The law of evidence must be adapted to the realities of contemporary business practice. Mainframe computers, minicomputers and microcomputers play a pervasive role in our society. Often the only record of a transaction, which nobody can be expected to remember, will be in the memory of a computer. The versatility, power and frequency of use of computer will increase. If computer output cannot relatively readily be used as evidence in criminal cases, much crime (and notably offences involving dishonesty) will in practice be immune from prosecution. On the other hand, computers are not infallible. They do occasionally malfunction. The phenomenon of a 'virus' attacking computer system is also well established. Realistically, therefore, computers must be regarded as imperfect devices.'[312]

The Criminal Justice Act of 1988 regulated documentary evidence for hearsay purposes after the PACE Act. The Act set out exceptions to the hearsay rule when it came to documents coming from unavailable witnesses and business documents.[313] A computer generated document that falls under section 23 and 24 of the Act is rendered admissible.[314]

[306] Mason S (2010) 83.
[307] [1989] 1 WLR 441.
[308] [1989] 1 WLR 441 at 450.
[309] [1989] 1 WLR 441 at 450.
[310] [1989] 1 WLR 441 at 450.
[311] [1989] 1 WLR 441 at 450.
[312] [1989] 1 WLR 441 at 442.
[313] Section 27 of the Criminal Justice Act of 1988; LRCI Consultation Paper 57 (2009) 159.
[314] [1997] AC 741 at 746.

Section 23 allowed for the admissibility of documents that contained first hand hearsay statements, subject to the certain requirements.[315] Section 24 provided for the admissibility of hearsay business documents, once the stipulated conditions are met.[316] Notably, a computer document that has met the conditions under the provision has further hurdle imposed by subsection (3) and (4).[317] In *R v Bedi*, the allegation against the defendants was that they made false sale vouchers using lost and stolen credit cards to defraud credit card companies.[318] The trail judge, in admitting the evidence, failed to assess the purpose for which the lost and stolen card reports were made.[319] On appeal, the court held the reports were not prepared for the purpose of criminal proceedings, but made for the efficient conduct of the bank's credit card business and were, thus, not subject to section 24(4) and admissible.[320]

The Criminal Justice Act of 2003 repealed the provisions relating to hearsay in criminal proceedings.[321] The Act set out conditions of admissibility for certain categories such as where the witness is unavailable,[322] business documents[323] and other common law exceptions[324].

The hearsay rule was abolished by the Civil Evidence Act.[325] Section 1 stipulates 'in civil proceedings evidence shall not be excluded on the ground that it is hearsay.' The effect of section 5 of the Civil Evidence Act was to permit the reception of statements that would be considered hearsay provided certain conditions were met.[326] These safeguards were put in place to regulate the introduction of hearsay evidence that does not fall within the common law exceptions.[327]

[315] Section 23(2) or subsection (3) of the Criminal Justice Act of 1988.
[316] Section 24(1)(i)-(ii) of the Criminal Justice Act of 1988.
[317] Section 24 of the Criminal Justice Act of 1988; *R v Bedi* (1992) 95 Cr App R 21 at 26.
[318] (1992) 95 Cr App R 21 at 23
[319] (1992) 95 Cr App R 21 at 26.
[320] (1992) 95 Cr App R 21 at 27.
[321] Section 114(1) of the Criminal Justice Act of 2003; Mason S (2010) 340.
[322] Section 116 of the Criminal Justice Act of 2003.
[323] Section 117 of the Criminal Justice Act of 2003.
[324] Section 118 of the Criminal Justice Act of 2003.
[325] Section 1(1) of the Criminal Justice Act of 2003; Mason S (2010) 339.
[326] LRCI Consultation Paper 57 (2009) 51.
[327] LRCI Consultation Paper 57 (2009) 113.

Evidence in digital format is (technically) considered to be hearsay evidence, however the emphasis is placed on demonstrating the reliability, integrity and trustworthiness of electronic evidence.[328] The modern view is to admit the evidence and to consider the weight of the evidence, while taking into account the integrity, reliability and trustworthiness.[329] The shift in emphasis means that electronic evidence will be not admissible or will carry little probative value where the reliability, *inter alia,* cannot be established.[330]

3.4 The Evidential Weight

Once the admissibility of the evidence is settled the question of weight, credibility and sufficiency of the evidence is a left for the judge or members of a jury.[331]

A jury determines evidential weight without guidance from the law.[332] There are no fixed rules to determine what weight to give any item of evidence.[333] The court will take into account the surrounding circumstances regarding the creation or transmission of the document and draw any inferences which would suggest anything about the reliability of this.[334] The court will also have regard to whether it would have been reasonable to expect the party adducing the evidence to have called upon the maker of the original to offer testimony.[335] The court will consider the time lag between the original event which the document records and the correlation between this time and when the original document was in fact produced.[336]

With regard to hearsay evidence, section 4 of the Civil Evidence Act states:

> (1) In estimating the weight (if any) to be given to hearsay evidence in civil proceedings the court shall have regard to any circumstances from which any inference can reasonably be drawn as to the reliability or otherwise of the evidence.
>
> (2) Regard may be had, in particular, to the following:

[328] Mason S (2010) 338.
[329] Mason S (2010) 338.
[330] LRCI Consultation Paper 57 (2009) 113.
[331] Mason S (2010) 319.
[332] Pattenden R (2008) 290.
[333] Mason S (2010) 319.
[334] LRCI Consultation Paper 57 (2009) 27.
[335] LRCI Consultation Paper 57 (2009) 27.
[336] LRCI Consultation Paper 57 (2009) 27.

(a) whether it would have been reasonable and practicable for the party by whom the evidence was adduced to have produced the maker of the original statement as a witness;

(b) whether the original statement was made contemporaneously with the occurrence or existence of the matters stated;

(c) whether the evidence involves multiple hearsay;

(d) whether any person involved had any motive to conceal or misrepresent matters;

(e) whether the original statement was an edited account, or was made in collaboration with another or for a particular purpose;

(f) whether the circumstances in which the evidence is adduced as hearsay are such as to suggest an attempt to prevent proper evaluation of its weight.

The English Civil Evidence Act is the only piece of legislation to provide a legal framework for the assessment of hearsay evidence.

3.5 Conclusion

The law in England as it applies to electronic evidence has a different foundation in comparison to South Africa law. In English law an inclusionary approach is adopted which focuses on the evidential weight of electronic evidence. In South African law an exclusionary approach is followed that emphasises the exclusionary rules of evidence.

Furthermore, electronic commerce should not be understood in a vacuum but in light of other international and foreign law. The next chapter will discuss the legal principles that govern the admissibility and evidential weight of electronic evidence in terms of Canadian law.

CHAPTER 4: ELECTRONIC EVIDENCE WITHIN THE CANADIAN LEGAL FRAMEWORK

4.1 Introduction

This chapter will discuss the law regarding the admissibility and evidential weight of electronic evidence in Canada.

Canada has a more segmented jurisdictional structure than other countries.[337] Canada is a federal state and the Constitution divides jurisdiction over legislative matters between the federal government, the governments of the ten provinces and three territories.[338] The federal government has jurisdiction over criminal matters, while jurisdiction over civil and property matters rests with the provinces and territories.[339]

The Canadian law of evidence is largely based on its common law.[340] The common law does not vary between the jurisdictions, however it is supplemented by statues at federal, provincial and territorial levels.[341] Criminal and federal regulatory matters are dealt with under the Canada Evidence Act,[342] while each of the provinces and territories has its own statute dealing with the law of evidence.[343] The Uniform Electronic Evidence Act of 1998 (referred to as the 'Evidence Act') is a model act produced by the Uniform Law Conference of Canada used to draft the electronic record provisions of the other Canadian evidence acts.[344] The Evidence Act deals with electronic evidence, which has been adopted, either completely or in modified form, in nine Canadian jurisdictions.[345]

Canada participated in the preparation of the UNCITRAL Model Law on Electronic Commerce and it has been implemented by the adoption of the Uniform Electronic Commerce Act of 1998 (referred to as the 'Commerce Act') by the Uniform Law Conference

[337] Currie RJ and Coughlan S 'Canada' in Mason S (ed) *Electronic Evidence* 2 ed (2010) 265.
[338] Currie RJ & Coughlan S (2010) 265.
[339] Currie RJ & Coughlan S (2010) 265.
[340] Gregory JD 'Canadian Electronic Commerce Legislation' (2002) 17 *BFLR* 327.
[341] Gregory JD (2002) 327.
[342] RSC 1985.
[343] Currie RJ & Coughlan S (2010) 266. For example, the Ontario Evidence Act RSO 1990, the Nova Scotia Evidence Act RSNS 1989 and the Alberta Evidence Act RSA 2000.
[344] Chasse K 'The Admissibility of Electronic Business Records' (2010) 8 *CANJTL* 105 at 106.
[345] Currie RJ & Coughlan S (2010) 270.

of Canada.[346] The Commerce Act was enacted to attain legal certainty in respect of electronic communications and electronic records.[347] The Commerce Act applies not only applies to commercial transactions, but to all rules of law that are not excluded from it.[348] The Act does not limit the operation of any provision of law that expressly authorizes, prohibits or regulates the use of electronic documents.[349] The Act contains common exclusions of documents in electronic format such as wills, testamentary trusts, power of attorney (in respect of health or financial affairs) and land transfers.[350] The rationale behind the exclusion is not that such documents should not be created electronically, but these documents require detailed rules, which safeguards the relevant parties.[351] The approach adopted by the Commerce Act is similar to the ECT Act in terms of South African law.

