South African Law Reform Commission

ISSUE PAPER 27

PROJECT 126: REVIEW OF THE LAW OF EVIDENCE

ELECTRONIC EVIDENCE IN CRIMINAL AND CIVIL PROCEEDINGS: ADMISSIBILITY AND RELATED ISSUES

Closing date for comments:
30 JUNE 2010

ISBN: 978-0-621-389226-5

INTRODUCTION

The South African Law Commission was established by the South African Law Commission Act, 1973 (Act 19 of 1973).

The members of the Commission are -

The Honourable Madam Justice Y Mokgoro (Chairperson)
The Honourable Mr Justice W Seriti (Vice-Chairperson)
The Honourable Mr Justice D Davis (Member)
Adv D Ntsebeza, SC (Member)
Professor C Albertyn (Member)
Professor PJ Schwikkard (Member)
Advocate M Sello (Member)
Advocate T Ncgukaitobi (Member)

The Secretary is Mr MF Palumbo. The Commission's offices are on the 12th floor, Sanlam Centre, c/o Andries and Pretorius Street, Pretoria. Correspondence should be addressed to:

The Secretary, South African Law Reform Commission
Private Bag X 668, PRETORIA, 0001
Telephone: (012) 392-9540
Telefax: (012) 320-0936
E-mail: nesingh@justice.gov.za
Internet: http://www.doj.gov.za/salrc/index.htm

The project committee on the review of the law of evidence is responsible for this project. The project leader for this project is Professor PJ Schwikkard. The members of the committee are -

The Honourable Mr Justice W Seriti (Vice Chairperson of the Commission)
The Honourable Madam Justice N Mhlantla
The Honourable Madam Justice T Ndita
Prof L Fernandez
Adv T Masuku

This Issue Paper is available on the Internet: http://www.doj.gov.za/salrc/index.htm

Preface

This Issue Paper, which reflects information gathered up to the end of January 2010, was prepared to serve as a basis for the Commission's deliberations, to elicit comment and suggestions from relevant stakeholders and to disseminate information on the issue of the use of electronic evidence in criminal and civil proceedings to the wider public. As a result, this paper does not contain clearly defined recommendations for law reform. The view, conclusions and recommendations in this paper are accordingly not to be regarded as the Commission's final views. The Issue Paper is published in full to provide persons and bodies wishing to comment or to make suggestions for the reform of this particular branch of the law with sufficient background information to enable them to place focused submissions before the Commission.

Submissions on this Issue Paper coupled with further intensive research will form the basis for a Discussion Paper which is to follow. The Discussion Paper will contain the Commission's preliminary proposals for law reform, comparative studies and draft legislation. The Discussion Paper will be circulated for general comment and extensive consultation with relevant role-players and members of the public will follow. The purpose of the consultation process will be to test public opinion on solutions identified by the Commission. Submissions on the Discussion Paper will form the basis for preparation of a Report. The Report will contain the Commission's final recommendations and will include the Commission's final proposals and draft legislation (where applicable), which will be submitted to the Minister for Justice and Constitutional Development for consideration. Should the Minister deem it fit, he or she may then implement the Commission's recommendations by introducing the draft legislation in Parliament.

Respondents are requested to submit written comments, representations or requests to the Commission by **30 JUNE 2010** at the address listed on the previous page. Respondents are not restricted to the questions posed and issues raised in this Issue Paper and are welcome to draw other relevant matters to the Commission's attention. In making submissions, the allocated researcher will endeavour to assist with any difficulties and/or questions in this regard. Comment already forwarded to the Commission should not be repeated; in such event, respondents should merely indicate that they abide by their previous comment, if this remains the position.

The Commission will assume that respondents agree to the Commission quoting from or referring to comments and attributing comments to respondents, unless representations are marked confidential. Respondents should be aware that the Commission might be required to release information contained in representation under the Constitution of the Republic of South Africa, Act 108 of 1996.

The researcher allocated to this project is Ms N Singh. The project leader responsible for the project is Professor PJ Schwikkard.

Ms Singh may be contacted for further information on this Issue Paper at the contact details listed on page ii above.

CONTENTS

SOURCES

South African Law Reform Commission

Annual Reports

29th Annual Report (2001/02) of the SA Law Reform Commission

30th Annual Report (2002/03) of the SA Law Reform Commission

31st Annual Report (2003/04) of the SA Law Reform Commission

Reports

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

South African Law Commission Report *Review of the Law of Evidence* (Project 6, October 1986)

South African Law Reform Commission *Report on the Preliminary Investigation into the Review of the Rules of Evidence* (Project 126, June 2002)

South African Law Reform Commission *The Use Of Electronic Equipment In Court Proceedings (Postponement Of Criminal Cases Via Audiovisual Link)* (Project 113, July 2003)

Discussion Papers

Discussion Paper 99 *Computer related crime: preliminary proposals for reform in respect of unauthorised access to computer, unauthorised modification of computer data and software applications and related procedural aspects* (Project 108, 2001).

Discussion Paper 113 *Review of the Law of Evidence—Hearsay and Relevance* (Project 126, January 2008).

Issue Papers

Issue Paper 26 *General Overview of the Rules of Evidence and Possible Areas for Reform* (Project 126, January 2008)

Books

R Buys and F Cronjé (ed) *Cyberlaw@SA: The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2000).

R Buys and F Cronjé (ed) *Cyberlaw@SA II: The Law of the Internet in South Africa* (Van Schaik Publishers Pretoria 2004).

E Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2nd edn Elsevier Academic Press CA 2004).

LH Hoffmann and DT Zeffertt *South African Law of Evidence* (4th edn Butterworths Durban1988).

DP van der Merwe *Computers and the Law* (2nd edn Juta Kenwyn 2000).

DP van der Merwe *et al Information and Communications Technology Law* (LexisNexis Durban 2008).

DT Zeffertt, AP Paizes and A St Q Skeen *The South African Law of Evidence* (LexisNexis Butterworths Durban 2001).

DT Zeffertt, AP Paizes and A St Q Skeen *The South African Law of Evidence* (LexisNexis Butterworths Durban 2003).

Articles

J Coetzee 'Incoterms, Electronic Data Interchange, and Electronic Communications and Transactions Act' (2003) 15 SA Merc LJ 1.

J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 Stell LR 501.

DW Collier 'Electronic Evidence and Related Matters' in PJ Schwikkard et al *Principles of Evidence* (3rd edn Juta & Co Wetton 2009).

D De Andrade 'Is the Pen Mightier than the Electronic Signature' <http://www.derebus.org.za/nxt/gateway.dll/bsxha/uei9/7okka/eqkka/svbua> (30 October 2009).

J Hofman 'South Africa' in S Mason *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths: London 2007).

J Hofman 'The Meaning of Exclusions in section 4 of the Electronic Communications and Transactions Act 25 of 2002' 2007 SALJ 262.

W Jacobs 'The Electronic Communications and Transactions Act: Consumer Protection and Internet Contracts' 2004 SA Merc LJ 556.

S Mason 'Sources of Digital Evidence' in S Mason (gen ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (1st edn LexisNexis Butterworths London 2007).

C Reed 'The Admissibility and Authentication of Computer Evidence: A Confusion of Issues' in T Green (ed) *British and Irish Legal Education Technology Association—5th Annual Conference* (Law and Technology Centre for UK Law Schools London 1990).

M Reimann *Comparative Law and Private International Law* in *The Oxford Handbook of Comparative Law* (2006) 1388

C Schulze 'Electronic Commerce and Civil Jurisdiction, with Special Reference to Consumer Contracts' 2006 SA Merc LJ 31.

SL Snail 'Demystifying Electronic Signatures in South Africa – A Global Overview' paper presented at 4th Annual South African Cyberlaw Conference, Pretoria, 27-29 October 2009.

P Sommer 'Digital Footprints: Assessing Computer Evidence' (1998) Crim LR *Special Edition: Crime, Criminal Justice and the Internet* 62.

P Sommer 'Digital Footprints: Assessing Computer Evidence' (1998) Crim LR *Special Edition: Crime, Criminal Justice and the Internet* 62.

P Sommer 'Downloads, Logs and Captures: Evidence from Cyberspace' [2002] CTLR 33

A St O Skeen 'Evidence and Computers' (1984) 101 SALJ 675.

C Visser 'Online Service Provider Liability under the Electronic Communications and Transactions Act 25 of 2002' 2002 SA Merc LJ 758.

I Walden 'Computer Crime' in C Reed and J Angel (eds) *Computer Law* (5th edn OUP Oxford 2003) 295; C Tapper 'Evanescent Evidence' [1993] 1(1) International J of Law and Information Technology 35

MC Wood-Bodley 'Wills, Data Messages, and the Electronic Communications and Transactions Act' 2004 SALJ 526.

Websites

D Carter and A Katz 'Computer Crime: An Emerging Challenge for Law Enforcement' (1997) <http://www.sgrm.com/art11.htm> (12 September 2008).

E Casey 'Error, Uncertainty, and Loss in Digital Evidence' 2002 1(2) Intl J of Digital Evidence <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-DC9-7FDE-C80B5E5B306A85C4.pdf.> (8 September 2008).

T Pistorius 'The Legal Effect of Input Errors in Automated Transactions: The South African Matrix' 2008(2) JILT 2008(2) <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/20

08_2/pistorius2/pistorius2.pdf> (30 October 2008).

SL Snail 'Electronic Contracts in South Africa—A Comparative Analysis' JILT 2008(2) <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_2/snail/> (30 October 2009).

--Digital Preservation Coalition 'Media and Formats' <http://www.dpconline.org/g raphics/medfor/media.html> (3 September 2008).

--Digital Preservation Coalition 'Organisational Activities' <http://www.dpconline.org/ graphics/orgact/storage.htm l> (3 September 2008)

United National Commission on International Trade Law (UNCITRAL)

2007 *Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods* <http://www.un citral.org/pdf/english/publications/sales_publications/PromConfEcom_e.pdf> (30 October 2009).

2005 *United Nations Convention on the Use of Electronic Communications in International Contracts* <http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_c commerce/2005Convention.html> (30 October 2009).

2001 *UNCITRAL Model Law on Electronic Signatures with Guide to Enactment* < http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_si gnatures.html> (30 October 2009).

1996 *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, with additional article 5 bis as adopted in 1998* <http://www.uncitral.org/ uncitral/en/u ncitral_texts/electronic_commerce/1996Model.html> (30 October 2009).

CASE LAW

South Africa

Council for Scientific and Industrial Research v Fijen 1996(2) SA (A)

Balzan v O'Hara and others 1964(3) SA (T) 1

Ex parte Rosch [1998] 1 All SA 319 (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)

S v De Villiers 1993 (1) SACR 574 (Nm) 579

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

S v Mashiyi and another 2002 (2) SACT 387 (Tk)

S v Ndiki and others 2008 (2) SACR 252 (Ck)

United Kingdom

Castle v Cross [1984] 1 WLR 1372 (QBD)

R v Porter (Ross Warwick) [2006] EWCA Crim 560

United States

United States v Hill 322 F.Supp.2d 1081, 1090-1 (C.D.Ca 2004)

United States v Hunter 13 F.Supp.2d 574, 583 (D.Vt.1998)

LEGISLATION

South Africa

Civil Proceedings Evidence Act 25 of 1965

Computer Evidence Act 57 of 1983

Criminal Procedure Act 51 of 1977

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002.

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

CHAPTER ONE

ORIGIN OF INVESTIGATION AND BACKGROUND

Background

Project 113: *The Use of Electronic Equipment in Court Proceedings*

1.1 The Minister of Justice requested the Commission, in a letter dated 13 November 1996, to consider a proposal by Mr Justice HCJ Flemming regarding the adoption of legislation authorising video conferences in court.[1] In Judge Flemming's view legislation was urgently required in the interests of access to the law and improvement of the operation of the courts in that video conferences have the potential to reduce costs in, for example, cases involving witnesses having to travel from distant places or even residing in foreign countries and to eliminate inspections *in loco* in certain instances.

1.2 In addition, a letter by Mr D Dalling, MP to the Minister dealing with electronic trials was referred to the Commission.[2] Mr Dalling pointed to the benefits that could be reaped in terms of savings and otherwise from adopting legislation authorising the use of telecommunication technology in trials in respect of less serious offences. Mr Dalling referred to procedures abroad involving telecommunication between a presiding officer in a court room in the usual court buildings or in his or her office and the accused person in a court room in the place of detention. In Mr Dalling's view, the major benefits of utilising this particular form of trial are that transportation costs are saved, prisoners do not have to be transported from one venue to another in circumstances which are often a danger to security and furthermore time is saved.