4.2 The Rules of Admissibility for Evidence

In the Canadian law of evidence, the judge (trier of law) decides whether an item of evidence offered by a party is admissible.[352] For evidence to be admitted, it must be relevant to a fact that is material.[353] The item of evidence must have a tendency to make the existence of a fact more of less probable and that fact must be at issue in the case.[354] Canada has a low threshold for the admissibility of evidence, and focus is seemingly rather on the quality of the evidence, which is dealt with under the evidential weight of the item.[355]

Beyond the basic relevance threshold, Canadian evidence law contains all of the traditional canons of exclusion, such as hearsay and the best evidence rule.[356] The Evidence Act does not modify the common law or any statutory rule relating to the admissibility of electronic records.[357] For example, the admissibility of an electronic record may be subject to the hearsay rule, which is not changed by the Act.[358]

---

[346] Gregory JD (2002) 277.
[347] Gregory JD (2002) 283.
[348] Gregory JD (2002) 283.
[349] Section 2(5) of the Uniform Electronic Commerce Act.
[350] Section 2(3) of the Uniform Electronic Commerce Act.
[351] Gregory JD (2002) 284.
[352] Currie RJ & Coughlan S (2010) 267.
[353] Currie RJ & Coughlan S (2010) 267.
[354] Currie RJ & Coughlan S (2010) 267.
[355] Currie RJ & Coughlan S (2010) 267.
[356] Currie RJ & Coughlan S (2010) 268.
[357] Section 2(1) of the Uniform Electronic Evidence Act. Note the rules relating to authentication and the best evidence rule are modified.
[358] Uniform Law Conference of Canada Commentary on the Uniform Electronic Evidence Act of 1998 available at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2 (accessed 15 August 2012).

The Canadian approach to electronic evidence is to treat it in some aspects as a new form of evidence, but also as traditional documentary evidence.[359] In the past, Canadian courts have treated records that contain computer-generated information in the same fashion as documentary evidence.[360] In terms of South African law, the courts follow a common sense approach whereby electronic evidence may be treated as real evidence or documentary evidence.

Electronic documents can be electronic versions of a paper document, for example a scanned document, or a printout of data generated on computer.[361] In light of this, the Evidence Act broadly defines 'electronic record' as data[362] that is recorded or stored on any medium, computer system or other similar device that can be read or perceived by a person, computer system or other similar device, which includes 'a display, print-out[363] or other output of that data'.[364]

The rules relating to the admissibility of electronic evidence are determined by the nature of the evidence. For instance, electronic information may be categorised as real or documentary evidence, and in each category different evidentiary rules apply. Electronic information may constitute real evidence when the data is captured automatically without human intervention.[365] On the other hand, if the electronic information is created by a human entering the data, it should be treated as documentary evidence.[366] However, it is possible that electronic information or data can be categorised as both real and documentary evidence. This classification of electronic evidence is analogous with common sense adopted in *Ndiki*. In *Saturley v CIBC World Markets Inc*., the court commented:

> '… if electronic information does not meet the criteria for admission as real evidence, it may still be admitted if it satisfies the requirements for admission of documentary evidence. It is possible that a given item of electronic information may have aspects of both real and documentary evidence. For example, an e-mail in electronic form will include electronic data identifying the computer on which it was created and when it

[359] Currie RJ & Coughlan S (2010) 269.
[360] Underwood G & Penner J (2010) 12.
[361] Currie RJ & Coughlan S (2010) 270.
[362] Section 1(a) of the Uniform Electronic Evidence Act defines 'data' as representations, in any form, of information or concepts.
[363] Except an original paper print-out in terms of section 4(2).
[364] Section 1(b) of the Uniform Electronic Evidence Act.
[365] Underwood G & Penner J *Electronic Evidence in Canada* 2 ed (2010) 12.
[366] Underwood G & Penner J (2010) 12.

was sent. That information is added automatically by the computer software and would likely constitute real evidence. If the content of the e-mail is being introduced for its truth, it would be considered a document and subject to admissibility as such.'[367]

The court identified a further category of electronic evidence which consists of a hybrid of real and electronic evidence. The requirements that govern the admissibility of this category of electronic will ultimately depend on the purpose for which the evidence is adduced.

4.2.1 Real Evidence

Real evidence covers objects which are immediately relevant to the case, for example a personal computer, but there are more specialised forms of real evidence such as electronic documents.[368]

Computer generated records may be accepted as real evidence has received some judicial support.[369] In *R v McCulloch* the court stated that:

> 'Where evidence is automatically recorded by any means, other than by human labour, and the evidence so recorded can be reproduced in any form, intelligible to the human mind, the reproduction is admissible as real evidence. The recording may be mechanical, chemical, electronic, photographic, or auditory, to name a few examples, and the reproduction (sic) may be by computer printout, audiovisual playback, photographs, or other means. The weight to be attached to such evidence will depend on the accuracy and integrity of the process employed.'[370]

In this case the admissibility of the data generated from a tracing apparatus installed on a customer's telephone line was at issue.[371] The court found that the printouts of the tracing apparatus were admissible as real evidence because of the automatic nature of the recording.[372]

[367] (2012) CarswellNS 420 at para 28.
[368] Currie RJ & Coughlan S (2010) 267.
[369] *R v Smeland* (1995) 54 BCAC 49; *R v Hall* [1998] BCJ 2515.
[370] 1992 CarswellBC 2586 at para 18.
[371] 1992 CarswellBC 2586 at para 2-4.
[372] 1992 CarswellBC 2586 at para 19.

In *Saturley v CIBC World Markets Inc.*, the defendant produced volumes of trading records, which contains details of all trades in equities and options entered by the plaintiff, in electronic form and hard copy.[373] The defendant argued that the records should be admitted as real evidence.[374] The court stated:

> 'The first step in the admissibility analysis is to determine whether the party offering the evidence can establish on a balance of probabilities that it fits within the parameters of real evidence as discussed above. That means, it must be data collected automatically by a computer system without human intervention. It appears that this could include a threshold consideration of reliability; however, it is important to remember that reliability is primarily an issue that goes to the weight to be given the evidence and not its admissibility.'[375]

Once electronic evidence meets the criteria for admission as real evidence, the court stipulated that:

> '[I]t is still necessary to consider whether the specific evidence before the court represents the electronic information. This may be accomplished by having a witness testify that the paper copy was printed from the original source … . If the information comes before the court in electronic form, it will be necessary to have a witness confirm that it comes from the original source. It may also be necessary to have evidence concerning the custody and protection of that information from the original source to the court, particularly if it is transferred to a number of different media.'[376]

The court held that the trading records, which represented the data of the equities program, are admissible as real evidence.[377]

Electronic information that constitutes real evidence simply needs to be authenticated and the trier of fact, a jury, will then draw their own inferences from it.[378]

4.2.2 Documentary Evidence

[373] (2012) CarswellNS 420 at para 4.
[374] (2012) CarswellNS 420 at para 8.
[375] (2012) CarswellNS 420 at para 8.
[376] (2012) CarswellNS 420 at para 7.
[377] (2012) CarswellNS 420 at para 64.
[378] (2012) CarswellNS 420 at para 11.

As indicated, a document is defined as 'any written thing capable of being evidence' in terms of English common law.[379]

The Commerce Act covers documents in electronic form by creating functional equivalence to paper documents.[380] The basic form of the rule in the Commerce Act is, 'where the law requires [paper] that requirement may be satisfied by an electronic record [if certain standards are met]'.[381] While it can also be treated as real evidence, most kinds of electronic data is submitted in a documentary form.[382]

Electronic information that is classified as documentary evidence is subject to a number of evidentiary requirements, for example the best evidence rule, which may require the production of an 'original' of the document or that the document be otherwise authenticated.[383]

Original

Section 11(1) of the Commerce Act makes an electronic document function as an original if the following conditions are met:

> '11(1)(*a*) there exists a reliable assurance as to the integrity of the information contained in the electronic document from the time the document to be presented or retained was first made in its final form, whether as a paper document or as an electronic document;
>
> (*b*) where the document in original form is to be provided to a person, the electronic document that is provided to the person is accessible by the person and capable of being retained by the person so as to be usable for subsequent reference;

Read with section 11(2) and (3):

> '11(2) For the purpose of paragraph (1)(*a*),(*a*) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the

[379] *R v Daye* [1908] 2 KB 333 at 340.
[380] Gregory JD (2002) 289.
[381] Gregory JD (2002) 290.
[382] Currie RJ & Coughlan S (2010) 269.
[383] (2012) CarswellNS 420 at para 12.

introduction of any changes that arise in the normal course of communication, storage and display;

(*b*) the standard of reliability required shall be assessed in the light of the purpose for which the document was made and in the light of all the circumstances.

(3) For the purposes of paragraph (1)(b), an electronic document is deemed not to be capable of being retained if the person providing the electronic document inhibits the printing or storage of the electronic document by the recipient.'

These standards are similar to those in terms of section 4 of the Evidence Act in order to satisfy the best evidence rule. In comparison to South African law, section 11(2)(a) of the Commerce Act is similar to section 15(3)(a) of the ECT Act, which states that consideration must be given to 'the reliability of manner in which the integrity of the data message was maintained'. Similarly, it is important that the information contained in a data message remains complete and unaltered.

Authentication

In the law of evidence, a document must be authenticated before it can be admitted.[384] There must be evidence show that demonstrates the document is what it is purported to be.[385]

The Evidence Act confirms the application of the common law on authentication.[386] The Act states that electronic records must be authenticated by providing 'evidence capable of supporting a finding that the electronic record is what the person claims it to be'.[387] Given the wording of the section, it should be interpreted as a strict evidential burden.[388] The evidence need only support such a finding, and does not have to prove the document *is* what it purports to be, for example the electronic record is a receipt.[389]

The authentication rule poses the following questions: 'What is the record? Where or who does it come from? Has the content been altered, either intentionally or unintentionally?'[390]

[384] Gregory JD (2002) 331.
[385] Currie RJ & Coughlan S (2010) 270.
[386] Currie RJ & Coughlan S (2010) 272.
[387] Section 3 of the Uniform Electronic Evidence Act.
[388] Currie RJ & Coughlan S (2010) 271.
[389] Gregory JD (2002) 331.
[390] Gregory JD 'Authentication Rules and Electronic Records' (2002) 81 *Can Bar Rev* 529 at 531.

Chasse submits that the American authentication rule serves a greater purpose.[391] Rule 901(a) of the Federal Rules of Evidence state:

> 'The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that a matter in question is what its proponent claims.'

The American authentication rule establishes, *prima facie*, the admissibility of the record.[392] This rule requires proof that the record contains authentic evidence of what it purports to prove.[393] In Canadian law the authentication rule is applied to a lesser extent as it only establishes who has the burden of proof;[394] it does not provide an initial assessment of the integrity of the record.[395] The integrity of the electronic record will only be tested, after the evidence was admitted, in terms of the best evidence rule, the hearsay evidence rule or at the determination of its evidential weight.[396]

4.3 The Exclusionary Rules of Evidence

4.3.1 The Best Evidence Rule

In regard to documentary evidence, the court generally wants to see an original document, or have a good explanation of why the original is not available.[397] The best evidence rule compelled a party to demonstrate the integrity of a document by either providing the original or demonstrating a copy was sufficiently trustworthy for use by the court.[398]

It is important to note that a document can be a printout, which serves as a display output of what is contained on the computer.[399] A document can also be created on a computer but what is always used is the document in paper form, such as business correspondence.[400] Section 4(2) of the Evidence Act allows for such a record to be treated as a paper record and would be the original for purposes of the best evidence rule.[401] In *R v Bell* the printouts of

[391] Chasse K (2010) 131.
[392] Chasse K (2010) 132.
[393] Chasse K (2010) 173.
[394] Chasse K (2010) 132.
[395] Chasse K (2010) 173.
[396] Gregory JD (2002) 331.
[397] Gregory JD (2002) 331.
[398] Currie RJ & Coughlan S (2010) 271.
[399] Gregory JD (2002) 336.
[400] Gregory JD (2002) 336.
[401] ULCC Commentary on the Evidence Act.

bank ledgers were held to be 'original' were the computer records had been erased, for the bank relied on paper records in practice.[402]

The Evidence Act states where the best evidence rule is applicable in respect of an electronic record, it is satisfied on the proof of integrity of the electronic records system[403] in or by which the data was recorded or stored.[404]

Chasse submits that the best evidence rule should indicate that accurate records, regardless of form, can be introduced into evidence, and that the best evidence will be the result of a trustworthy process or system used to produce the records.[405] Chasse argues that the best evidence rule is dead; any doubts regarding an electronic record should not be categorized as a best evidence rule issue, but the focus should be placed on the integrity of the electronic record system.[406]

This rule becomes problematic when applied to electronic documents. In many instances, electronic documents cannot be traced down to an 'original', especially in a network environment.[407] Furthermore, the original is not necessarily more reliable than the copy.[408]

The Evidence Act focuses on replacing originality with proof of integrity of the electronic storage system (and not the individual record) by using standards.[409] Note, the integrity of the electronic storage system is not a guarantee of the integrity of the individual electronic record, but it supports the integrity to the degree of admissibility.[410] The electronic storage system that produced an electronic record will often include procedures for creation, storage, including access controls, security features, verification rules and retention or destruction schedules.[411] The integrity is usually proven by an affidavit[412], and expert evidence may be required depending on the nature of the technology.[413]

---

[402] (1982) 65 CCC (2d) 377.
[403] Section 1(c) states an 'electronic storage system' includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and storage of electronic records.
[404] Section 4(1) of the Uniform Electronic Evidence Act.
[405] Chasse K (2010) 114.
[406] Chasse K (2010) 115-166, 138-139.
[407] Currie RJ & Coughlan S (2010) 271; Gregory JD (2002) 297.
[408] Currie RJ & Coughlan S (2010) 271; Gregory JD (2002) 297.
[409] ULCC Commentary on the Evidence Act.
[410] Gregory JD (2002) 333.
[411] ULCC Commentary on the Evidence Act.

Section 5 of the Evidence Act contains several presumptions in favour of the integrity[414] of an electronic records system namely, that the electronic storage system was operating properly at all material times,[415] proof that the document was recorded or stored by an adverse party,[416] or proof that the document was recorded or stored in the ordinary course of business by a party outside litigation.[417]

The Evidence Act provides that the court may consider the standards of the electronic record system for purposes of assessing the integrity of the system.[418] Section 6 states that 'evidence may be presented in respect of any standard, procedure, usage or practice' on how electronic records are to be recorded or stored, having regard to the type of business and the nature and purpose of the electronic record.

Evidence regarding the standards of the electronic record system is used to create or to rebut a presumption in terms of section 5.[419] However, the standards of the electronic record system can also provide proof of the integrity of the electronic document system, which is relevant to the question of admissibility (subject to arguments of evidential weight).[420] For example, industry standards such as the *Standards on Electronic Records as Documentary Evidence* generated by the Canadian General Standards Board[421] is not binding on the court, but will have persuasive value.[422] The adherence of an electronic record system to recognised standards is relevant, and not compulsory, to the admissibility of the electronic record, for example a business may have other agreements on the rules regarding electronic communication.[423]

4.3.2 The Hearsay Evidence Rule

---

[412] Section 7 of the Uniform Electronic Evidence Act.
[413] Currie RJ & Coughlan S (2010) 271.
[414] As required by section 4 to satisfy the best evidence rule.
[415] Section 5(a) of the Uniform Electronic Evidence Act.
[416] Section 5(b) of the Uniform Electronic Evidence Act.
[417] Section 5(c) of the Uniform Electronic Evidence Act.
[418] Section 6 of the Uniform Electronic Evidence Act.
[419] Gregory JD (2002) 335.
[420] Currie RJ & Coughlan S (2010) 272.
[421] CAN/CGSB 72.34-2005 (1 December 2005).
[422] Currie RJ & Coughlan S (2010) 272.
[423] ULCC Commentary on the Evidence Act.

Documents that are adduced for the truth of their contents may be classified as hearsay.[424] The difficulties of defining hearsay have been noted by the courts.[425] The recent definitions of hearsay focus on the absence of an opportunity to cross-examination the declarant in regard to the truth of the statement.[426]

It is generally accepted that there are no special problems for the admission of electronic records, for the medium on which indirect evidence is stored does not alter the characteristics of that evidence as hearsay.[427] The common law rules as set out in *Ares v Venner,*[428] a *locus classicus* on documentary evidence in Canada, could be applied to electronic documents.[429] A hearsay document must be sufficiently reliable and necessary under the common law.[430]

In terms of the Evidence Act, electronic documents must still satisfy other applicable rules of evidence, such as the hearsay evidence rule, in order to be admitted.[431] The hearsay rule in terms of Canadian law requires that the hearsay evidence must be 'necessary' and 'reliable' for the evidence to be admissible, if it does not fall under the exceptions.[432]

The necessary requirement can be satisfied by demonstrating the need to preserve information beyond human capacity.[433] In *R v Khelawon* the court found that the hearsay evidence rule, due to the massive amounts of electronic records, was necessary for the purposes efficiency.[434] The central concern is testing the reliability of the declarant's assertion.[435] For information in electronic form to satisfy the requirement of reliability is problematic due to its transience and malleability.[436] Evidence regarding the integrity of the document's storage system will help in deciding whether the document is a 'reliable' source of evidence for hearsay purposes.[437]

[424] Currie RJ & Coughlan S (2010) 270.
[425] *R v Abbey* [1982] 2 SCR 24 at 40-41.
[426] *R v Starr* [2000] 2 SCR 144 at para 159.
[427] Gregory JD (2002) 328.
[428] [1970] SCR 608.
[429] Gregory JD (2002) 329.
[430] [1970] SCR 608.
[431] Section 2(1) of the Uniform Electronic Evidence Act; Currie RJ & Coughlan S (2010) 272.
[432] Currie RJ & Coughlan S (2010) 272.
[433] Gregory JD (2002) 330.
[434] *R v Khelawon* [2006] SCC 57 at para 35.
[435] *R v Khelawon* [2006] SCC 57 at para 35.
[436] Gregory JD (2002) 329.
[437] Gregory JD (2002) 329.