1.3 The Commission's Working Committee approved the inclusion of an investigation into the use of electronic equipment in court proceedings in its programme; subsequently endorsed by the Minister. The investigation was included in the Commission's programme on 14 June 1997. The objective of the investigation

---

[1] In a letter to the Minister of Justice dated 14 October 1996, Justice HCJ Flemming proposes the introduction of legislation concerning the use of video conferences in court proceedings with particular reference to the giving of evidence by means of video-conferences in criminal matters.

[2] Proposal by Mr D Dalling, MP in a letter to the Minister of Justice dated 29 July 1997.

was to determine whether the use of electronic equipment in court proceedings was a viable option to save costs or prevent delays in civil and criminal trials.[3]

The Commission's approach to Project 113

1.4 In view of the several investigations with higher priority and lack of personnel due to vacancies, this investigation did not receive attention until 2003 when the Commission was requested by the office of the National Director of Public Prosecutions to expedite the investigation and to conduct a separate investigation into the possibility of postponement of cases via video conferencing.[4] The office of the National Director of Public Prosecutions identified the transportation of accused persons awaiting trial to the courts for the purpose of postponements as a problem area in that great costs are incurred in the process and it provided opportunities for prisoners to escape. It therefore embarked on a process to promote the use of video-conferencing to postpone cases of prisoners awaiting trial. The project committee on the review of the rules of evidence approved the request.[5]

1.5 The Commission recommended the use of audio-visual links with reference to applications for leave to appeal and appeals in respect of accused persons in custody in prison. The Commission's Report, *The Use of Electronic Equipment in Court Proceedings (Postponement of Criminal Cases via Audiovisual Link)* was submitted to the Minister in July 2003; and has been published. The recommendations of this report have been incorporated in the Criminal Procedure Amendment Bill, which was passed by Parliament on 22 October 2008.

---

[3] 29th Annual Report (2001/02) of the SA Law Reform Commission, p 37.

[4] See 30th Annual Report (2002/03) of the SA Law Reform Commission, p 28: "At a meeting between the Department of Justice and Constitutional Development and the National Director of Public Prosecutions it was decided that a project be launched to accelerate the initiative to postpone cases of awaiting trial prisoners by means of audio visual link between correction facilities and courts. The project committee was requested to assist in the pilot project by reviewing the legislative implications. A draft discussion document was considered by the project committee at its first meeting on 13 March 2003. The committee was of the view that the procedure should also be allowed for postponements and bail applications but that it should not extend to the actual trial and hearing of evidence".

[5] The initial proposal from the office of the National Director of Public Prosecutions was extended to include bail applications, applications for leave to appeal and the hearing for an appeal in respect of persons in custody. See 31st Annual Report (2003/04) of the SA Law Reform Commission, p 18.

Project 126: *Review of the Rules of Evidence*

1.6 The review of the law of evidence was included for research in the Commission's programme soon after its establishment in 1973. The Commission's original intention was to codify the South African law of evidence in its entirety and to consolidate it in one Act.[6] Research with a view to the eventual codification of the law of evidence was embarked upon. During 1979, the Commission gradually came to realise that the codification of the law of evidence as a whole was an enormous task which would take years to complete. The Commission noted that attempts elsewhere, for instance Canada, to codify the law of evidence had entailed much more human and financial resources than was available to the Commission. It was therefore necessary to plan the investigation anew.[7]

1.7 In view of the considerations noted above, the Commission decided to abandon the codification of the law of evidence. It decided to ascertain through research which aspects of the law of evidence were unsatisfactorily or do not meet current need, and to formulate suggestions for their reform. The Commission concluded that reform was desirable in respect of the following matters: judicial notice of customary law and foreign law, copies of documents, the marital privilege.[8] The recommendations formulated in the Commissions Report formed the basis of the Law of Evidence Amendment Act 45 of 1988.

1.8 In December 2001, the Minister approved the inclusion of the investigation into the review of the rules of evidence in the Commission's programme. A project committee for the investigation was approved on 26 November 2003. The Commission resolved that the project committee on the review of the rules of evidence should also direct project 113, the investigation into the use of electronic equipment in court proceedings.

1.9 A project committee for the investigation was approved on 26 November 2002. The committee, chaired by My Justice LTC Harms, was appointed by the Minister during February 2003. The committee's first meeting took place on 13 March 2003. It was decided that an incremental approach to this investigation should be

---

[6] See South African Law Commission Report, Project 6 *Review of the Law of Evidence* (October 1986) [1.1]-[1.2].
[7] Ibid [1.4].
[8] Ibid [1.6]-[1.8].

adopted. The principles of *relevance* and *hearsay* evidence were aspects of the law identified for immediate research.[9]

1.10 Judge Harms (project leader) and Judge Nugent (project committee member), however, resigned during February 2005. The Commission appointed Professor Schwikkard as the new project leader on 2 March 2007. The Minister appointed two new project committee members in August 2007 and the first meeting of the new committee was held on 26 October 2007. The project committee resolved to publish an issue paper in the format of a questionnaire to invite comment from all relevant role-players. The Committee also approved the publication of a discussion paper on hearsay evidence and relevance.[10]

Combining *Project 113* with *Project 126* under a single comprehensive project

1.11 Project 113 was introduced in the Commission's programme with a view to adopting legislation authorising video conferences in court proceedings and, subsequently, the postponement of criminal cases via audio-visual link. At its meeting on 15 November 2008, the project committee reconsidered the status of project 113 since completion and publication of the report on the postponement of criminal cases via audiovisual link in July 2003; including the issue of consolidating outstanding matters relating to evidence, in view of advancements in technology, with project 126.

1.12 It was recognised as necessary that any further investigation bridging the technology/law divide should extend beyond an investigation into the *use of equipment in court proceedings* and proposals for reform of the law of evidence in criminal and civil proceedings in view of technological developments should be approached in a holistic manner having regard to rules of evidence and procedures for collecting electronic evidence, storing it and presenting such evidence in court. An

[9] Professor PJ Schwikkard, one of the project committee members at the time, was requested to prepare a draft discussion paper on the principles of relevance and the hearsay rule. The project committee considered a revised discussion paper on 10 August 2004, after which the committee requested Professor Schwikkard to do further research with the assistance of Judge Nugent.

[10] The publication of an issue paper and discussion paper on hearsay evidence and relevancy was announced at a media conference on 7 March 2008. The closing date for comments in respect of both publications was 30 June 2008. The closing date for comments was subsequently extended to 31 March 2009.

important consideration is whether many of the technology-related evidentiary questions can be resolved or sufficiently dealt with under the existing rules of evidence and procedure.[11]

1.13 Following a recommendation by the project committee, the Commission approved at its meeting on 1 August 2009 that project 113 be deemed finalised and closed; and that any outstanding issues relating to evidence in project 113 be included as a sub-project under the comprehensive project of the review of the rules of evidence, project 126.

1.14 As a sub-project under project 126, an overarching investigation reviewing aspects of criminal and civil law in view of the challenging nature of technological developments is a long term goal. In adopting an incremental approach to this sub-project on electronic evidence and related matters, the Commission has in the first instance resolved to publish an Issue Paper exploring issues relating to the admissibility of electronic evidence in criminal and civil proceedings. In the case of criminal proceedings, this Issue Paper is particularly concerned with the relationship between chapter three of the Electronic Communications and Transactions (ECT) Act 25 of 2002 and the rule against hearsay.[12] The purpose of this Issue Paper is twofold. Firstly, to facilitate a focused debate on issues concerning the admissibility of electronic evidence in criminal and civil proceedings; and secondly, to allow stakeholders and practitioners in two sectors (criminal and civil) affected by the applicability and scope of the evidential provisions of the ECT Act 25 of 2002 to consider the issues raised and be provided with an opportunity to raise other relevant matters to the Commission's attention.

1.15 This Issue Paper is divided into seven chapters in which a preliminary survey of the current legal position is taken. An important consideration throughout this Issue Paper is whether technology-related evidentiary questions, subject to considerations of the unique nature and characteristics of electronic evidence can be resolved under the existing rules of evidence.

---

[11] Recent legislative interventions include the Electronic Communications and Transactions Act 25 of 2002; the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 and the Electronic Communications Act 36 of 2005.

[12] A review of the law of hearsay and recommendations for reform are detailed in Discussion Paper 113 published by the South African Law Reform Commission: *Review of the Law of Evidence—Hearsay and Relevance* (January 2008).

1.16 These chapters will form the basis of the Commission's further investigation and discussion. Consequently, the issues raised will be properly discussed and detailed in a dedicated Discussion Paper. Comment and submissions received on this Issue Paper, together with further in-depth research, will form the basis of a Discussion Paper where the issues identified for review and reform will be discussed in detail and preliminary recommendations for reform considered.

CHAPTER TWO

ASSESSING ELECTRONIC EVIDENCE

Introduction

2.1 Electronic evidence in criminal and civil proceedings is without doubt problematic.[13] Mindful of emerging new technologies, this chapter considers the nature and some of the special characteristics of electronic evidence that raise legitimate concerns about its accuracy and authenticity. Now that formal conditions to the admissibility of electronic evidence have been removed,[14] the increasing complexity and sophistication of rapidly-developing technology necessitates a shift from concerns about exclusion and admissibility subject to overly-technical requirements towards a more precise focus on issues relevant to establishing authenticity and suitable weight for the evidence which it generates.

2.2 The first reported South African case involving the admissibility of electronic evidence was heard twenty-five years before Parliament passed the ECT Act 25 of 2002. Since the judgment of *Narlis v South African Bank of Athens*,[15] the last twenty-five years have witnessed rapid developments in technology resulting in significant changes to the physical nature of computers, networked-technology, communications and a range of applications. Many of the features of modern communications technology such as low cost, ease of use and the potential of anonymity and pseudonymous activity make new technologies an appealing medium for committing and facilitating criminal activity. The involvement of technology in criminal activity also means an abundance of evidence. Data in the course of transmission or stored in some form of storage media are now valuable sources of evidence in criminal and civil proceedings.

---

[13] N Singh, DPhil thesis, University of Oxford, *Computer Evidence in Criminal Proceedings: New Challenges in Relation to Rapidly-Changing Technology* (submitted January 2009).

[14] The Computer Evidence Act 57 of 1983, now repealed by section 92 of the Electronic Communications and Transactions Act 25 of 2002, provided that an "authenticated computer-print-out [was] admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible". "Authenticated" required the printout being accompanied by an authenticated affidavit and other supplementary affidavits necessary to establish the reliability of the information contained in the printout.

[15] 1976 (2) SA 573 (A).

2.3 New technological capabilities, a range of applications and a modern global communications system with a growth in network-based crimes have produced many new forms of electronic evidence. Many of the earlier held assumptions that a computer is *just like* a "compact filing cabinet"[16] or that computer documents are *just like* the paper equivalent no longer hold true.[17] A modern and global communications system has substantially increased information that is routinely stored *only* in an electronic form. Increasingly courts are being presented with evidence that includes more than the obvious computer printouts. Electronic evidence can originate from a variety of sources, in different file formats and application systems, across a number of jurisdictions. Sources of such evidence include seized computer hard-drives and back-up media, real-time email messages, chat-room logs, ISP records, web pages, digital network traffic, local and virtual databases, digital directories, wireless devices and memory cards.

2.4 With technology rapidly evolving, "unique file formats" across various storage media are in the "hundreds of thousands … making it impossible to be familiar with every variation of every kind of digital evidence".[18] This evidence can take the form of data digitally stored as text files, graphics files, sounds, motion pictures, databases, temporary files, cache files, deleted files, and computer data generated on the storage device by the operating system or application program.[19] A simple file can contain incriminating information and have associated properties useful for investigations such as details about when a file was created, on which computer and by whom.[20]

2.5 In a networked environment, sources of evidence include server logs, the contents of devices connected to the network and the records of traffic activity.[21] Different crimes involving computers result in different types of evidence: cyber

---

[16] C Reed 'The Admissibility and Authentication of Computer Evidence: A Confusion of Issues' in T Green (ed) *British and Irish Legal Education Technology Association—5th Annual Conference* (Law and Technology Centre for UK Law Schools London 1990).