4.3.2.1 The Exceptions to the Hearsay Evidence Rule

The Evidence Act, as indicated, does not change any common law or statutory rules relating to the admissibility of records.[438] The admission of a record may be subject to the hearsay rule and its exceptions, such as the business records rule.[439]

The English decision of *Myers v DPP* had the effect that records could not be admitted under the business record exception because an anonymous worker could not be proven dead.[440] The UK consequently enacted legislation to address this matter.[441] However, in the *Ares* case the Supreme Court of Canada disagreed with this approach and extended the business record exception to the hearsay rule.[442] Hall J states that:

> '[h]ospital records, including nurses' notes, made contemporaneously by someone having a personal knowledge of the matters then being recorded and under a duty to make the entry or record should be received in evidence as prima facie proof of the facts stated therein This should, in no way, preclude a party wishing to challenge the accuracy of the records or entries from doing so.'[443]

In *R v Hall* the accused were charged with theft of telecommunication services using ghost accounts.[444] The court had to decide the admissibility of computer generated billing records for the various telephone accounts.[445] The court stated, in regard to the necessity requirement, that the issue of vast pools of data generated by nameless computers makes the admission of such records necessary in a modern age.[446] The court found that the records satisfied the reliability requirement insofar as records in the usual and ordinary course of business provide some circumstantial guarantee of trustworthiness, and was admitted under common law.[447] The court noted, '[a]s common experience and the evidence above show, even computers are subject to error. These problems, however, go to weight rather than admissibility'.[448]

[438] Section 2(1) of the Uniform Electronic Evidence Act.
[439] ULCC Commentary on the Evidence Act.
[440] [1965] AC 1001 at 1036 (per Lord Peace dissenting); Discussed above at 3.3.2.
[441] Criminal Evidence Act of 1965.
[442] [1970] SCR 608; Chasse K (2010) 106.
[443] 1970] SCR 608.
[444] 1998 CarswellBC 2139 at para 1.
[445] 1998 CarswellBC 2139 at para 29.
[446] 1998 CarswellBC 2139 at para 56.
[447] 1998 CarswellBC 2139 at para 65.
[448] 1998 CarswellBC 2139 at para 64.

Section 5(c) of the Evidence Act, as indicated, contains a presumption in favour of the integrity of a document was recorded or stored in the ordinary course of business by a party outside litigation. This provision also serves the purposes for the bank record exception, for example as contained in section 29 of the Canada Evidence Act.[449]

Most electronic business records are a product of usual and ordinary business activities.[450] Consequently, almost any electronic business record can satisfy the business record exception without the need to adduce proof in regard to the integrity of the electronic record system.[451] The only protection against electronic business records that lack integrity is the assessment of evidential weight.[452] This is in accordance with the Canadian approach in regard to the admission of evidence.

4.4 The Evidential Weight

The jury (trier of fact) determines with the evidential weight of an item of evidence, which is admitted.[453] Weighing involves the members of a jury to scrutinise the evidence, deciding which parts to accepted and which to reject, in order to arrive at a decision as to what the facts of the case were, and whether one party or the other has proven its case in accordance with the applicable burden and standard of proof.[454]

The assessment of the evidential weight of an electronic record goes primarily to the reliability of an electronic record system.[455] In *R v McCulloch*, the court briefly stated that the evidential weight of the tracing apparatus depends on the accuracy and integrity of the process employed in the recording of the information.[456] Thus, a computer record will not carry much evidential weight if the computer system, in question, was fraught with errors.

4.5 Conclusion

Canada has a similar foundation in regard to the law that regulates electronic evidence as South Africa. It is important to note the manner in which Canada and South Africa has adopted legislation to ratify the Model Law.

---

[449] ULCC Commentary on the Evidence Act.
[450] Chasse K (2010) 136.
[451] Chasse K (2010) 136.
[452] Chasse K (2010) 136.
[453] Currie RJ & Coughlan S (2010) 267.
[454] Currie RJ & Coughlan S (2010) 267.
[455] (2012) CarswellNS 420 at para 22.
[456] 1992 CarswellBC 2586 at para 18.

The next chapter will briefly summarise and compare how electronic evidence is treated in England, Canada and South Africa. It is important to take note of these different approaches to electronic evidence in order to make possible recommendations with regard to the current South African law.

CHAPTER 5: RECOMMENDATIONS AND CONCLUSION

5.1 Introduction

This chapter will briefly compare the legal rule that relate to the admissibility and evidential weight of electronic evidence in Canada, England and South Africa, and will make recommendations in light of South African law.

5.2 Recommendations

5.2.1 The Rules of Admissibility for Evidence

Canada generally has a low threshold for the admissibility of evidence and issues of reliability of the evidence will go to the weight.[457] The courts have adopted an inclusionary approach to the law of evidence in order to replace formal categorisation with principled[458] flexibility.[459]

The admissibility of electronic evidence is regulated by the Uniform Electronic Evidence Act and the Uniform Electronic Commerce Act. The Evidence Act provides for the legal recognition of electronic records. Notably, the common law is still applicable to the admissibility of electronic evidence. The Canadian courts have found that electronic records may be categorised as real or documentary evidence.[460]

In terms of English law, the modern view is to admit evidence and, rather, to focus on the evidential weight.[461] Similarly, the question of weight, sufficiency and credibility of the evidence are decisions for the jury or the judge (where a case is tried without a jury) during the assessment of evidential weight.[462]

In England there is not one piece of dedicated legislation dealing with electronic evidence and commerce. The Civil Evidence Act and Criminal Justice Act, *inter alia*, regulate electronic evidence that can be assimilated to documentary evidence and electronic real evidence is mostly dealt in terms of the common law. The English courts also distinguish between two categories of electronic evidence, namely real evidence and documentary

[457] Currie RJ & Coughlan S (2010) 267.
[458] Currie RJ & Coughlan S (2010) 268. This principled approach is summarised by the phrase 'evidence may be excluded where its probative value is outweighed by its prejudicial effect'.
[459] Currie RJ & Coughlan S (2010) 268. See *R v Corbett* [1988] 1 SCR 670.
[460] *Saturley v CIBC World Markets Inc.* (2012) CarswellNS 420.
[461] Tapper C (1995) 72.
[462] Mason S (2010) 319.

evidence.[463] The submission of secondary evidence[464] has always been the norm for electronic evidence.[465] The admissibility of secondary evidence is dependent upon its evidential weight.[466] For instance, electronic evidence will be excluded when the probative value is outweighed by its prejudicial effect.[467]

South African law takes an exclusionary approach to the law of evidence.[468] Electronic evidence must be relevant, not excluded by an exclusionary rule and its value should not be outweighed by the prejudice.[469]

The ECT Act provides for the legal recognition of data messages, which is to not deny the admissibility of electronic evidence on the mere ground that it is constituted by a data message. However, it may be denied on other grounds as found, for example in the common law.[470] Thus, electronic evidence is regulated in terms of the ECT Act and the common law.

The definition of a data message in the ECT Act differs from the Model Law[471] by substituting its own examples.[472] The recording of a voice outside an automated transaction is excluded and would make it problematic for anyone doing business via voice to comply with legislation that required a written record of the transaction.[473] The aim of the Model Law is to encompass all types of messages that are generated, stored or communicated in a paperless form. The Canadian Uniform Electronic Evidence Act includes voice mail as an electronic record,[474] since the information has been stored. It has been submitted that the ECT Act should include such voice transactions as a data message, which is the equivalent of documentary evidence, but must require that the voice transaction be recorded and authenticated.

[463] *R v Spiby* (1990) 91 Cr App R 186.
[464] Discussed above in 3.2.2.
[465] Mason S (2010) 312.
[466] Mason S (2010) 316.
[467] *R v Fowden and White* [1982] Crim LR 588.
[468] Hofman J (2010) 675.
[469] Hofman J (2010) 675.
[470] Hofman J (2010) 682.
[471] Article 2 of the UNCITRAL Model Law on Electronic Commerce with Guide to the Enactment 1996.
[472] Hofman J (2010) 680.
[473] Hofman J (2010) 680. The ECT Act would override section 3 of the Interpretation Act which included voice in the definition of writing.
[474] A 'message' includes the notion of a 'record'. See UNCITRAL Model Law on Electronic Commerce with Guide to the Enactment 1996 para 30.

The South African courts found that section 15 distinguishes between data message that amount to real and documentary evidence.[475] Similarly, the English and Canadian courts acknowledge the importance of this distinction as stated by Van Zyl J in *Ndiki*:

> 'The distinction plays an important role in approach, for example real evidence should not be tested under the hearsay rule, as it does not seek to prove the truth of any contents merely to prove that an object exists.'

A suggestion was made that the admissibility of data messages should be regarded as *sui generis,* in other words neither traditional evidentiary principles that are applicable to documentary or real evidence should govern data messages, is unsupported.[476] Hofman states that differential treatment between information in electronic and written format will either result in discriminating against those transacting in electronically or provide an unfair advantage.[477] Electronic evidence should be treated on the basis of functional equivalence in order to prevent 'format shopping'.[478] The distinction between electronic evidence based on functional equivalence should be maintained to ensure that the legal principles address those issues which are unique to particular category of evidence.

5.2.1.1 Real Evidence

The Canadian courts have accepted that computer generated evidence can be treated as real evidence.[479] Electronic records are introduced as real evidence where it consists of data which is captured automatically without human intervention.[480] Because the information that is captured is recorded automatically it does not have to fall under any exception to the hearsay rule.[481]

The Evidence Act does not alter the existing law relating to authentication.[482] The common law rules relating to authentication was codified in terms of the Act. Therefore, electronic

[475] *S v Ndiki and Others* [2007] 2 All SA 185 (Ck).
[476] Watney (2009) 11.
[477] Hofman (2010) 679.
[478] Defined as '… converting hard copy evidence to electronic evidence and destroying originals or presenting a hardy copy version and destroying the electronic version in order to take advantage of differences in the law of evidence that applies to each.' See Hofman J (2010) 679.
[479] 1992 CarswellBC 2586 at para 18.
[480] Underwood G & Penner J (2010) 12.
[481] Underwood G & Penner J (2010) 12.
[482] Section 2(1) of the Uniform Electronic Evidence Act of 1998.

records that constitute real evidence have to be authenticated and evidence should be adduced that supports a finding that it claims what it purports to be.[483]

Under English law real evidence is described as 'material objects other than documents, produced for inspection of the court'.[484] 'Evidence derived from a computer constitutes real evidence when it is used circumstantially rather than testimonially, that is to say that the fact that it takes one form rather than another is what makes it relevant, rather than the truth of some assertion which it contains.'[485] The English courts have accepted that when data is processed by a computer without any human input of any description it amounts to real evidence.[486]

If there is no consensus as to the authenticity of the evidence, there must be some admissible evidence of provenance and integrity.[487]

South African law states that real evidence consists of things which are examined by the court as means of proof upon proper identification and becomes evidence of itself.[488] Real evidence is seemingly mostly seen to be graphics, audio or video, but as technology develops real evidence may now include computer programs and data. Word processing documents, emails, cache and cellphone applications are examples of the latter.

Real evidence in the form of graphics, audio or video in electronic format should be produced,[489] be original[490] in a proper form and be authenticated to guard against any alterations.[491] In regard to computer programs, a logical approach must be adopted, which is to ask what the computer program is used for to establish and to treat it accordingly.[492] For instance, a computer program that is produced to show how it operates is treated as the functional equivalent of a piece of equipment.[493] The courts have accepted computer-

[483] Section 3 of the Uniform Electronic Evidence Act of 1998.
[484] Mason (2010) 302.
[485] Tapper C *Computer Law* 4 ed (1989) 373.
[486] *R v Spiby* (1990) 91 Cr App R 186 at 191.
[487] Pattenden R (2008) 280.
[488] *S v M* 2002 (2) SACR 411 (SCA) at para 31.
[489] Section 17 of the Electronic Communications and Transactions Act.
[490] Section 14 and section 15(1)(b) of the Electronic Communications and Transactions Act.
[491] Zeffert DT, Paizes A and Skeen A St Q (2003) 704-706.
[492] Hofman J (2010) 690.
[493] Hofman J (2010) 690.

generated data as real evidence when the data was generated without the assistance of a human agency.[494]

In all the evaluated countries, the courts view electronic real evidence as mechanical evidence without human intervention or evidence used to prove that an object exists. Collier notes that all computer-generated data contains human intervention at some level,[495] however emphasis should be placed on whether or not the computer requires human input during the operation of the computer in order to produce the data.

With regard to the authentication of electronic evidence, the ECT Act should codify the common law rules of authentication, similar to the Canadian Uniform Electronic Evidence Act, and real evidence in electronic format should in addition to proper identification be authenticated.

The Canadian Uniform Electronic Evidence Act does not provide for the assessment of the integrity of an electronic record system under authentication.[496] The integrity of an electronic record system is only considered in terms of the exclusionary rules, such as the hearsay evidence rule, which are mostly applicable to documentary evidence. Thus, an electronic record, which is the functional equivalent of real evidence, will not have the integrity of its system assessed.

The ECT Act should adapt the principle of authentication to include a systems integrity test in regard to data messages in the form of real evidence to ensure that evidence is properly authenticated. The factors that may be taken into account to establish the integrity is the nature of the system, for example proving the reliability of a server will differ from that of a personal computer.[497] Whether the integrity of the system responsible for the data message is established will depends on the facts of each case.

The South African Law Reform Commission has also considered the introduction of a presumption of regularity, as expressed in *Castle v Cross* by Brown LJ as 'in the absence of evidence to the contrary, the courts will presume the mechanical instruments were in order at material time'.[498] In English law, section of 129 (2) of the Criminal Justice Act of 2003 contains such a presumption that 'the mechanical device has been properly set or calibrated'.

[494] [1998] 1 All SA 319 (W) at 327.
[495] Collier D (2005) 6.
[496] The ULCC felt the question of integrity should only be dealt with once.
[497] Mason S (2010) 106.
[498] [1984] 1 WLR 1372 (QBD); SALRC Issue Paper 27 (2010) 47.

However, there can be no value in requiring evidence that a computer, communications device or network was in order at the material times.[499] There is no evidence against the presumption that software is notorious for being subject to defects.[500] Secondly, the party seeking to rebut the presumption will rarely be in the position to substantiate the claims, because most of the evidence will be in the opposing party who is in control of the computer system.[501]

A presumption of regularity would be problematic if data messages are merely admitted, because it was too onerous on the opposing party to rebut. Generally, the integrity of system responsible for the data messages should be established by the party relying on the data message.

5.2.1.2 Documentary Evidence

In Canadian law, a document is broadly defined as 'any written thing capable of being evidence', which can include electronic documents.[502] The Uniform Electronic Evidence Act states that paper records produced directly by a computer system, such as printouts, constitute electronic records.[503] The courts have considered electronic records as documentary evidence for purposes of admissibility, when the information contained in the records has filtered through a human author and it is offered for the truth of its contents.[504] Electronic records that are the functional equivalent of documents are subject to exclusionary rules, such as the hearsay rule.[505]

The common law principle of authentication[506] requires that 'documents be authenticated before it can be used as evidence'. The Uniform Electronic Evidence Act codified this principle, which requires evidence capable to support a finding that the electronic record is

[499] Mason S (2010) 131.
[500] Mason S (2010) 131.
[501] Mason S (2010) 132.
[502] *R v Daye* [1908] 2 KB 333 at 340; Discussed above in 3.2.3 and 4.2.3.
[503] Section 1(b) of the Uniform Electronic Evidence Act. The Uniform Electronic Commerce Act also treats electronic records as the functional equivalent of documentary evidence.
[504] See *Saturley v CIBC World Markets Inc.* (2012) CarswellNS 420.
[505] Underwood G & Penner J (2010) 12.
[506] [T]his is the capacity to prove that the digital object is what it purports to be. The authenticity of a digital object is preserved by the use of techniques to prevent the data from being manipulated, altered or falsified deliberately or inadvertently. Such methods include providing audit trails of transmissions and maintaining records of encryption. A number of attributes, taken together, provide evidence of authenticity: the mode, stature and form of transmission, together with the way in which the data is preserved and how it is managed.' See Mason S (2010) 101.

what the person it claims to be.[507] At the authentication stage it is not concerned with the integrity of the electronic record system.[508]

As indicated, a 'document' is also widely defined in terms of the English common law. The Criminal Justice Act and the Civil Evidence Act has adopted a non-prescriptive definition to include documents in electronic format, which provides for 'anything in which information of any description is recorded'.[509] Computer-generated printouts are considered a form of documentary evidence when it proves the truth of its content.[510]

English law requires that document must be authenticated.[511] There are no special rules for the authentication of computer-generated documents.[512] The Criminal Justice Act and the Civil Evidence Act leaves it up to judicial discretion how to authenticate the document.[513] Mason has suggested that reference will not be made to the standards of the computer system in question, but rather the testimony digital specialist.[514]

In South African law a document is also broadly defined as 'everything that contains written or pictorial proof of something [and] it does not matter of what material it is made'.[515]

In South African law a document must be authenticated before it can be admitted as evidence, in other words it must be shown that the document is what it claims to be.[516] The Electronic Communications and Transactions Act do not exclude the common law rule of authentication.[517] The authenticity of a data messages can be established by the person responsible for the data message, unless the data message was made by a person in ordinary course of business.[518]

The South African Law Reform Commission questioned if the review of the principle of authentication is necessary in view of the nature of electronic evidence that raise legitimate