[17] P Sommer 'Digital Footprints: Assessing Computer Evidence' (1998) Crim LR *Special Edition: Crime, Criminal Justice and the Internet* 62.

[18] E Casey *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet* (2nd edn Elsevier Academic Press CA 2004) 231.

[19] This may also include files not normally viewed by the ordinary computer user. Such user may not even know of its existence. See *R v Porter (Ross Warwick)* [2006] EWCA Crim 560 where in a charge involving possessing indecent photographs of children, deleted images were only retrievable using specialist forensic techniques that would have not been available to the public.

[20] Casey (n 18) 2.

[21] S Mason 'Sources of Digital Evidence' in S Mason (gen ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* (1st edn LexisNexis Butterworths London 2007) 1, 12.

stalkers often use electronic mail communications to harass their victims; computer hackers may leave evidence of their activities in network logs files; and cases involving pornographic material the most likely source of evidence are digitised images found on computers or other storage media.[22]

Ease of manipulation

2.6 The special characteristics of electronic evidence also raise concerns about the accuracy and authenticity of the evidence. This is primarily due to the intangible and transient nature of data, especially in a networked environment where such evidence can be created, stored, copied and transmitted with relative ease. It can also be modified or tampered without signs of obvious distortions, thereby rendering the process of investigation and recording of evidence extremely vulnerable to claims of errors, accidental alteration, prejudicial interference or fabrication.[23] The nature of computers and data storage provide a myriad of ways in which users can hide, disguise or obscure their files:

> Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent. … Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing their names and extension of files to disguise their contents to the casual observer. …There is no way to know what is in a file without examining its content, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated—forecloses defendant's proposed search methodology [based on file names or extensions].[24]

2.7 Electronic evidence can also be easily changed because of the processes involved in collecting it as evidence.[25] Errors can be introduced during examination and interpretation of the evidence or the examination tools being used can contain malicious software or viruses that can cause them to represent the data incorrectly.[26] Shutting down a system for example may necessarily destroy all process-related

---

[22] Casey (n 18) 216.
[23] I Walden 'Computer Crime' in C Reed and J Angel (eds) *Computer Law* (5th edn OUP Oxford 2003) 295; C Tapper 'Evanescent Evidence' [1993] 1(1) International J of Law and Information Technology 35.
[24] *United States v Hill* 322 F.Supp.2d 1081, 1090-1 (C.D.Ca 2004) quoting *United States v Hunter* 13 F.Supp.2d 574, 583 (D.Vt.1998).
[25] P Sommer 'Downloads, Logs and Captures: Evidence from Cyberspace' [2002] CTLR 33.
[26] Casey (n 18) 133.

data. The process of opening a file or printing is not always neutral and its source and integrity is not always easy to prove. Given the volatility of the data, a failure to follow crime-scene protocols and proper procedures for handling computer evidence may render such evidence unusable or vulnerable to defence claims of errors or prejudicial distortions.[27]

Rapidly-changing technology

2.8 Developments in technology have brought about newer versions of operating systems, including software applications and hardware. Forms of data storage media, for example, are evolving at a very fast pace resulting in obsolescence of previous storage media. Whereas previously a key feature of computer operating systems included floppy disks, they are now rarely fitted in modern computers and are for the most part considered obsolete. They have now been replaced by USB (universal serial bus) flash drives and various writable and rewritable forms of CDs and DVDs.

2.9 However, a consequence of new forms of hardware and versions of software applications is that data may reach a stage, due to media or software incompatibility, where they cannot be read, understood or used.[28] Transferring data to new media and software applications also creates risks of alteration and manipulation of data. Technical obsolescence is a major problem: maintaining access to digital records over the long-term involves interdependent strategies for preservation in the short to medium term based on safeguarding storage media, content and documentation, and computer software and hardware; and strategies for long-term preservation to address the issues of software and hardware obsolescence.[29]

Media fragility

2.10 The media upon which electronic documents are stored is generally considered fragile. Unless stored correctly, storage media can deteriorate quickly and without external signs of deterioration and are at risk from accidental or deliberate

[27] Walden (n 23) 295.
[28] Mason (n 21) 25.
[29] Digital Preservation Coalition 'Organisational Activities' <http://www.dpconline.org/graphics/orgact/storage.htm l> (3 September 2008).

damage or deletion.[30] As noted earlier, forms of storage media also change. Floppy disks, for example, rapidly progressed from 8 in to 5.25 in and then 3.5 in formats, with each change leading to rapid discontinuation of previous formats and difficulty in obtaining or maintaining access devices for them.[31] They have now been replaced by USB flash drives and CDs/DVDs.

"Reading" data

2.11 The main obvious issue in *reading* data relates to what can be *seen*. Electronic evidence is, by its very nature, binary patterns in magnetic, optical or electronic form—all of which need to be translated and interpreted for the court:

> "Evidence of these crimes is neither physical nor human, but, if it exists, is little more than electronic impulses and programming codes. If someone opened a digital storage device, they would see no letters, numbers, or pictures on it".[32]

2.12 Immediate electronic evidence is not obviously readable to humans and different applications and formats of "reading" results in different displays that might change the nature of the record. Unlike documents in physical format, changes in computer data offer a greater range of variability. Data migration or use of different software applications may lead to different formatting for example, and viewings of the same source of data may not be the same. A common example familiar to all users of the Internet is that a website can look very different depending on when it is viewed and whichever browser is used to view it. This means that there can be no concept of a single, definitive representation of a particular source of data:

> The software brings together separate items of data and constructs them in a format that appears to indicate the file is a complete entity. The computer undertakes an exercise in the display of sequential logical relationships between various items of data that are retrieved by the operator for the benefit of the human. The file does not exist as it claims to exist on the screen and, in the same way, the individual components of the 'file' are not guaranteed to be preserved in the manner that will enable the file to be reconstructed over time.[33]

---

[30] Mason (n 21) 32.
[31] Digital Preservation Coalition 'Media and Formats' <http://www.dpconline.org/g rap hics/medfor/media.html> (3 September 2008).
[32] D Carter and A Katz 'Computer Crime: An Emerging Challenge for Law Enforcement' (1997) < http://www.sgrm.com/art11.htm> (12 September 2008).
[33] Mason (n 21) 30-40.

Dependence on specific hardware and software applications

2.13 Related to the above discussion on "reading data" follows dependency of specific hardware and software applications. Computer data is dependant on specific hardware (in machine form) and software applications to obtain access to it. Both the machines used and software applications are likely to yield evidence such as metadata and date-time stamps revealing information about when a document was altered or modified.

The "who", "what" and "when" of data

2.14 Physical or hard copy records, in the absence of specific reference points, reveal little about the details surrounding its compilation or composition. Computer data on the other hand is unique in that information embedded in the text or "properties" of the document known as "metadata" (data-about-data). All documents, irrespective of its format or application, will contain some form of metadata that may reveal details such as the title of the document, the date of its creation, the author, when the document was last modified, its location, including details about when it may have been transmitted.

Sources: A plethora of evidence residing almost anywhere

2.15 Most computers and operating systems now function in a networked environment, using products (notebook computers, mobile phones, PDAs, etc) and using various applications (e-mailing, instant/text messaging, 'blogging', chat-rooms) that run over networks (the Internet, wireless and cellular networking).[34] For investigators the challenges involve a greater variety of evidence that may be found anywhere on the global communications network:

> The nature of this structure means that almost everything anybody does on a device that is connected to a network is capable of being distributed and duplicated with ease. As a result, the same item of digital data can reside almost anywhere.[35]

[34] Mason (n 21) 33.
[35] Ibid.

Challenging aspects of evidence collected from a networked environment

2.16 As with stored evidence found on computers and other storage media, networks contain evidence that can be used by investigators to establish that a crime has been committed, determine how it was committed, provide investigative leads in identifying likely suspects, disclose links between an offender and victim, and disprove or support witness statements.[36] However, when dealing with network-based evidence, investigators face a number of unpredictable challenges:

> Data on networked systems are dynamic and volatile, making it difficult to take a snapshot of a network at any given instant. Unlike a single computer, it is rarely feasible to shut a network down because digital investigators often have a responsibility to secure evidence with minimal disruption to business operations that rely on the network. Besides, shutting down a network will result in the destruction of most of the digital evidence it contains. Also, given the diversity of network technologies and components, it is often necessary to apply best evidence collection techniques in unfamiliar contexts.[37]

2.17 Given the nature of a networked environment and the availability of anonymous and pseudonymous services, a suspect can be at several places on a network at any given time and the distribution of criminal activity and associated digital evidence makes it difficult to isolate a crime scene.[38] As a result, the reconstruction process can be more challenging with network-based crimes. With the possibility of a criminal or victim being at several (virtual) places on a network at any given time, the reconstruction process is more complex and difficult and because it is almost impossible to obtain all relevant information relating to a crime from a network due to mobility of hosts and changeability of networks, there are often gaps in parts of the crime reconstruction.[39]

2.18 Offenders can also use the Internet to conceal their actual location by connecting through computers located in other parts of the country or world. Computer hackers often use this method by initiating attacks from a compromised computer in a distant location to conceal their IP (Internet protocol) address and

---

[36] Casey (n 18) 383. See also E Casey 'Error, Uncertainty, and Loss in Digital Evidence' 2002 1(2) Intl J of Digital Evidence <https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.> (8 September 2008).
[37] Casey (n 18).
[38] ibid 383-4. The advantage however is that such a wide distribution of evidence makes it difficult to destroy the evidence to remove any trace of criminal activity. Even if destroyed, the evidence is likely to be available around the network on various back-up copies.
[39] Ibid 408.

geographic location.[40] Also, a Virtual Private Network (VPN) effectively and securely extends a local area network to anywhere in the world, providing an encrypted channel from the individual's computer at a remote VPN server and obtain their IP address on that network, giving the impression that their computers are on a remote network.[41]

2.19 In what is referred to as the "identity" problem, investigators face a number of challenges when dealing with TCP/IP addresses as evidence. For example, IP headers only contain information about computers, not people, and as a result, it is difficult to prove that a specific individual created a given packet. However, such information certainly is beneficial as an investigative lead and the source IP address can be used to get closer to the origin of the crime which may help identify suspects.[42] However, this may be hindered by offenders who frequently change their IP addresses (using dynamic IP addresses) so as to avoid detection. Investigators face similar difficulties in tracing the offender when information in the IP header is falsified or when a source IP address has been falsified and tracking becomes a lengthy and tedious process of examining log files on all of the routers that the information passed through.[43] The design and insecure nature of networks also make evidence collection extremely difficult:

> … few networks are designed to make evidence collection simple. Evidence is scattered and there is rarely one person in an organisation who has access to, or even knows about, all of the possible sources of computer evidence on their network. Also, every network is unique, compromising many different components that are sometimes held together by little more than the digital equivalent of duct tape. … the distributed and insecure nature of networks can introduce significant uncertainty of origin in computer evidence. The most common example of origin uncertainty on networks is forged emails. Individuals who impersonate others in email and unsolicited bulk e-mailers fabricate emails to make it more difficult to determine where the message came from. [44]

2.20 Given the unique nature and characteristics of electronic evidence discussed, some attention will have to be given to demonstrating its reliability, both at the investigative stage and in trial proceedings.

---

[40] Ibid 408.
[41] Ibid 409.
[42] Ibid 473.
[43] Ibid.
[44] Ibid 474.

2.21 Section 15(3) of the Electronic Communications and Transactions Act 25 0f 2002, gives guidelines for assessing the evidential weight of data messages:

(3) In assessing the evidential weight of a data message, regard must be had to-
  (a) the reliability of the manner in which the data message was generated, stored or communicated;
  (b) the reliability of the manner in which the integrity of the data message was maintained;
  (c) the manner in which its originator was identified; and
  (d) any other relevant factor.

2.22 Good practice and procedure guidance (national and international standards) on technical and organisational criteria such as hash values, metadata, long-term preservation strategies due to technological obsolescence, are likely to inform the courts in assessing the worth of evidence before it.

CHAPTER THREE

COMPUTER-RELATED MATTERS AND THE SOUTH AFRICAN LAW REFORM COMMISSION[45]

3.1 In April 1982, the Commission's *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers,* Project 6, Review of the Law of Evidence (1982) was presented to the Minister of Justice. As a result, in 1983 the Computer Evidence Act 57 of 1983 was passed and was largely based on the draft Bill proposed by the Commission. The Act was applicable only to civil proceedings.