[507] Discussed in 4.2.3.
[508] ULCC commentary on the Uniform Electronic Evidence Act.
[509] Section 134 of the Criminal Justice Act of 2003; Section 13 of the Civil Evidence Act of 1995; Law Reform Commission of Ireland Consultation Paper 57 *Documentary and Electronic Evidence* (2009) 12.
[510] Mason S (2010) 308. See *R (on the application of O) v Coventry Justices* [2004] EWHC 905.
[511] Pattenden R (2008) 293.
[512] Pattenden R (2008) 297.
[513] Section 8(1)(b) of the Civil Evidence Act and section 133(b) of the Criminal Justice Act.
[514] Mason S (2010) 86.
[515] *Seccombe v Attorney-General* 2002 (2) All SA 185 (Ck) 270 at 277; Schwikkard & van der Merwe (2009) 404; Zeffert DT, Paizes A and Skeen A St Q (2003) 685.
[516] Hofman J (2010) 683.
[517] Hofman J (2010) 682.
[518] Discussed in 2.2.2; Section 15(4) of the Electronic Communications and Transactions Act; Watney (2009) 8.

concerns about its accuracy.[519] The SALRC considered whether courts should apply a higher admissibility hurdle in the context of authentication than for other form of tangible evidence.[520] For instance, should the standard of proof applicable to the authentication of electronic evidence require *prima facie*[521] or conclusive proof that the evidence is what it purports to represent?[522] A higher degree of admissibility in the context authentication, such as a standard of conclusive proof, should not be required for electronic evidence than for other forms of evidence. However, it has been suggested that the authentication rule, as stated in the Canadian Uniform Electronic Evidence Act, is inadequate to safeguard against the use of unreliable electronic records as evidence.[523] For example, a software failure casts doubt on credibility of the content the electronic record and a sufficient guarantee of reliability is necessary.[524] The authentication should establish *prima facie* admissibility as to the reliability of the electronic record, and not merely state who has the burden of proving that the electronic record is in fact what it purports to be.[525]

The ECT Act should codify the common law principle of authentication which applies to data messages the functional equivalent of documentary and real evidence. A standard of *prima facie* proof should be required, otherwise the integrity and reliability of data messages that are the functional equivalent of real evidence will not be evaluated as it is not subject to any exclusionary rules.[526] The ECT Act should, similar to the English Civil Evidence Act and Criminal Justice Act, provide for the authentication of data messages in a manner determined by the court based on the circumstances of each case.

5.2.2 The Exclusionary Rules of Evidence

5.2.2.1 The Best Evidence Rule

[519] SALRC Issue Paper 27 (2010) 66.
[520] SALRC Issue Paper 27 (2010) 67.
[521] In *Ex parte Minister of Justice: In re R v Jacobson and Levy* 1931 AD 466, Stratford JA said: '*Prima facie* evidence in its usual sense is used to mean *prima facie* proof of an issue, the burden of proving which is upon the party giving that evidence. In the absences of further evidence from the other side, the *prima facie* proof becomes conclusive proof and the part giving it discharges his onus.' Zeffert DT, Paizes A and Skeen A St Q (2003) 685.
[522] SALRC Issue Paper 27 (2010) 68.
[523] Chasse K (2010) 173
[524] Chasse K (2010) 122-123.
[525] Chasse K (2010) 132.
[526] Discussed above in 5.2.1.1.

In Canadian law, the best evidence rule requires a party to produce the original or a copy that is sufficiently trustworthy.[527] As discussed, an electronic copy is not necessarily more reliable than the original.[528] Thus, it is important to rather prove the integrity[529] of the electronic document.

The Uniform Electronic Evidence Act shifted emphasis to the integrity electronic record system.[530] Evidence of the reliability[531] of the system must be produced.[532] For example, access controls, security features, verification rules, and retention or destruction schedules.[533] This can be proven by an affidavit or expert evidence, depending on the nature of the technology.[534]

The Act also allows for evidence to be presented in respect of any current standards, procedures and practices in regard to the integrity of the electronic record or storage system.[535] Such standards are not binding on the court, but will have persuasive value.[536] The extent of the standards, procedures and practices depend on the circumstances of the business or the person, for instance one could show compliance with your own standards.[537]

In England, the Civil Evidence Act and the Criminal Justice Act effectively abolished the best evidence rule and removed the difficulties associated with a copy and the original. Both acts permit the introduction of secondary evidence for the purpose of proving the statement contained in a document, authenticated in such a manner approved by the court.[538]

In the *Springsteen* case, Parker LJ stated that 'the "admissibility" of secondary evidence of the contents of documents is, in my judgment, entirely dependent upon whether or not any

[527] Discussed above in 4.3.1.
[528] Discussed above in 4.3.1.
[529] '[T]his relates to how sound the data is, such as whether the data is damaged in some way, and whether it is complete, in that is possesses all the necessary parts and links.' See Mason S (2010) 102.
[530] Section 4 of the Uniform Electronic Evidence Act.
[531] '[T]his is the capacity of a digital object to stand for the facts to which it purports to attest, which in turn is linked to t ensuring sufficient procedural and technical attributes (including a combination of preventative measures, such as to prevent unauthorised amendments and changes, and verification measures to provide for a degree of assurance to the identity of users and provision of audit trails to the document when data is viewed and manipulated) are in place and working to provide a degree of assurance that the digital object can be deemed to be reliable.' See Mason S (2010) 102.
[532] ULCC Commentary on the Uniform Electronic Evidence Act.
[533] ULCC Commentary on the Evidence Act.
[534] Currie RJ & Coughlan S (2010) 266.
[535] Section 6 of the Uniform Electronic Evidence Act.
[536] Currie RJ & Coughlan J (2010) 272.
[537] ULCC Commentary on the Evidence Act.
[538] Section 8 of the Civil Evidence Act and section 133 of the Criminal Justice Act.

weight is to be attached to that evidence'.[539] The submission of secondary evidence has always been the norm for electronic evidence, and proving the integrity of the data is essential where authenticity is in issue.[540] It is superfluous to debate whether the electronic data constitutes a copy or an original, it is more important to establish the reliability of the data.[541]

In South African law, the rule of evidence is that '… no evidence is ordinary admissible to prove the contents of a document except the original document itself'.[542] Section 14 of the ECT Act states a data message will satisfy the requirement of originality if the integrity of the information is established. To assess the integrity, consideration must be given to whether the information is complete and unaltered and the purpose for which the information was generated.[543]

Chasse suggests the best evidence rule (and the hearsay rule) should be abolished. Both these rules are centered on authenticity for electronic evidence.[544] Thus, electronic records should only have to satisfy the authentication rule. The removal of the best evidence rule will alleviate many problems associate with electronic documents, such as searching for the original or another format as good as the original.[545] The focus should be on whether an adequate protocol or standard was adopted and terms such as 'original', 'copy' and 'best evidence' should be forgotten.[546] It has been submitted that the ECT Act should provide that, at authentication stage, the integrity of the data message be considered. If necessary, at this stage an expert may explain why the content of the data message is to be trusted.[547] Mason also points out that it is important to ascertain whether that specific item of electronic evidence in question is to be trusted or not.[548] Reference to protocols or standards should not be binding on the court, but should rather have persuasive value as in terms of the Canadian Uniform Electronic Evidence Act.[549] If the best evidence rule is removed, the public and private sectors should know the best possible methods of producing and storing records with

[539] [2001] EMLR 654 at para 85.
[540] Mason S (2010) 312.
[541] Mason S (2010) 318.
[542] *Barclays Western Bank Ltd v Creser* 1982 (2) SA 104 (T) at 106.
[543] Section 14(2) of the Electronic Communications Act.
[544] Chasse K (2010) 174.
[545] LRCI Consultation Paper 57 (2009) 74.
[546] Van der Merwe D et al (2008) 128.
[547] Van der Merwe D et al (2008) 128.
[548] Mason S (2010) 86.
[549] Section 6 of the Uniform Electronic Evidence Act.

the minimum amount of uncertainty regarding their legal rights.[550] Industry standards would serve as a guideline for the public and private sectors.

Section 15(1)(b) of the ECT Act serves as a qualification of the best evidence rule, and stipulates that if a data message was the best evidence that could be reasonable expected to obtain, the requirement of originality is also met.[551] What is reasonable will depend on the circumstances of each case. An original of an electronic document may be interpreted to mean a reproduction in printed form, or a copy of an electronic document, whichever form is adopted should provide as much certainty as possible under the circumstances.[552]

5.2.2.2 The Hearsay Evidence Rule

The Uniform Electronic Evidence Act does not modify the common law, thus the admission of an electronic record may depend on the hearsay evidence rule.[553]

In Canadian law the courts follow a principled approach to the hearsay rule, namely that if an electronic record does not fall under an exception to the hearsay rule, it must be necessary and reliable to become admissible.[554] The necessity of an electronic record is usually proven by demonstrating the need to preserve information beyond human capacity.[555] An electronic record can satisfy the requirement of reliability by adducing proof of the integrity of the electronic record or storage system.[556]

In England, the Criminal Justice Act and the Civil Evidence Act virtually abolished the hearsay rule.[557] Both pieces of legislation allows for the admissibility of hearsay evidence upon satisfaction of certain conditions.

Evidence in electronic format is mostly considered to be hearsay.[558] However, the emphasis is placed on showing the reliability, integrity and trustworthiness of the electronic

[550] LRCI Consultation Paper 57 (2009) 74.
[551] Hofman J (2010) 683.
[552] LRCI Consultation Paper 57 (2009) 74.
[553] Section 2(1) of the Uniform Electronic Evidence Act.
[554] *R v Khelawon* [2006] SCC 57.
[555] Gregory JD (2002) 330.
[556] Currie RJ & Coughlan S (2010) 272.
[557] Section 1(1) of the Civil Evidence Act and Section 114(1) of the Criminal Justice Act.
[558] Mason S (2010) 338.

evidence.[559] Electronic evidence that contains a human input must be shown that the information that was fed to the device is accurate.[560]

In South Africa the hearsay rule states where evidence is used to show the truth of its contents, the common law requires that the person responsible for the evidence should be available to be cross-examined about its contents.[561] The ECT Act stipulates that data messages must satisfy the ordinary requirements of admissibility in terms of South African law.[562]

The hearsay rule only applies to data messages that are the functional equivalent to documents.[563] The data message will be inadmissible, unless the author of the data message testifies as to the contents.[564]

In various jurisdictions the approach to hearsay matters is not focused on the definition or the exceptions, but the safeguards for the assessment of reliability.[565] The South African Law Reform Commission considered the following possibility in regard to the hearsay rule. In terms of the ECT Act, section 15(1) could make all data messages admissible, including data messages subject to the hearsay rule and exempt it from the exception contained in section 3 of the Law of Evidence Amendment Act.[566] However, the reliability of the data messages must be assessed in some manner. In terms of English law, a possible approach is to show the reliability of the data message while taking into account the considerations in section 15(3), and if the reliability cannot be established the probative value does not justify its admission into evidence. However, a preferable approach would be to show the reliability of electronic hearsay evidence at authentication stage.[567] Chasse suggests to incorporate a system integrity test for the integrity of an electronic record is dependent upon the electronic record system it comes from.[568]

5.2.2.2.1 The Exceptions to the Hearsay Evidence Rule

[559] Mason S (2010) 339.
[560] Section 129 of the Criminal Justice Act.
[561] Hofman J (2010) 684.
[562] Section 15(1) of the Electronic Communications and Transactions Act.
[563] Hofman J (2010) 684.
[564] Hofman J (2010) 684.
[565] LRCI Consultation Paper 57 (2009) 71.
[566] SALRC Issue Paper 27 (2010) 60.
[567] Chasse K (2010) 173.
[568] Chasse K (2010) 107.

In Canadian law, an electronic record that does not fall under an exception to the hearsay rule must be necessary and reliable.[569] The Uniform Electronic Evidence Act contains an exception to the hearsay rule in the form of a presumption in regard to business records.[570] In such an instance, the integrity of electronic records is presumed when the record is stored or recorded in the usual and ordinary course of business by a person not party to the proceedings or under the control of the proponent of the record.[571] This is problematic because the integrity of electronic business records is not tested under the Uniform Electronic Evidence Act.

In England, the Civil Evidence Act and the Criminal Justice Act has retained a number of exceptions to the hearsay rule that is relevant to evidence in electronic format, including a business record exception.[572] Section 9 allows for a document, and not the statements recorded therein, to be allowed into evidence if it forms part of the records of a business or public authority. Section 117 provides for an exception for documents created in the ordinary course of business, trade, profession, or other occupation subject to certain conditions.

In terms of South African law, a data message is inadmissible if the truth of its contents cannot be established without the testimony of the person responsible for the data, unless it falls under an exception to the hearsay evidence rule.[573] Section 15(4) makes business records admissible without the testimony of the person responsible for the data message.[574]

The business rule exception is problematic in South Africa, since it does not follow the Model Law. The broad exception goes against the functional equivalence approach in the Model Law as argued by Hofman.[575] The SALRC questioned whether section 15(4) should be reviewed and 'in the ordinary course of business' be given a restrictive interpretation.[576] Although bank records or records of a public are regulated it should be given probative value, the business records, however, should not constitute rebuttable proof on the mere production.[577] Reliability cannot be assumed, because there is no guarantee that all businesses

[569] *R v Khelawon* [2006] SCC 57.
[570] Section 5(1)(c) of the Uniform Electronic Evidence Act.
[571] ULCC Commentary on the Uniform Electronic Evidence Act.
[572] Section 9 of the Civil Evidence Act; Sections 117 of the Criminal Justice Act.
[573] Hofman J (2010) 684.
[574] Mason S (2010) 686.
[575] Hofman J (2010) 688.
[576] SALRC Issue Paper 27 (2010) 69.
[577] Hofman J (2010) 689.

kept their records accurately or honestly.[578] It has been submitted that the ECT Act should provide for the consideration of the integrity of the system responsible for the data of the business, failing which a restrictive interpretation should be given to section 15(4).

5.2.2 The Evidential Weight

In Canada, in terms of the Uniform Electronic Evidence Act, when assessing the evidential value of an electronic record the integrity of the electronic record system will be considered.[579] The Act permits reference to recognised standards, but it is not binding on the court and will merely have persuasive value.[580]

In England, there are no fixed rules to determine the weight of evidence.[581] In regard to electronic evidence, it is likely that the court will take into account the testimony of a digital expert.[582]

Section 4 of the Civil Evidence Act provides for factors the court can take into account when assessing hearsay evidence, which is relevant to electronic documentary evidence when it is submitted to prove the truth of its contents.

In South African law, once evidence is admitted the court needs to decide what weight to attach to it.[583]

The ECT Act set out guidelines that the court can take into account when assessing the evidential value of a data message.[584] The reliability of the manner in which the data message was generated, stored or communicated,[585] the manner in which the integrity of the data message was maintained,[586] and the manner in which the originator of the data message is identified is regarded.[587] For example, an electronic signature can used to identify the author of the data message. The court may also take into account any other relevant factor.[588] When

[578] Hofman J (2010) 689.
[579] Section 6 of the Uniform Electronic Evidence Act.
[580] Currie RJ & Coughlan S (2010) 272.
[581] Mason S (2010) 319.
[582] Mason S (2010) 86.
[583] Hofman J (2010) 691.
[584] Section 15(3) of the Electronic Communications and Transactions Act.
[585] Section 15(3)(a) of the Electronic Communications and Transactions Act.
[586] Section 15(3)(b) of the Electronic Communications and Transactions Act.
[587] Section 15(3)(c) of the Electronic Communications and Transactions Act.
[588] Section 15(3)(d) of the Electronic Communications and Transactions Act.

dealing with electronic real evidence, the testimony of an expert[589] may be needed.[590] When relying on expert evidence, courts will expect the experts to refer to international standards.[591]

The South African ECT Act has stipulated guidelines that the court may take into account when assessing the weight of a data message.[592] The Canadian Uniform Electronic Evidence Act contains no such guidelines. However, the English Civil Evidence Act does contain guidelines, but only in regard to electronic hearsay evidence.[593]

The ECT Act states that regard must be had to the reliability of the communication, generation or storage, and the maintenance of integrity of the data message. In order to make such an assessment, the court will have to refer the system responsible for the data message. The Canadian Uniform Electronic Evidence Act clearly states that the integrity of the electronic record system must be taken into account, albeit under the admissibility of the electronic record.[594] This will no doubt prove useful for the court during the assessment of the evidential weight of a data message.

The Canadian Uniform Electronic Evidence Act provides that recognised standards may be considered for purposes of admissibility of electronic records.[595] South African academics have submitted that an objective criterion is necessary to evaluate electronic evidence that use new technology.[596] In England, a more circumstantial view is held that it is uncommon standards will be considered, and rather testimony of a digital expert, who as to explain whether or not the electronic evidence, in question, is reliable. South African courts should rely on expert evidence when assessing the evidential weight of a data message of a highly technical nature. For instance, the mere fact that a business has not adopted a universal standard does not necessarily mean the data message or the system is unreliable.

5.3 Conclusion

[589] Experts that establish their credentials will explain technical procedures to the court. Hofman J (2010) 696.
[590] Hofman J (2010) 691.
[591] Hofman J (2010) 692
[592] Section 15(3) of the Electronic Communications and Transactions Act.
[593] Section 4 of the Civil Evidence Act.
[594] Section 4 of the Uniform Electronic Evidence Act.
[595] Section 6 of the Uniform Electronic Evidence Act.
[596] Hofman J (2010) 692; van der Merwe D et al (2008) 127.

South African can be considered a frontrunner in the area of electronic evidence in Africa because of the recent adoption of technology-related statutes.[597] However, Hofman stated that South African law is missing procedures for the collection, storage and presentation of electronic evidence in court.[598] Such procedures can be introduced in terms of the court rules or practice notes. The emphasis should be on the importance of such procedures as it essentially deals with the chain of custody of the evidence, which would ensure the integrity of the electronic evidence, even during litigation. This would provide judicial confidence regarding the treatment of electronic evidence in legal proceedings.