3.2 The admissibility of computer generated evidence was considered by the Commission in its Discussion Paper on computer-related crime.[46] A preliminary recommendation made in the Discussion Paper as section 8 of the draft Proposed Computer Misuse Bill was the adaptation of the following evidentiary provision:

> **8** (1) Notwithstanding the provisions of any law, information in any medium, including but not confined to data or computer output, shall be admissible as evidence of any fact stated therein in any criminal proceedings in terms of this Act, it is shown –
> (a) that a standard or best procedure, acceptable to the court, has been followed in obtaining the information concerned;
> (b) in the event of any departure from such procedure, which in the opinion of the court, is not gravely prejudicial to the accused, such information shall still be admissible as evidence, but the court may then attach correspondingly less weight to such evidence;
> (2) For the purposes of deciding on the admissibility and weight of the evidence referred to in subsection (1), the court may draw any reasonable inference from the circumstances in which the application or data was found, or was originally made or came into being.

3.3 However, the Discussion Paper did not consider sections 221 or 236 of the Criminal Procedure Act or the manner in which computer generated evidence is admitted in criminal cases.

---

[45] The paragraphs under this heading are quoted from the Commission's *Report on the Preliminary Investigation into the Review of the Rules of Evidence* (Project 126, June 2002) and Issue Paper 26 *General Overview of the Rules of Evidence and Possible Areas for Reform* (Project 126, January 2008).

[46] Discussion Paper 99, Project 108 *Computer related crime: preliminary proposals for reform in respect of unauthorised access to computer, unauthorised modification of computer data and software applications and related procedural aspects* (2001).

3.4 In its 1986 report,[47] the Commission considered whether the application of the Computer Evidence Act 57 of 1983 should be extended to criminal matters but deferred any decision in this regard to further Commission investigations. The Commission published a Discussion Paper dealing with computer-related crime in 2001.[48] Further investigations by the Commission in this regard were superseded by the ECT Act 25 of 2002.

[47] South African Law Commission Report, *Review of the Law of Evidence*, Project 6, October 1986.

[48] Discussion Paper 99, Project 108 *Computer related crime: preliminary proposals for reform in respect of unauthorised access to computer, unauthorised modification of computer data and software applications and related procedural aspects* (2001).

CHAPTER FOUR

ELECTRONIC EVIDENCE IN CIVIL PROCEEDINGS

Admissibility of Electronic Evidence in Civil Proceedings

Before the ECT Act 25 of 2002

4.1 Before the ECT Act 25 of 2002, computer-related evidence was regulated in terms of the Computer Evidence Act 57 of 1983; the Civil Proceedings Evidence Act 25 of 1965 ("the CPEA Act) and the Criminal Procedure Act 51 of 1977 ("the CPA").[49]

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

4.2 The Computer Evidence Act 57 of 1983 was enacted to overcome difficulties created by *Narlis v South African Bank of Athens*.[50] In considering the admissibility of computerised bank statements under section 34(2) and 34(4) of the Civil Proceedings Evidence Act 25 of 1965, where subsection (1) specifically refers to "any statement made by a *person* in a document", the court held that the computerised bank statement could not be admitted in terms of this section since they have not been made by a *person* as contemplated by the Act.[51] Indeed, noting the problematic nature of the situation, Holmes JA remarks: "This is perhaps a matter which might well engage the attention of the Legislature in South Africa".[52]

---

[49] In terms of section 92 of the ECT Act 25 of 2002, the provisions of the Computer Evidence Act 57 of 1983 are repealed in its entirety. The provisions of the CPEA and the CPA remain relevant and may be used to assist with the admissibility of particular types of electronic evidence, such as trade or business records.

[50] 1976 (2) SA 573 (A).

[51] At 577h, Holmes JA states: "…it is essential to note that sec. 34(2) deals only with such a statement as referred to in sub-sec. (1). And straightaway one finds that sub-sec. (1) refers only to 'any statement made by *a person* in a document'. (My italics). Well, a computer, perhaps, fortunately, is not a person".

[52] At 578.

Computer Evidence Act 57 of 1983

4.3 As a result of the decision in *Narlis*, the Clearing Bankers Association of South Africa requested the South African Law Commission to investigate the need for specific legislation regulating the admissibility of computer-generated evidence in civil proceedings. This request was accepted.[53] In recognising the extent of the reform necessary, the Commission examined the possibility of amending section 34 of the Civil Proceedings Evidence Act 25 of 1965 to accommodate the admissibility of computerised records.[54] However, the Commission recognised that a "simple amendment of this nature would not solve all the problems related to the proof of computerised records"[55] and recommended that specific provision be made for computerised records.[56]

4.4 The Commission's *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computer,* Project 6, Review of the Law of Evidence (1982) was presented to the Minister of Justice in April 1982, and as a result the Computer Evidence Act 57 of 1983 was passed, largely based on the draft Bill proposed by the Commission. The Act was applicable only to civil proceedings.

4.5 The Computer Evidence Act 57 of 1983 caused numerous difficulties due to over technical requirements. Section 3(1) of the Act provided that an "authenticated computer-print-out [was] admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible".

> "Authenticated" meant that the printout must be accompanied by an authenticating affidavit and other supplementary affidavits necessary to establish the reliability of the information contained in the printout. The court could attach as much or as little evidential weight to the printout as the circumstances of the case dictated (s 4). The Act required that the deponent to the authenticating affidavit had to be a person qualified to depose thereto in two respects (s 2(3)). First, by reason of his knowledge and experience of computers and the particular system in question; and, secondly, 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. The records and facts had to be verified by him if he had control of or access to them in the ordinary course of his business, employment, duties or activities (s 2(4)(a)). If not, then a supplementary affidavit was required from a person who had control of or access to them (s 2(4)(b)). Records and facts were sufficiently

---

[53] South African Law Commission *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computer,* Project 6, Review of the Law of Evidence (April 1982) 1.
[54] Ibid 3.
[55] Ibid.
[56] Ibid 4-5.

> verified if the deponent stated that, to the best of his knowledge and belief, they comprised all the relevant records and facts.[57]

4.6 The fact that the Act was applicable only in civil proceedings was problematic and there were increasing calls for legislation relating to admissibility of computer evidence in criminal cases.[58]

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

4.7 Despite the cumbersome technical requirements of the Computer Evidence Act 57 of 1983, the court in *Ex parte Rosche* held:

> In our view a reading of the statute makes it plain that the statute does not require that whatever is retrieved from a computer can only be used if the statute's requirements have been met. *It is a facilitating act not a restricting one*.[59]

4.8 The relevant evidence in *Rosche* consisted of a telephone company's computer printouts which were automatically generated for all calls made by its subscribers, in this case the printout consisted of information of phone calls made from a hotel in Mozambique to a guest house in South Africa. Even though the provisions of the Computer Evidence Act 57 of 1983 had not been met, the court approach was to accept the printout as *real evidence*:

> The printout is real evidence in the sense that it came about automatically and not as a result of any input of information by a human being. There is therefore no room for dishonesty or human error.[60]

4.9 The trustworthiness and reliability of the printouts was established with the following evidence: (a) the information in handwritten records of the calls—they were carbon copies of the chits prepared by the telephone operator on duty at the hotel on the day in question, reflected the same information as in the printouts (although the

---

[57] DW Collier 'Electronic Evidence and Related Matters' in PJ Schwikkard et al *Principles of Evidence* (3rd edn Juta & Co Wetton 2009) 412.
[58] See para 3.4. above. See also discussions on *S v Mashiyi and another* 2002 (2) SACT 387 (Tk), chapter five below (n 86 to 94).
[59] [1998] 1 All SA 319 (W) at 327 (emphasis added).
[60] Ibid 328.

operator could not be traced to give evidence);[61] (b) evidence of the functional workings of the telephone recording equipment was adduced;[62] (c) evidence of the reliability of the information contained in the printout and similar printouts as being "accepted by both the telephone company and its subscribers as being correct over a number of years";[63] (d) information concerning the software qualities, namely (i) the software in this case did not generate random impulses as in the case of games; and (ii) it did not do creative interpretation of input as when virtual reality is created from an architect's plan.[64]

4.10 To overcome technical difficulties and in response to the growing need for new legislation providing for the use of electronic evidence in criminal cases, the Computer Evidence Act 57 of 1983 was repealed in its entirety and replaced with the ECT Act 25 of 2002.

The ECT Act 25 of 2002

4.11 The provisions of the ECT Act 25 of 2002 are considered in detail in chapter six below. In particular, chapter six sets out provisions facilitating electronic transactions with focus on the legal recognition of "data messages",[65] including the definitions of "writing"[66] and "signature"[67] in their application to electronic transacting. The chapter also focuses on section 15 of the Act (admissibility and evidential weight of data messages),[68] including a discussion on the admissibility of business records in which section 15(4) provides for the admissibility of data messages *made by a person in the ordinary course of business*.[69] In addition, chapter six examines the use of presumptions (in favour of the accuracy of data messages) created in the ECT Act 25 of 2002.[70]

---

[61] Ibid 326.
[62] Ibid 328.
[63] Ibid 328.
[64] Ibid 329.
[65] Para 6.21 below.
[66] Para 6.22 below.
[67] Paras 6.23-6.28 below
[68] Paras 6.33-6.37 below.
[69] Paras 6.38-6.41.
[70] Para 6.42 below.

CHAPTER FIVE

ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS

Admissibility of Electronic Evidence in Criminal Proceedings

Before the ECT Act 25 of 2002

5.1 The ECT Act 25 of 2002 came into effect on 30 August 2002.[71] As noted earlier, prior to its enactment, computer-related evidence was regulated in terms of the Computer Evidence Act 57 of 1983; the Civil Proceedings Evidence Act 25 of 1965 ("the CPEA Act); and the Criminal Procedure Act 51 of 1977 ("the CPA").[72]

The Criminal Procedure Act (CPA) 51 of 1977, s 221 and s 236

5.2 Admissibility of computer print-outs in criminal proceedings is based on section 221 (business records) and section 236 (banking records) of the CPA 51 of 1977. The latter allows for the admissibility of accounting records and documents in the possession of a bank, including a computer print-out or device that recorded or stored the document,[73] subject to the requisite supporting affidavits,[74] including an affidavit by a person stating that (a) they are in the service of the bank; (b) such accounting records and documents are the records of the bank; (c) the said entries or document have been made compiled, printed or obtained in the usual and ordinary course of the business of the bank; and (d) such accounting records or documents are in the custody or under the control of such bank.

---

[71] Proclamation R68, *GG* 230809 of 30 August of 2002 (Reg Gaz 7449).
[72] In terms of section 92 of the ECT Act 25 of 2002, the provisions of the Computer Evidence Act 57 of 1983 are repealed in its entirety. The provisions of the CPEA and the CPA remain relevant and may be used to assist with the admissibility of particular types of electronic evidence, such as trade or business records.
[73] In terms of section 236(6), "'document' includes a recording or transcribed computer printout produced by any device by means of which information is recorded or stored".
[74] S 236 (1) and (2).

5.3 In terms of section 221, certain trade records or business records are admissible as evidence of proof of their contents if:

(a) the document is or forms part of a record relating to any trade or business and has been compiled in the court of that trade or business, from information supplied, directly or indirectly, by persons who have or may reasonably be supposed to have personal knowledge of the matters dealt with in the information they supply; and
(b) the person who supplied the information recorded in the statement in question is dead or it outside the Republic or is unfit by reason of his physical or mental condition to attend as a witness or cannot with reasonable diligence be identified or found or cannot reasonably be expected, having regard to the time which as elapsed since he supplied the information as well as all the circumstances, to have any recollection of the matters dealt with in the information he supplied.

5.4 In terms of section 221(5): "'document' includes any device by means of which information is recorded or stored" and "'statement' includes any representation of fact, whether made in words or otherwise". The Act does not provide a definition of a 'record'.