The ECT Act is, in certain respects, sufficient to regulate the admissibility and evidential weight of electronic evidence. However, the ECT Act and the South African law of evidence require some streamlining to assure efficiency and predictability of producing electronic evidence (even as modern technology develops).[599] South Africa should adopt a more inclusionary approach to the regulation of electronic evidence, which based on principled flexibility[600] and technological neutrality[601].

The South African legislature should adhere to international standards and the South African Bureau of Standards also has an important role to play.[602] However, this approach should not be overstressed. The tendency in other countries, such as Canada, is to not prescribe special rules for electronic evidence and treat such evidence on the same basis as other form of evidence.[603] Any reform should be part of the general reform of the South African law of evidence.[604]

Final word count: 26 335.

[597] Van der Merwe D et al (2008) 290.
[598] Hofman J (2006) 30.
[599] LRCI Consultation Paper 57 (2009) 72.
[600] Currie RJ & Coughlan S (2010) 268.
[601] LRCI Consultation Paper 57 (2009) 74.
[602] Van der Merwe D et al (2008) 290.
[603] Hofman J (2010) 702.
[604] Hofman J (2010) 702.

BIBLIOGRAPHY

BOOKS

Canada

Underwood G & Penner J *Electronic Evidence in Canada* 2 ed (2010) Toronto: Carswell

Currie RJ and S Coughlan S 'Canada' in Mason S (ed) *Electronic Evidence* 2 ed (2010) London: LexisNexis Butterworths

England and Wales

Mason S in 'England and Wales' in Mason S (ed) *Electronic Evidence* 2 ed (2010) London: LexisNexis Butterworths

Tapper C *Computer Law* 4 ed (1989) Harlow: Longman

Tapper C (ed) *Cross & Tapper on Evidence* 8 ed (1995) London: Butterworths

South Africa

Hofman J 'South Africa' in Mason S (ed) *Electronic Evidence* (2010) London: LexisNexis Butterworths

Hoffmann LH & Zeffert DT *South African Law of Evidence* 4 ed (1988) Durban: Butterworths

Schwikkard PJ & Van der Merwe SE *Principles of Evidence* 3 ed (2009) Wetton: Juta

Van der Merwe D *Computers and the Law* 2 ed (2000) Kenwyn: Juta

Van der Merwe D *et al Information and Communications Technology Law* (2008) Durban: LexisNexis

Zeffert DT, Paizes A and Skeen A St Q *The South African Law of Evidence* (2003) Durban: LexisNexis

CASES

Canada

Ares v Venner [1970] SCR 608

R v Abbey [1982] 2 SCR 24

R v Bell (1982) 65 CCC (2d) 377

R v Corbett [1988] 1 SCR 670

R v Hall [1998] BCJ 2515

R v McCulloch 1992 CarswellBC 2586

R v Smeland (1995) 54 BCAC 49

R v Starr [2000] 2 SCR 144

R v Khelawon [2006] SCC 57

Saturley v CIBC World Markets Inc. (2012) CarswellNS 420

England and Wales

Branagan v Director of Public Prosections [2000] RTR 235

Omychund v Barker 1 ATK 21

Darby v Director of Public Prosecutions [1995] RTR 294

Director of Public Prosecutions v McKeown [1997] 1 WLR 295

Gillespie (1967) 51 Cr App R 172

Myers v Director of Public Prosecutions [1965] AC 1001

R v Bedi (1992) 95 Cr App R 21

R v Daye [1908] 2 KB 333

R v Dove [2005] EWCA Crim 1982

R v Ewing [1983] QB 1039

R v Fowden and White [1982] Crim LR 588

R v Governor of Brixton Prison and Another, ex parte Levin [1997] AC 741

R v Governor of Pentonville ex parte Osman [1990] 1 WLR 277

R v Harper [1989] 1 WLR 441

R v Murphy [1990] NI 306

R (on the application of O) v Coventry Justices [2004] EWHC 905.

R *v Penny (2002)* 163 CCC (3d) 329

R v *Saward* [2005] EWCA Crim 3183

R v Shepard (1991) 93 Cr App Rep 139

R v *Skinner* [2005] EWCA Crim 1439

R v Spiby [1991] Crim LR 199 CA

Springsteen v Masquerade Music Ltd [2001] EMLR 654

Victor Chandler International Ltd v Customs and Excise Comrs [2000] 2 Akk ER 315

South Africa

Aruba Construction v Aruba Holdings 2003 (2) SA 155 (C)

Barclays Western Bank Ltd v Creser 1982 (2) SA 104 (T)

Ex parte Rosche [1998] 1 All SA 319 (W)

Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa 1971 (3) SA 937 (T)

Ex parte Minister of Justice: In re R v Jacobson and Levy 1931 AD 466

MTN Service Provider (Pty) Limited v L A Consortium & Vending CC t/a L A Enterprises and Others 2011 (4) SA 562 (W)

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

Ndlovu v Minister of Correctional Services and another [2006] 4 All SA 165 (W)

R v Matthews 1960 (1) SA 752 (A)

R v Pelunsky 1914 AD 360

R v Schaube-Kuffler 1969 2 SA 40 (RA)

R v Trupedo 1920 AD 58

S v De Villiers 1993 (1) SACR 574 (Nm)

S v Gokool 1965 3 SA 461 (N)

S v Harper 1981(1) SA 88 (D)

S v Naidoo 1998 1 SACR 479 (N)

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

S v M 2002 (2) SACR 411 (SCA)

S v Mark 2001 1 SACR 572 (C)

S v Madiba 1998 1 BLCR 38 (D)

S v Mashiyi 2002 (2) SACR 387 (Tk)

S v Motata (Johannesburg District Court) unreported case no 63/968/07

S v Mphala 1998 1 SACR 654 (W)

S v Ramgobin 1986 (4) SA 117 (N)

S v Tandwa 2008 (1) SACR 613 (SCA)

Seccombe v Attorney-General 2002 (2) All SA 185 (Ck)

Shrosbee v Klerck 2000 (4) SA 457 (SE)

Standard Merchant Bank v Creaser 1982 (4) SA 671 (W)

Vulcan Rubber Works (Pty) Ltd v South African Railways and Harbours [1958] 3 All SA 241 (A)

Welz v Hall 1996 4 SA 1073 (C)

INTERNET SOURCES

Uniform Law Conference of Canada Commentary on the Uniform Electronic Evidence Act of 1998 available at http://www.ulcc.ca/en/us/index.cfm?sec=1&sub=1u2 (accessed 15 August 2012)

JOURNAL ARTICLES

Canada

Chasse K 'The Admissibility of Electronic Business Records' (2010) 8 *CANJTL* 105

Chasse K 'Electronic Discovery - Sedona Canada Is Inadequate on Records Management - Here's Sedona Canada in Amended Form' (2011) 9 *CANJLT* 143

Gregory JD 'Authentication Rules and Electronic Records' (2002) 81 *Can Bar Rev* 529

Gregory JD 'Canadian Electronic Commerce Legislation' (2002) 17 *BFLR* 277

England

Pattenden R 'Authenticating "things" in English law: Principles for adducing tangible evidence in common law jury trials' (2008) 12 *E&P* 290

South Africa

Collier D 'Evidently not so simple: Producing computer print-outs in court' 2005 (1) *JBL* 6

Hofman J'The meaning of the exclusions in section 4 of the Electronic Communications and Transactions Act 25 of 2002' 2007 *SALJ* 262

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

LAW COMMISSION REPORTS AND PAPERS

South Africa

South African Law Commission Discussion Paper 99 (Project 108) *Computer-related Crime* (2001)

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 Report (Project 6) *Review of the Law of Evidence* (1987)

South African Law Commission Issue Paper 14 (Project 108) *Computer-related crime* (1998)

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 Commission Working Paper 60 (Project 95) *Investigation into the Computer Evidence Act 57 of 1983* (1995)

Ireland

Law Reform Commission of Ireland Consultation Paper 57 (Project 7) *Documentary and Electronic Evidence* (2009)

LEGISLATION

Canada

Alberta Evidence Act RSA 2000

Canada Evidence Act RSC 1985

Nova Scotia Evidence Act RSNS 1989

Ontario Evidence Act RSO 1990

Uniform Electronic Evidence Act of 1998

Uniform Electronic Commerce Act of 1998

England and Wales

Civil Evidence Act 1995

Civil Procedure Rules of 1998

Criminal Evidence Act of 1965

Criminal Justice Act of 1988

Criminal Justice Act 2003

Electronic Communications Act of 2000

English Evidence Act of 1938

Police and Criminal Evidence Act of 1984

Youth Justice and Criminal Evidence Act 1999

South Africa

Civil Proceedings Evidence Act 25 of 1965

Constitution of the Republic of South Africa Act 108 of 1996

Criminal Procedure Act 51 of 1977

Computer Evidence Act 57 of 1983

Electronic Communications and Transactions Act 25 of 2002

Law of Evidence Amendment Act 45 of 1988

RESOLUTIONS

United Nations

United Nations Commission on International Trade Law Model Law on Electronic Commerce with Guide to Enactment 1996

THESES

Marshall A *Liability of Defective Software in South Africa* (LLM minor dissertation, University of Cape Town, 2005)