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

5.5 The scope and meaning of section 221 of CPA 1977 was considered in *S v Harper*.[75] On the question of whether the computer-printouts are documents within the meaning of 'document' in section 221(5), it was held that the word 'document' in section 221(5) in its ordinary grammatical sense is wide enough to include computer print-outs of information stored or recorded on computer. On the question of whether the computer itself, namely the machine, would fall under the extended meaning of the definition of 'document' in section 221(5) Milne J held:

> In my view, if the computer print-outs … are 'documents' within the ordinary grammatical meaning of that word, then they are admissible. If they are not, then in my view, they are inadmissible. … Computers do record and store information but they do a great deal else; *inter alia*; they sort and collate information and make adjustments. The computer used by York in this case on the evidence of Mrs Withers, not only added the rentals received by York, it sorted them into those relating to particular buildings and made adjustments to the rent 'receipts' which it produced in advance for the next month, in the light of over and under-payments which had previously occurred. *The extended definition of "document" is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.* Quite apart from that, however, how would the document, that is in this case the computer, be

[75] 1981(1) SA 88 (D).

> produced? Even if the section could be interpreted to mean that what must be produced is that part of the computer on which information is recorded or stored, that would mean the tape or disc on which it was stored, and this would be meaningless unless the electronic impulses on that tape or disc were to be translated or transcribed into a representation or statement intelligible to the ordinary human eye – or perhaps ear. The section does not refer to the product of the device, nor does it refer to any document produced by the device, it refers to the document itself being produced. The wording of the section, read with the extended definition contained in ss (5), is entirely appropriate to the production of microfilm as evidence since the microfilm itself can be produced. Further microfilm is a means by which information is stored and recorded. No process other than storage and recording is involved so far as I am aware.[76]

5.6 Several commentators and courts have interpreted the above 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 (e.g. a computer print-out of information sorted and collated) would be inadmissible.[77] From a careful reading of the above dictum of Milne J it is clear that the court was concerned with the question of whether the computer itself, namely the machine, fell under the extended definition of "document" defined in section 221(5) as "any device by means of which information is recorded or stored". As O'Linn J in *S v De Villiers*[78] rightly pointed out, the dictum of Milne J was "misread"[79] and the general statement by Hoffmann and Zeffertt to the effect that a "computer print-out produced by a computer that sorted and collated information would be inadmissible" is incorrect.[80]

5.7 On the "question as to whether or not a computer print-out is a *document* within the ordinary grammatical meaning of that word",[81] Milne J concluded that the computer print-outs are documents within the meaning of 'document' in section 221(5) and subsequently proceeded to establish whether the other requirements enumerated in section 221 were satisfied:[82]

> The computer print-outs consist of typed words and figures and would, *prima facie*, clearly fall within the ordinary meaning of the word "document".
> …

---

[76] Ibid 95.
[77] See A St O Skeen 'Evidence and Computers' (1984) 101 SALJ 675 and Hoffmann and Zeffertt *South African Law of Evidence* (4th edn 1988) 142.
[78] 1993 (1) SACR 574 (Nm).
[79] Ibid 577 f-j. Endorsed by Van Zyl J in *S v Ndiki and others* 2008 (2) SACR 252 (Ck) at [17]-[18]. In the learned judge's view, the *Harper* decision resulted in the issue of admissibility of computer generated documents being approached from the wrong premises.
[80] Hoffmann and Zeffertt (n 77)142.
[81] *S v Harper* (n 75) 96.
[82] Ibid 96-97.

> 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, 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.* Once that situation has been achieved, then it seems to me that the main thrust of the attack upon the admissibility of these documents disappears.[83]

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

5.8 In *S v De Villiers*, the court was concerned with the question of whether or not computer print-outs of bank statements were admissible in terms of section 221 of CPA 1977.

5.9 Following the decision in *Harper*, O'Linn J held that such computer print-outs were admissible in evidence under section 221. Based on the evidence about its production, namely, that the computer print-outs certified as authentic, were in fact duplicate originals and admissible in evidence.

5.10 In assessing the weight to be attached to the statements, the court considered the factors enumerated in section 221(3)[84] and in addition to the fact that the accused did not rebut anything contained in the computer print-outs of bank statements, O'Linn J "accepted these statements as a correct reflection of the transactions recorded in therein".[85]

---

[83] *S v Harper* 1981 (1) SA 88 (D) 96-97.

[84] In terms of section 221(3): "In estimating the weight to be attached to a statement admissible as evidence under this section, regard shall be had to all the circumstances from which any inference may reasonably be drawn as to the accuracy or otherwise of the statement, and, in particular, to the question whether or not the person who supplied the information recorded in the statement, did so contemporaneously with the occurrence or existence of the facts stated, and to the question whether or not that person or any person concerned with making or keeping the record containing the statement, had any incentive to conceal or misrepresent facts".

[85] *S v De Villiers* 1993 (1) SACR 574 (Nm) 579.

***S v Mashiyi and another* 2002 (2) SACR 387 (Tk)**

5.11 The narrow reading of *Harper* was nonetheless applied in *S v Mashiyi and another*[86] and section 221 of CPA 1977 was read to exclude computer print-outs that contained information "obtained after treatment by arrangement, sorting, synthesis and calculation by the computer".[87] After quoting the following from Milne J's dictum:

> Computers do record and store information but they do a great deal else; *inter alia*, they sort and calculate information and make adjustments. … The extended definition of "document" (in ss(5)) is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than there mere storage or recording of information.[88]

Miller J placed significant confidence on the interpretation of Milne J's dictum in Hoffmann and Zeffertt[89] and Skeen,[90] albeit incorrect. Quoting the following statement from Skeen, Miller J erroneously held that the disputed documents which contained information that has been processed and generated by a computer are not admissible as evidence under section 221 of CPA 1977:

> It appears from both *Pettigrew* [*R v Pettigrew, R v Newark (1980) 71 CRR 39 (CA)]* and *Harper* that information obtained from computer print-outs is admissible under s 221 and its English equivalent only if the function of the computer was purely passive in that it merely recoded or stored the information. Implicit in both decisions is the conclusion that if the computer carried out active functions, over and above storage, then the fruits of its endeavours would be inadmissible. This conclusion would appear to be derived for two reasons, namely, the passive attributes given to a computer by the definition of 'document' and because personal knowledge would be required, either directly or indirectly, by the person supplying the information. In *Narlis v South African Bank of Athens* Holmes JA summed up that status of a computer with the following pithy remark: "Well, a computer, perhaps, fortunately, is not a person". This remark aptly expresses the underlying reasons for the decision referred to above.
> It would appear, therefore, that the admissibility of computer generated information under s 221 rests on proof that the computer was merely recording or storing information supplied by a person who originally had knowledge.[91]

5.12 Recognising the predicament of the situation and the fact that at the time there were "no statutory developments relating to the admissibility as evidence of

---

[86] 2002 (2) SACR 387 (Tk).
[87] Ibid 390.
[88] *S v Harper* 1981 (1) SA 88 (D) 95.
[89] Hoffmann and Zeffertt (n 77) 142.
[90] Skeen (n 77)
[91] Ibid 680-1. The 2001 and 2003 publications of DT Zeffertt, AP Paizes and A St Q Skeen *The South African Law of Evidence* (LexisNexis Butterworths Durban) rectified this view to be in line with the correct interpretation of *Harper* by O'Linn J in *De Villiers*.

computer generated information, in criminal cases since *Harper's* case",[92] Miller J added support to calls[93] for this "lacunae in our law be filled and for new legislation relating specifically to computer evidence in criminal cases be considered and promulgated".[94]

5.13 Such legislation comes in the form of the ECT Act 25 of 2002, which was lead through Parliament by the Department of Communications.[95]

The ECT Act 25 of 2002

5.14 The provisions of the ECT Act 25 of 2002 are set out in chapter six below. Given that the ECT 25 of 2002 is largely based on an electronic commerce Model Law (that only applies to commercial activities), this chapter questions the adequacy of the ECT Act 25 of 2002 in governing the admissibility of electronic evidence in criminal proceedings.[96] In considering the admissibility of data messages as evidence in legal proceedings, chapter six is concerned with the provisions of section 15 of the Act and its interaction with the rule against hearsay.[97] Of particular concern is whether the definition of "data message" includes real evidence as well as hearsay evidence. The discussion follows with an overview of case law after the promulgation of the ECT Act 25 of 2002 and the approach of courts as having distinguished between two types of evidence: (i) *hearsay* computer evidence; and (ii) *real* computer evidence.[98]

---

[92] *S v Mashiyi and another* 2002 (2) SACT 387 (Tk) 392.
[93] Hoffmann and Zeffertt (n 77) at 142 state: "(B)cause of what has been held in *S v Harper And Another* as regards the non-admissibility of computer print-outs in terms of s 221 of the Criminal Procedure Act 1977 (at least when the computer has processed data) there is a need for legislation that relate specifically to computer evidence in criminal cases".
[94] *S v Mashiyi and another* 2002 (2) SACT 387 (Tk) 392. The provisions of the ECT Act 25 of 2002 were not considered as the Act only came into operation on 30 August 2002.
[95] While the Department of Justice and Constitutional Development (DOJCD) took part in the consultation process preceding the Act, neither the DOJCD nor the SA Law Reform Commission contributed to the evidential provisions contained in the Act. For details of the consultation phase, see *A Green Paper on Electronic Commerce for South Africa* (November 2000) co-ordinated and compiled by the Department of Communications, Republic of South Africa.
[96] Para 6.5 below.
[97] Para 6.33 below. Discussions on assessing the evidential weight of data messages is considered at para 6.37 below.
[98] Paras 6.34-6.36 below.

CHAPTER SIX

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

6.1 This chapter discusses the current legal position concerning the admissibility of electronic evidence in criminal and civil proceedings and the conditions under which evidence stored or produced by a computer or other mechanically operated device can be admitted into evidence. This chapter considers the provisions of the Electronic Communications and Transactions (ECT) Act 25 of 2002 and its interaction with the rule against hearsay. In doing so, this chapter raises questions about the adequacy of the ECT Act 25 of 2002 in regulating the admissibility of electronic evidence in court proceedings. The ECT Act 25 of 2002 has been in operation since August 2002 and a review of its effectiveness in view of rapid developments in technology remains overdue.

Bridging the technology/law divide

6.2 New technologies pose serious challenges to existing legal concepts. While the technology/law divide cannot be fully overcome, the challenges in reducing the gap should not be underestimated. The legal issues associated with the technology/law divide require constant attention in view of the exponential growth of information technology structures driving social and economic trends.

1. BRIDGING THE TECHNOLOGY/LAW DIVIDE—QUESTION FOR COMMENT

- **Should the ECT Act 25 of 2002 be reviewed on a regular basis to take account of advances in technology?**
    - **If so, what should such a review entail?**
    - **When/how often should such a review take place?**
    - **Who should undertake the review?**

-o-

The ECT Act 25 of 2002

6.3 The ECT Act 25 of 2002 is based on a resolution adopted by the General Assembly of the United Nations Commission on International Trade Law (UNCITRAL) regarding electronic commerce, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, with additional article 5 bis as adopted in 1998 (UNCITRAL Model Law on Electronic Commerce or Model Law).[99] As one of sixty member states of UNCITRAL South Africa as with other "implementing states", aims to give effect to the Model Law by enacting the ECT Act 25 of 2002 based on the Model Law.[100] According to its preamble, the Act endeavours to facilitate and regulate electronic communications and transactions, as well as to promote universal access to electronic communications and transactions. Section 3 of the Act provides as follows:

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

6.4 A key object of the Act is "legal certainty and confidence in respect of electronic communications and transactions".[101] The Act creates legal certainty on issues such as the validity and enforceability of electronic contracts, the time and place of contract information, and formalities such as writing and signature. Section 4 sets out the *sphere of application* of the Act which states: "this Act applies in respect of any electronic transaction or data message".[102]

---

[99] UNCITRAL is a subsidiary of the General Assembly of the United Nations (http://www.uncitral.org). The resolution in the first instance recommended that all States gives favourable consideration to the Model Law in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communicating and storing information. Secondly, it encouraged efforts to popularise the Model Law and its Guide (General Assembly Resolution 85th Plenary Meeting 16/12/96).

[100] M Reimann *Comparative Law and Private International Law* in *The Oxford Handbook of Comparative Law* (2006) 1388. The ECT Act 25 of 2002 therefore has much in common with the following statutes which are also based upon the Model law: (1) Australia's Electronic Transactions Act of 1999; (2) Bermuda's Electronic Transactions Act of 1999; (3) Canada's Uniform Electronic Commerce Act of 1999; (4) Mauritius' Electronic Transactions Act of 2000; (5) The Philippines Electronic Communications Act of 2000; (6) Singapore's Electronic Transactions Act 25 of 1998; and (7) The United States of America's Uniform Electronic Transactions Act 25 of 1999.

[101] S 2(e).

[102] For transactions not covered by the ECT Act 25 of 2002, see section 4(3) and (4) and schedules 1 and 2.

6.5 Chapter 3 specifically deals with facilitating electronic transactions. Part 1 of this chapter sets out the legal requirements for data messages.[103] While the Model Law applies only to commercial matters,[104] the ECT Act 25 of 2002 does not expressly limit the provisions of the Act, including chapter three, facilitating electronic transactions, to commercial matters only—in the absence of other legislation governing admissibility, such interpretation would create a substantial gap in South African law.[105]

2. THE ECT ACT 25 OF 2002—QUESTION FOR COMMENT

- **Adequacy of the ECT Act 25 of 2002 to govern use and admissibility of electronic evidence in criminal and civil proceedings: -**

  Given that the Act, including the approach of evidence provisions in section 15, is largely based on an electronic commerce Model law (that only applies to commercial activities),[106] should the evidence provisions relating to the use and admissibility of electronic evidence in criminal and civil proceedings be regulated outside the provisions of the ECT Act 25 of 2002?

-o-

[103] Generally, see J Coetzee 'Incoterms, Electronic Data Interchange, and Electronic Communications and Transactions Act' (2003) 15 SA Merc LJ 1 and J Coetzee 'The Electronic Communications and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 Stell LR 501.

[104] Art 1, UNCITRAL Model Law on Electronic Commerce: "This Law applies to any kind of information in the form of a data message used in the context of commercial activities". In effect, art 9 on evidence (equivalent chapter 3 in ECT Act 25 of 2002) does not apply to non-commercial or criminal matters.

[105] See J Hofman 'South Africa' in S Mason *Electronic Evidence: Disclosure, Discovery & Admissibility* (LexisNexis Butterworths: London 2007) 459-485. Note: footnote *** of the Model expressly allows implementing States to "extend the applicability of this Law [beyond commercial matters]".

[106] The long title of the ECT 25 of 2002 provides as follows: "To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMME's [small, medium and micro-enterprises]; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith".

Definitions

6.6 While "electronic evidence" and "digital evidence" are often considered interchangeable, an important distinction lies between *analogue* and *digital*:

> Examples of evidence obtained from analogue devices include vinyl records, audio tape, photographic film and telephone calls made of the public switched telephone network. Analogue systems or products generate evidence in the form of data that is capable of being produced in a permanent form. … Examples of digital data include anything that has been created or stored on a computer[107] or is made available by way of the Internet, including CDs, DVDs, MP3s and digital broadcast radio.[108]

6.7 Casey's definition of "digital evidence" which specifically relates to crime proffers the following: "any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi".[109] Casey's definition assumes that the word 'computer' is to be interpreted as widely as possibly to include a device of any form that stores, manipulates and stores data.[110] It is clear that the definition specifically applies to criminal investigations and not digital evidence in general.[111]

6.8 Mason, on the other hand, offers an all-encompassing definition of "electronic evidence" that includes both criminal and civil proceedings: "data (comprising the output of analogue devices or data in digital format) that is created, manipulated, stored or communicate by any device, computer or computer system or transmitted over a communication system that is relevant to the process of adjudication".[112] Comprising of three elements, the definition intends to (1) include all forms of evidence that is created, manipulated or stored in a product (in its widest meaning, considered a computer); (2) include the various forms of device by which data can be stored or transmitted, including analogue devices that produce an output; and (3) restrict the data to information that is relevant to an adjudication. [113]

---

[107] "Computer" is defined in the now repealed Computer Evidence Act 57 of 1983 as" "any device or apparatus, whether commonly called a computer or not, which by electronic, electro-mechanical, mechanical or other means is capable of receiving or absorbing data and instructions supplied to it, of processing such data according to mathematical or logical rules and in compliance with such instructions, of storing such data before or after such processing, and of producing information derived from such data as a result of processing".
[108] Mason (n 21) 2.01.
[109] See Casey (n 18) 12. See also Collier (n 57) 410.
[110] Mason (n 21) 2.03.
[111] Ibid.
[112] Ibid.
[113] Ibid.

6.9 Based on article 2 of the Model Law, the ECT Act 25 of 2002 refers to and defines "data" and "data messages" rather than "electronic evidence" or "digital evidence". In terms of section 12(a) and (b) of the Act, a data message is treated as a document or information in writing it if is accessible or usable for subsequent reference. The Act moves beyond the concept of electronic evidence as regular printouts from a computer.

6.10 However, the ECT Act 25 of 2002 differs from the definition in the Model Law by substituting its own examples of a data message. In terms of article 2 of the Model Law:

> "*data message* means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy".[114]

6.11 In terms of section 1 of the ECT Act 25 of 2002:

> 'data' means electronic representations of information in any form
> 'data' message' means data generated, sent, received or stored by electronic means and includes—
>
> a. voice, where the voice is used in an automated transaction; and
> b. a stored record.

6.12 A difficulty with the Act's definition of 'data message' refers to subsection (a) and is seen as problematic for the following reasons:

> [I]f taken as a deliberate change to the wording of the Model Law meaning that the recording of a voice outside of an automated transaction is not a data message. This would make it difficult for anyone doing business by voice to comply with legislation that required a written record of a transaction. It would also override the existing interpretation of section 3 of the Interpretation Act 33 of 1957[115] which has included voice in the definition of writing.[116]

---

[114] In Part II of the Model Law *Article-by-Article Remarks* [30] it is stated: "The notion of 'data message' is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication". At [31], it is further stated: "The aim of the definition of 'data message' is to encompass all types of messages that are generated, stored or communication in essentially paperless form. For that purpose, all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means list in the definition are intended to be covered by the reference to "similar means", although, for example, "electronic" and "optical" means of communication might not be, strictly speaking, similar. For the purposes f the Model Law, the word "similar" connotes "functionally equivalent".

[115] Section 3 of the Interpretation Act 33 of 1957—"Interpretation of expressions relating to writing: In every law expressions relating to writing shall, unless the contrary intention

6.13 The ECT Act 25 of 2002 also does not provide any clarity as to what is precisely meant by "electronic". While the Act provides that in legal proceedings courts should not deny the admissibility of data messages, because they are not original,[117] it does not define what is meant by "copy" or "original" in an electronic environment.

3. DEFINITIONS— QUESTIONS FOR COMMENT

- **Should the current definition of "data message" in the Act be revised?**
- **For the purposes of consistency and clarity, should the ECT Act 25 of 2002 or other legislation relevant to admissibility of electronic evidence in court proceedings include definitions of "electronic", "copy" and "original"?**

-o-

Interpretation of the ECT Act 25 of 2002

6.14 Section 3 of the ECT Act 25 of 2002, dealing with the interpretation of the Act, makes clear that the adoption of the Act must not be interpreted to exclude any statutory law or the common law principles applicable to recognising or accommodating electronic transactions, data messages or any other matter provided for in this Act and that will still apply.

Sphere of Application

6.15 Section 4 of the ECT 25 of 2002 specifically excludes some transactions from the operation of the Act.[118] In relation to these excluded transactions, insofar as the Act applies "an electronic document does not satisfy the requirement of writing and

---

appears, be construed as including also references to typewriting, lithography, photography and all other modes of representing or reproducing words in visible form".

[116] Hofman (n 105) 15.07.

[117] Sections 11 and 15.

[118] See J Hofman 'The Meaning of Exclusions in section 4 of the Electronic Communications and Transactions Act 25 of 2002' 2007 SALJ 262. See also MC Wood-Bodley 'Wills, Data Messages, and the Electronic Communications and Transactions Act' 2004 SALJ 526.

an advanced electronic signature does not satisfy the requirement of signature",[119] advanced or otherwise. Section 4(3) specifically excludes the application of the sections of the ECT Act mentioned in Column B to the laws mentioned in Column A of Schedule 1 as follows:

Schedule 1

Item	Column A	Column
1.	Wills Act, 1953 (Act 7 of 1953)	11, 12, 13, 14, 15, 16, 18, 19 and 20
2.	Alienation of Land Act, 1981 (Act 68 of 1981)	12 and 13
3.	Bills of Exchange Act, 1964 (Act 34 of 1964)	12 and 13
4.	Stamp Duties Act, 1968 (Act 77 of 1968)	11, 12, 14

6.16 Section 4(4) provides as follows: "[t]his Act must not be construed as giving validity to any transaction mentioned in Schedule 2" as follows:

Schedule 2

1.	An agreement for alienation of immovable property as provided for in the Alienation of Land Act, 1981 (Act 68 of 1981)
2.	An agreement for the long-term lease of immovable property in excess of 20 years as provided for in the Alienation of Land Act, 1981 (Act 68 of 1981)
3.	The execution, retention and presentation of a will of codicil as defined in the Wills Act, (Act 7 of 1953)
4.	The execution of a bill of exchange as defined in the Bills of Exchange Act, 1964 (Act 34 of 1964)

6.17 Section 4(5) further stipulates that the Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages.

[119] Hofman (n 118) 262.

4. SPHERE OF APPLICATION—QUESTIONS FOR COMMENT

- **In view of technological developments, should the ECT Act 25 of 2002 be amended to extend its sphere of application to the laws mentioned in Column A of Schedule 1, specifically including the excluded transactions mentioned in Schedule 2?**

-o-

Common law position on electronic contracts[120]

6.18 Prior to the enactment of the ECT Act 25 of 2002, there are no reported cases specifically dealing with the formation of a contract via the interchange of electronic mail.[121] In *Balzan v O'Hara and others*,[122] the court was concerned with whether a telegram could constitute "written authority" with the meaning of 1 (1) of Act 68 of 1957 (Land Alienation Act). Coleman J held that a telegram could constitute "written authority" within the meaning of the section which required a sale of land to be reduced to writing and signed by the parties or their agents acting on their written authority, but only if the contract which the agents conclude is one which they are thereby authorised to conclude.

6.19 Arguably, expressions relating to writing to include electronic email could be read into section 3 of the Interpretation Act 53 of 1957 which provides: "In every law expressions relating to writing shall, unless the contrary intention appears, be construed as including also references to typewriting, lithography, photography and *all other modes of representing or reproducing words in visible form*".

6.20 The ECT Act 25 of 2002 now contains comprehensive provisions facilitating electronic transactions with legal recognition of "data messages" including definitions of "writing" and "signature" in their application to electronic transacting.

---

[120] See SL Snail 'Demystifying Electronic Signatures in South Africa – A Global Overview' paper presented at 4th Annual South African Cyberlaw Conference, Pretoria October 2009.
[121] However, see *Council for Scientific and Industrial Research v Fijen* 1996(2) SA (A).
[122] 1964(3) SA (T) 1.

Legal recognition of data messages

6.21 Similarly following Article 11 of the UNCITRAL Model Law on Electronic Commerce and Article 8 of the United Nations Convention on the Use of Electronic Communications in International Contracts, section 11 of the ECT Act 25 of 2002 provides for the legal recognition of data messages as follows:

> 11 Legal recognition of data messages
> (1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.
> (2) Information is not without legal force and effect merely on the grounds that it is not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.
> (3) Information incorporated into an agreement and that is not in the public domain is regarded as having been incorporated into a data message if such information is-
> (a) referred to in a way in which a reasonable person would have noticed the reference thereto and incorporation thereof; and
> (b) accessible in a form in which it may be read, stored and retrieved by the other party, whether electronically or as a computer printout as long as such information is reasonably capable of being reduced to electronic form by the party incorporating it.

Writing

6.22 Similar to Article 6(1) of UNCITRAL Model Law on Electronic Commerce and Article 9 of the United Nations Convention on the Use of Electronic Communications in International Contracts that recognises data as the functional equivalent of writing or evidence in writing, section 12 of the ECT Act 25 of 2002 guarantees data messages legal validity equal to messages written on paper:[123]

> 12 Writing
> A requirement in law that a document or information must be in writing is met if the document or information is-
> (a) in the form of a data message; and
> (b) accessible in a manner usable for subsequent reference.

[123] Section 22(1) on the formation and validity of agreements further provides:
> (1) An agreement is not without legal force and effect merely because it was concluded partly or in whole by means of a data message.
> (2) An agreement concluded between parties by means of data messages is concluded at the time when and place where the acceptance of the offer was received by the offeror.

Signature

6.23 Section 13 of the ECT Act 25 of 2002 similarly follows Article 7(1) of the UNCITRAL Model Law on Electronic Commerce and Article 9 of the United Nations Convention on the Use of Electronic Communications in International Contracts, which ensures that data messages can satisfy the signature requirement by providing:

> 13 Signature
> (1) Where the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.
> (2) Subject to subsection (1), an electronic signature is not without legal force and effect merely on the grounds that it is in electronic form.
> (3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if-
> (a) a method is used to identify the person and to indicate the person's approval of the information communicated; and
> (b) having regard to all the relevant circumstances at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated.
> (4) Where an advanced electronic signature has been used, such signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.
> (5) Where an electronic signature is not required by the parties to an electronic transaction, an expression of intent or other statement is not without legal force and effect merely on the grounds that-
> (a) it is in the form of a data message; or
> (b) it is not evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.

6.24 In terms of the wording of section 13(1), *advanced* electronic signatures are the only means of validating electronic transacting where such signature is required by law. “Advanced electronic signature” is defined as “an electronic signature which results from a process which has been accredited by the Authority as provided for in section 37”.[124] Accreditation in terms of section 38, is necessary to authenticate an *advanced* electronic signature. “Electronic signature” is defined as “data attached to, incorporated in, or logically associated with other data and which is intended by the use to serve as a signature”.[125] Sections 33-41 provide for the creation of an *Accreditation Authority*. In terms of section 37:

---

[124] S 1, ECT Act 25 of 2002.
[125] Ibid.

> 37 Accreditation of authentication products and services
> (1) The Accreditation Authority may accredit authentication products and services in support of advanced electronic signatures.
> (2) An application for accreditation must-
> (a) be made to the Accreditation Authority in the prescribed manner supported by the prescribed information; and
> (b) be accompanied by a non-refundable prescribed fee.
> (3) A person falsely holding out its products or services to be accredited by the Accreditation Authority is guilty of an offence.

6.25 Section 13 differentiates between *advanced* electronic signatures and electronic signatures. In terms of its scope and applicability, three contractual situations arise depending on the nature of the signature.[126] The first situation as set out in section 13(5) is where parties to an electronic transaction do not require a signature:

> The absence of an "electronic signature" in this instance does not invalidate the expression of intent or other statement merely because the expression of intent is in the form of a data message or is not evidenced by an "electronic signature". Relevant exampled of where an agreement could be formed without the use of a signature is by shrink-wrap and click-wrap agreements. Shrink wrap agreement are the terms and conditions that accompany software distributed in computer stores or other or other retail outlets normally. Click-wrap agreements are online agreements structured in such a way that visitors to a web site attempting to download programs offered by a vendor are required affirmatively to agree to the contractual terms and conditions of the vendor by clicking an icon that usually states 'I agree' or 'I accept' [127]

6.26 Section 13(3) sets out the second situation where an "electronic signature is required by the parties to an electronic transaction", however, the parties have not agreed on the type of electronic signature to be used. In this instance, any electronic signature or distinct electronic mark would be sufficient and acceptable for the existence of an electronic transaction between the parties.[128] The third contractual situation, referred earlier, is set out in section 13(1) which prescribes that where the law requires a signature, and the law does not specify the type of signature, such signature in its electronic format must be an *advanced* electronic signature [by definition to be provided by the South African Department of Communications, although the structure of the accreditation authority as required by the Act is yet to come into operation].

---

[126] D De Andrade 'Is the Pen Mightier than the Electronic Signature' <http://www.derebus.org.za/nxt/gateway.dll/bsxha/uei9/7okka/eqkka/svbua> (30 October 2009).
[127] Ibid.
[128] Ibid. See also SL Snail 'Electronic Contracts in South Africa—A Comparative Analysis' JILT 2008(2) <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2008_2/snail/> (30 October 2009).

6.27 Section 18 further provides:

> (1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the advanced electronic signature of the person authorised to perform those acts is attached thereto, incorporated in or logically associated with the electronic signature or data message.

6.28 As the establishment and development of an authorised accreditation authority is yet to take place, it remains doubtful whether provisions for advanced electronic signatures in section 13(1) and (4) read together, apply to international signatures not accredited by a South African accreditation authority.[129]

5. SIGNATURE—QUESTIONS FOR COMMENT

- **Section 13**
  - **Having regard to the provisions of sections 33-41 of the Act which govern the establishment and functions of a national accreditation authority *coupled* with the definition of "advanced electronic signature" in section 1 of the Act, will internationally accepted and widely used electronic signatures, not accredited by national authorities obtain legal status provided for in section 13(4) of the Act?[130]**
  - **Should the distinction between "advanced electronic signature" and "electronic signature" as used in the ordinary sense be abolished?**
- **Biometric Technology**
  - **In view of developments in biometric technology, should physiological features of biometrics (such as, but not limited to, fingerprints, iris recognition, hand and palm geometry) be included in the ECT Act 25 of 2002 as a form of assent and electronic identity?**

-o-

[129] While the process has begun and the South African Accreditation Authority has implemented *Accreditation Regulations of 2007* (*GG* 2995 of 20 June of 2007 (Reg Gaz 8701)), the intended foreign recognition policy is not yet available. See South African Accreditation Authority <http://www.saaa.gov.za/policy.htm#> (10 February 2010).
[130] De Andrade (n 126).

The concept of "original" revisited

6.29 In the absence of specific evidence, if an "original" and a copy of it are presented as identical in every respect, it will be impossible to distinguish which was produced first. While this may not create much concern with documents in a physical format which can be stored and retrieved as it was originally created, documents in an electronic medium may be transferred to another storage media or migrated to another form of software causing the data to undergo changes.

6.30 The ECT Act 25 of 2002, in accordance with the Model Law on electronic commerce, is based upon the principle of functional equivalence:

> Functional equivalence, or media neutrality, means that the law should treat paper-based and electronic transactions in the same way, without prejudicing either or favouring one above the other".[131]

6.31 Section 14 introduces the principle of functional equivalence by requiring: (i) that the integrity of the information must be assessed by considering whether it is complete and unaltered, and the purpose for which it is generated;[132] and (ii), that the information is capable of being displayed or produced to the person to whom it is to be presented.[133]

6.32 Thus, where the law requires information to be presented or retained in its original form, the requirement of "originality" will be satisfied if one has a document which originated from a computer and is now capable of being produced, either in electronic or paper format. It is also clear that section 14 will cover situations where a paper document is reduced to electronic format for storage purposes.[134]

Admissibility and evidential weight of data messages

6.33 Section 15, of the ECT Act 25 of 2002, dealing with admissibility and evidential weight of data messages requires special scrutiny. The scope and

---

[131] W Jacobs 'The Electronic Communications and Transactions Act: Consumer Protection and Internet Contracts' 2004 SA Merc LJ 556, 557.
[132] S 14(2)(a) and (b).
[133] S 14(1)(a) and (b).
[134] For a general discussion, see Coetzee (n 103) 512.

meaning of its provisions remain uncertain.[135] The purpose of the section is two-fold, namely to establish: (i) the admissibility of data messages as evidence in legal proceedings; and (ii) the evidential value of data messages. Section 15 provides:[136]

> 15 Admissibility and evidential weight of data messages
> (1) In any legal proceedings, the rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence-
> (a) on the mere grounds that it is constituted by a data message; or
> (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
> (2) Information in the form of a data message must be given due evidential weight.
> (3) In assessing the evidential weight of a data message, regard must be had to-
> (a) the reliability of the manner in which the data message was generated, stored or communicated;
> (b) the reliability of the manner in which the integrity of the data message was maintained;
> (c) the manner in which its originator was identified; and
> (d) any other relevant factor.
> (4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on the mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with the rules against hearsay:-**
  - **Should section 15 prescribe that a data message is automatically admissible as evidence in terms of section 15(2) and a court's discretion merely relates to an assessment of evidential weight based on the factors enumerated in section 15(3)?[137]**

---

[135] See discussion by DT Zeffertt, P Paizes and A St Q Skeen *The South African Law of Evidence* (LexisNexis Butterworths Durban 2003) 393-395.

[136] Cf section 3(1) of the Computer Evidence Act which provided that an "authenticated computer print-out [was] admissible on its production as evidence of any fact recoded in it of which direct oral evidence would be admissible".

[137] See *S v Ndiki and others* 2008 (2) SACR 252 (Ck).

- **Should a "data message" constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act 45 of 1988?**[138]
  - **If yes, does section 15(1) therefore make all data messages, including hearsay data, admissible? In doing so, should section 15 of the ECT Act 25 of 2002 exempt a data message from the rules relating to hearsay evidence in terms of section 3 of the Law of Evidence Amendment Act 45 of 1988?**
  - **If not, should section 3 of the Law of Evidence Amendment Act prescribe a rule of admissibility for hearsay representations made by a person via the mechanical agency of a machine?**

- **Section 15 interaction with other statutory exceptions:-**
  - **What is the effect of section 15(1) on other statutory exceptions such as section 221 (admissibility of certain trade or business records) and section 222 (application to criminal proceedings of certain provisions of Civil Proceedings Evidence Act 25 of 1965) of the Criminal Procedure Act; AND Part VI (documentary evidence) of the Civil Proceedings Evidence Act 25 of 1965?**

-o-

Case law after the ECT Act 25 of 2002

Section 15: Two types of evidence?

6.34 Although adopting different approaches, two courts have interpreted section 15 as distinguishing between two types of evidence: (i) *hearsay* computer evidence; and (ii) *real* computer evidence.

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

6.35 In an obiter statement in *Ndlovu v Minister of Correctional Services and another*,[139] Gautschi AJ states:

[138] See Zeffertt et al (n 135) 393-395.
[139] [2006] 4 All SA 165 (W).

> Where the probative value of the information in a data message depends upon the credibility of a (natural) person other than the person giving evidence, there is no reason to suppose that section 15 seeks to override the normal rules applying to hearsay evidence. On the other hand, where the probative value of the evidence depends upon the "credibility" of the computer (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.[140]

***S v Ndiki and others* 2008 (2) SACR 252 (Ck)**

6.36 In *S v Ndiki and others*,[141] Van Zyl J states:

> As I shall attempt to show when I deal with the provisions of the Law of Evidence Amendment Act 45 of 1988, computer evidence which falls within the definition of hearsay evidence in s 3 thereof may become admissible in terms of the provisions of that Act. Evidence 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 given thereto (ss (3)). The ECT Act 25 of 2002 is therefore inclusionary as opposed to exclusionary.

7. Section 15: Two Types of Evidence—QUESTION FOR COMMENT

- **For the purposes of facilitating admissibility of data messages, should the ECT Act 25 of 2002 (or other relevant legislation) make a clear distinction between *mechanically produced evidence without the intervention of the human mind* (akin to real evidence) AND *mechanically produced evidence with the intervention of the human mind* (hearsay)?**
- **If so, should a free-standing provision prescribe that representations made by machines, based on information supplied by a person, is only admissible if the information is proved accurate?**
- **In an obiter statement in *Ndiki* Van Zyl J states, "a more preferable approach to computer generated evidence" is to extend the meaning of hearsay to include evidence that depends upon the accuracy of the machine which would do "away with the necessity to distinguish in each**

[140] Ibid, 173 (emphasis added).
[141] 2008 (2) SACR 252 (Ck).

case between what would constitute hearsay evidence and what real evidence".[142] Is such an approach practicable? Should provision be made in the ECT Act 25 of 2002 for such an approach?

-o-

Assessing the evidential weight of a data message

6.37 In terms of section 15(3), the following factors must be taken into account in determining the weight to be attached to a data message:

(a) the reliability of the manner in which the data message was generated, stored or communicated;
(b) the reliability of the manner in which the integrity of the data message was maintained;
(c) the manner in which its originator was identified; and
(d) any other relevant factor.

8. ASSESSING THE EVIDENTIAL WEIGHT OF A DATA MESSAGE—QUESTIONS FOR COMMENT

- **In view of the fragmented nature of case law focusing on authentication of specific types of evidence, is a review of the principle of authentication necessary in view of the nature and characteristics of electronic evidence that raise legitimate concerns about its accuracy and authenticity?**
- **While section 15(3) provides guidelines for assessing the evidential weight of data messages, should courts apply a higher admissibility hurdle in the context of authentication (as an aspect of relevance) for electronic evidence than for other forms of tangible evidence?**
- **Given the concerns raised in chapter 2, what standard of proof, applicable to the authentication of evidence, is necessary, if at all? Will a prima facie showing (in a sufficiency sense) that the evidence is what it purports to represent suffice? Or should conclusive evidence of authenticity (again as an aspect of relevance) be required?**

-o-

[142] Ibid at [33].

Section 15(4)—Admissibility of business records

6.38 Section 15(4) creates a general exception to the rule against hearsay for any data message made *in the ordinary course of business*. It provides for the admissibility of business records as follows:

> (4) A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on the mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

6.39 In *Ndlovu*,[143] Gautschi AJ takes the view that s 15(4) provides for two situations in which a data message may on its mere production be admissible in evidence as follows:

> The first is "a data message made by a person in the ordinary course of business", which, juxtaposed, with the words that follow, clearly refers to an original data message, and is required to have been made "in the ordinary course of business". The second is a copy or printout of or an extract from such data message which is certified to be correct by an officer in the service of such person (being 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 facts contained therein. Section 15(4) appears to be self-contained, and does not admit of or require a qualitative enquiry to be made in terms of section 15(2) or (3) in regard to the weight to be attached thereto. It provides for its own weight, namely that the facts contained therein will be rebuttable proof, ie if not rebutted, then they will stand as evidence.

6.40 While section 15 is based on the UNCITRAL Model Law on Electronic Commerce, section 15(4) is South Africa's departure from the Model Law. Hofman argues that by creating such a broad exception to the rules for the admissibility of data messages, section 15(4) goes against the functional equivalence approach that should apply between data messages and written documents as advocated in the UNCITRAL Model Law on Electronic Commerce.[144] Section 15(4) is considered "problematic for a number of reasons, including the sheer scope of the data

---

[143] *Ndlovu v Minister of Correctional Services and another* [2006] 4 All SA 165 (W) at 172-3.
[144] Hofman (n 105) 15.26

messages made *in the ordinary course of business* that may now constitute rebuttable proof on mere production".[145]

6.41 Hofman questions the meaning and constitutionality of section 15(4) and in particular highlights the following six main difficulties with the way the section is worded:

(a) First, an exception for communications made 'in the ordinary course of business' is much wider that 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.
(b) 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.
(c) 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.
(d) 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.
(e) 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.
(f) 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.[146]

9. ADMISSIBILITY OF BUSINESS RECORDS—QUESTION FOR COMMENT

- **Should section 15(4) be reviewed to give a restrictive interpretation to the words "in the ordinary course of business"?**
- **Should section 15(4) as applicable in criminal cases be reviewed in view of the current law on reverse onus provisions?**

[145] Collier (n 57) 416-7.
[146] Hofman (n 105) 15.26 [footnotes omitted].

-o-

Presumptions

6.42 The ECT Act 25 of 2002 creates two presumptions in favour of the accuracy of data messages: (i) presumption in favour of the accuracy of business records;[147] and (ii) presumption in favour of advanced electronic signatures.[148]

10. PRESUMPTIONS—QUESTION FOR COMMENT

- **The presumption of regularity expressed in the maxim *omnia praesumuntur rite esse acta*, described by Stephen Brown LJ in *Castle v Cross* [1984] 1 WLR 1372 (QBD) as: "In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time".**
    - **Should the law of evidence prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breathe testing devices)?**

-o-

In general

6.43 In the Commission's *Report on the Preliminary Investigation into the Review of the Rules of Evidence*[149] and in Issue Paper 26 *General Overview of the Rules of Evidence and Possible Areas for Reform*,[150] chapters dealing with the general overview of the rules of evidence identified issues relating to electronic evidence as part of preliminary research study and intended to form the basis of future research and discussion.[151] Issue Paper 26 posed the following question for comment[152] and repeated for consideration for the purposes of this Issue Paper.

---

[147] S 15(4). See Hofman (n 105) at [15.26] for a discussion of this presumption, including concerns about the constitutionality of section 15(4).
[148] S 13.
[149] Project 126, June 2002.
[150] Project 126, January 2008.
[151] South African Law Reform Commission Report, *Preliminary Investigation into the Review of the Rules of Evidence*, Project 126, June 2002.

11. IN GENERAL: QUESTION FOR COMMENT

Are the provisions in the Electronic Communications Act sufficient to regulate the admissibility of computer generated evidence?

[152] At page 35. By the closing date of 31 March 2009 for comment and input on Issue Paper 26, only three of the nineteen comments received specifically addressed the issue of computer evidence.

CHAPTER SEVEN

CONCLUSION AND SUMMARY FOR COMMENT

7.1 This Issue Paper has attempted to draw attention to issues for law reform with regard to matters relating to admissibility of electronic evidence in criminal and civil proceedings. In relation to the longer term objectives, this preliminary research paper has set out to identify shortcomings in the evidential provisions of the ECT Act 25 of 2002 and to define possible scope for further investigation.

7.2 While significant steps have been taken to facilitate the use of electronic evidence in court proceedings, the preceding chapters indicates that much can be done to clarify and simplify the rules of evidence in bridging the technology/law divide. Given the proliferation of technology, the unavoidable future for the courts is the use of technology, whether this involves the use of hash algorithms or metadata as proof of authenticity or the use of digital reconstruction technology as a means of presenting evidence or as a means of proving substantive facts in a case. Given the existence of electronic data in various formats and applications, there is clearly no “one-size-fits-all” approach that will work in all instances.

7.3 The Commission therefore invites all interested parties and role players to identify any other issues not raised in the Issue Paper which should be considered for reform in criminal and civil proceedings. This information will prove valuable in its consideration of the reform of the rules of evidence and further planning of the project.

7.4 For ease of reference, the Commission provides a summary of questions raised in this Issue Paper for comment and input as follows.

QUESTIONS FOR COMMENT

1. BRIDGING THE TECHNOLOGY/LAW DIVIDE—QUESTION FOR COMMENT

- **Should the ECT Act 25 of 2002 be reviewed on a regular basis to take account of advances in technology?**
    - **If so, what should such a review entail?**
    - **When/how often should such a review take place?**
    - **Who should undertake the review?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

2. THE ECT ACT 25 OF 2002—QUESTION FOR COMMENT

- **Adequacy of the ECT Act 25 of 2002 to govern use and admissibility of electronic evidence in criminal and criminal proceedings: -**

  Given that the Act, including the approach of evidence provisions in section 15, is largely based on an electronic commerce Model law (that only applies to commercial activities), should the evidence provisions relating to the use and admissibility of electronic evidence in criminal and civil proceedings be regulated outside the provisions of the ECT Act 25 of 2002?

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

3. DEFINITIONS— QUESTIONS FOR COMMENT

- **Should the current definition of "data message" in the Act be revised?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

3. DEFINITIONS— QUESTIONS FOR COMMENT

- **For the purposes of consistency and clarity, should the ECT Act 25 of 2002 or other legislation relevant to admissibility of electronic evidence in criminal proceedings include a definition of "electronic", "copy" AND "original"?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

4. SPHERE OF APPLICATION—QUESTIONS FOR COMMENT

- **In view of technological developments, should the ECT Act 25 of 2002 be amended to extend its sphere of application to the laws mentioned in Column A of Schedule 1, specifically including the excluded transactions mentioned in Schedule 2?**

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

…………………………………………………………………………

5. SIGNATURE—QUESTIONS FOR COMMENT

- **Section 13**
  - **Having regard to the provisions of sections 33-41 of the Act which govern the establishment and functions of a national accreditation authority *coupled* with the definition of "advanced electronic signature" in section 1 of the Act, will internationally accepted and widely used electronic signatures, not accredited by national authorities obtain legal status provided for in section 13(4) of the Act?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

5. SIGNATURE—QUESTIONS FOR COMMENT

- **Section 13**
  - **Should the distinction between "advanced electronic signature" and "electronic signature" as used in the ordinary sense be abolished?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

5. SIGNATURE—QUESTIONS FOR COMMENT

- **Biometric Technology**
  - **In view of developments in biometric technology, should physiological features of biometrics (such as, but not limited to, fingerprint, iris recognition, hand and palm geometry) be included in the ECT Act 25 of 2002 as a form of assent and electronic identity?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with the rules against hearsay:-**
    - **Should section 15 prescribe that a data message is automatically admissible as evidence in terms of section 15(2) and a court's discretion merely relates to an assessment of evidential weight based on the factors enumerated in section 15(3)?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with the rules against hearsay:-**
    - **Should a "data message" constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act 45 of 1988?**

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with the rules against hearsay:-**
  - **If yes, does section 15(1) therefore make all data messages, including hearsay data, admissible? In doing so, should section 15 of the ECT Act 25 of 2002 exempt a data message from the rules relating to hearsay evidence in terms of section 3 of the Law of Evidence Amendment Act 45 of 1988?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with the rules against hearsay:-**
  - **If not, should section 3 of the Law of Evidence Amendment Act prescribe a rule of admissibility for hearsay representations made by a person via the mechanical agency of a machine?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

6. ADMISSIBILITY OF DATA MESSAGES AS EVIDENCE IN LEGAL PROCEEDINGS—QUESTIONS FOR COMMENT

- **Section 15 interaction with other statutory exceptions:-**
    - **What is the effect of section 15(1) on other statutory exceptions such as section 221 (admissibility of certain trade or business records) and section 222 (application to criminal proceedings of certain provisions of Civil Proceedings Evidence Act 25 of 1965) of the Criminal Procedure Act; AND Part VI (documentary evidence) of the Civil Proceedings Evidence Act 25 of 1965?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

7. Section 15: Two Types of Evidence—QUESTION FOR COMMENT

- **For the purposes of facilitating admissibility of data messages, should the ECT Act 25 of 2002 (or other relevant legislation) make a clear distinction between *mechanically produced evidence without the intervention of the human mind* (akin to real evidence) AND *mechanically produced evidence with the intervention of the human mind* (hearsay)?**

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

7. Section 15: Two Types of Evidence—QUESTION FOR COMMENT

- **If so, should a free-standing provision prescribe that representations made by machines, based on information supplied by a person, is only admissible if the information is proved accurate?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

7. Section 15: Two Types of Evidence—QUESTION FOR COMMENT

- **According to Van Zyl J in *Ndiki*, "a more preferable approach to computer generated evidence" is to extend the meaning of hearsay to include evidence that depends upon the accuracy of the machine which would do "away with the necessity to distinguish in each case between what would constitute hearsay evidence and what real evidence". Is such an approach practicable? Should provision be made in the ECT Act 25 of 2002 for such an approach**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

8. ASSESSING THE EVIDENTIAL WEIGHT OF A DATA MESSAGE—QUESTIONS FOR COMMENT

- **In view of the fragmented nature of case law focusing on authentication of specific types of evidence, is a review of the principle of authentication necessary in view of the nature and characteristics of electronic evidence that raise legitimate concerns about its accuracy and authenticity?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

8. ASSESSING THE EVIDENTIAL WEIGHT OF A DATA MESSAGE—QUESTIONS FOR COMMENT

- **While section 15(3) provides guidelines for assessing the evidential weight of data messages, should courts apply a higher admissibility hurdle in the context of authentication (as an aspect of relevance) for electronic evidence than for other forms of tangible evidence?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

8. ASSESSING THE EVIDENTIAL WEIGHT OF A DATA MESSAGE—QUESTIONS FOR COMMENT

- **Given the concerns raised in chapter 2, what standard of proof, applicable to the authentication of evidence, is necessary, if at all? Will a prima facie showing (in a sufficiency sense) that the evidence is what it purports to represent suffice? Or should conclusive evidence of authenticity (again as an aspect of relevance) be required?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

9. ADMISSIBILITY OF BUSINESS RECORDS—QUESTION FOR COMMENT

- **Should section 15(4) be reviewed to give a restrictive interpretation to the words "in the ordinary course of business"?**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

9. ADMISSIBILITY OF BUSINESS RECORDS—QUESTION FOR COMMENT

- **Should section 15(4) as applicable in criminal cases be reviewed in view of the current law on reverse onus provisions?**

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

10. PRESUMPTIONS—QUESTION FOR COMMENT

- **The presumption of regularity expressed in the maxim *omnia praesumuntur rite esse acta*, described by Stephen Brown LJ in *Castle v Cross* [1984] 1 WLR 1372 (QBD) as: "In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time".**
    - **Should the law of evidence prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breathe testing devices)?**

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

11. IN GENERAL: QUESTION FOR COMMENT

- **Are the provisions in the ECT Act 25 of 2002 sufficient to regulate the admissibility of electronic evidence in court proceedings?**

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....