South African Law Reform Commission

REPORT

PROJECT 126

REVIEW OF THE LAW OF EVIDENCE

ISBN: 978-0-621-45389-8

TO ADV T MASUTHA, MINISTER OF JUSTICE AND CORRECTIONAL SERVICES

I am honoured to submit to you in terms of section 7(1) of the South African Law Reform Commission Act, 1973 (Act 19 of 1973), for your consideration the Commission's report on The Review of the Law of Evidence.

JUSTICE J KOLLAPEN

CHAIRPERSON: SA LAW COMMISSION

31 MARCH 2017

ii

Introduction

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

The members of the Commission are -

The Honourable Justice Narandran Kollapen (Chairperson)
Professor Vinodh Jaichand (Member)
Mr Irvin Lawrence (Member)
Advocate Mahlape Sello (Member)
Ms Thina Siwendu (Member)
Professor AW Oguttu
Professor M Carnelley;

The Secretary is Mr TN Matibe. The Commission's offices are located at Spooral Park, 2007 Lenchen Avenue South, Centurion. Correspondence should be addressed to:

The Secretary
South African Law Reform Commission
Private Bag X 668
PRETORIA
0001

Telephone: (012) 622-6313
E-mail: NMatibe@justice.gov.za
Website: *http://www.justice.gov.za/salrc/*

An Advisory Committee on the review of the law of evidence was responsible for the project. The project leader for this project was Judge Narandran Kollapen. The members of the committee are:

The Hounarable Justice Narandran Kollapen (Chairperson)
The Honourable Madam Justice N Mhlantla
The Honourable Madam Justice T Ndita
Professor L Fernandez (University of the Western Cape)
Advocate T Masuku (Private practice)
Professor Tana Pistorius (University of South Africa)

Table of Contents

List of Acronyms

AU	African Union
CA	Certification Authority
CPA	Criminal Procedure Act 51 of 1977
CPEA	Civil Proceedings Evidence Act 25 of 1965
DNA	Deoxyribonucleic acid
DTPS	Department of Telecommunications and Postal Services
e-commerce	electronic commerce
ECT Act	Electronic Communications and Transactions Act 25 of 2002
EDI	electronic data interchange
e-evidence	electronic evidence
eIDAS	EU Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the European internal market.
e-signature	electronic signature
EU	European Union
GUIDEC	General Usage for International Digitally Ensured Commerce
ICC	International Chamber of Commerce
ICT	Information communications technology
ISO	International Standards Authority
ITU	International Telecommunications Union
LEAA	Law of Evidence Amendment Act 45 of 1988

LSSA	Law Society of South Africa
MLES	Model Law on Electronic Signatures
NPA	National Prosecuting Authority
PKI	Public key infrastructure
QES	Qualified Electronic Signatures
SA	South Africa
SAAA	South African Accreditation Authority
SADC	Southern African Development Community
SALRC	South African Law Reform Commission
SMMEs	Small, Medium and Micro Enterprises
UETA	Uniform Electronic Transaction Act
UECA	Uniform Electronic Commerce Act
UNECIC	United Nations Convention for the Use of Electronic Communications in International Contracts, 2005
UN	United Nations
UNCITRAL	United Nations Commission on International Trade Law
US	United States

Bibliography

List of Books

AJ Kerr *The Principles of Law of Contract* 5 ed (1998)

Benjamin Wright, *The Law of Electronic Commerce EDI, Fax and E-Mail: Technology, Proof, and Liability* (1991)

Charles T. Cullen "Authentication of Digital Objects: Lessons from a Historian's Research" in *Authenticity in a Digital Environment* (Council on Library and Information Resources 2000)

David M. Levy "Where's Waldo? Reflections on Copies and Authenticity in a Digital Environment" in *Authenticity in a Digital Environment* (Council on Library and Information Resources 2000)

DP van der Merwe 'Appliances and Devices' in 'Evidence' by CWH Schmidt and DT Zeffert (updated by DP van der Merwe) *LAWSA* (LexisNexis Butterworths 2005) 8.4.

Jeff Rothenberg "Preserving Authentic Digital Information" in *Authenticity in a Digital Environment* (Council on Library and Information Resources 2000)

LH Hoffmann & DT Zeffertt *South African Law of Evidence* 3rd ed (1981) 308-309.

Michael Chissick & Alistair Kelman *Electronic Commerce Law and Practice* 2nd ed (2000)

Peter B. Hirtle "Archival Authenticity in a Digital Age" in *Authenticity in a Digital Environment* (Council on Library and Information Resources 2000)

Ryk Meiring 'Electronic Transactions' *Cyberlaw @ SA II*

Stephen Mason (ed) *International Electronic Evidence* (British Institute of International and Comparative Law (2008)

Stephen Mason, *Electronic Evidence* (3rd edn, LexisNexis Butterworths, 2012)

Stephen Mason, *Electronic Signatures* 4th ed (OBserving Law - the IALS Open Book Service for Law, 2016) available at http://ials.sas.ac.uk/sites/default/files/files/IALS%20Digital/OBserving%20Law/ElectronicSignaturesStephenMason.pdf

Tim Kevan & Paul McGrath, *E-mail, the Internet and the Law Essential Knowledge for Safer Surfing* 2001 (Hertfordshire: EMIS Professional Publishing Ltd)

Toh See Kiat, *Paperless International Trade: Law of Telematic Data Interchange* (1992)

Vivienne Lawack-Davis (*Aspects of Internet Payment Instruments* (unpublished LLD Thesis University of South Africa (2000))

List of Articles

Aashish Srivastava and Michel Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' *African Journal of International and Comparative Law* 21.3 (2013): 427–446.

A J Ebden "Computer evidence in court" (1985) *SALJ* 687

A st Q skeen "Evidence and Computers" (1984) *SALJ* 675

André R van Staden & Christa Rautenbach 'Enkele Gedagtes oor die Behoefte aan en die Toekoms van Elektroniese Testamente' (2006) 39 *De Jure* 586;

Andrew Phang & Daniel Seng, 'The Singapore Electronic Transactions Act 1998 and the proposed art 2b of the Uniform Commercial Code' (1999) 2/7 *International Journal of Law and Information Technology* 103;

Arno R Lodder 'Electronic Contracts and Signatures: National Civil Law in the EU Will Change Drastically Soon', paper delivered at *15th BILETA Conference 'Electronic Datasets and Access to Legal Information',* held on 14 April 2000 at the University of Warwick (available at <http://www.bileta.ac.uk/00papers/lodder.html>).

Assafa Endeshaw, 'Singapore gets to grips with the Internet' (1996) 7/2 *Journal of Law and Information Science* 208

Assafa Endeshaw, 'The Singapore E-commerce 'code' (1998) 3/8 *Information & Communications Technology Law* 189

Christina Hultmark Ramberg 'The E-commerce Directive and Contract Formation in a Comparative Perspective' 22, available at <http://www.juridicum.su.se>.

Christina Hultmark Ramberg, 'The E-Commerce Directive and Formation of Contract in a Comparative Perspective' (2001) 26 *European Law Review* 429

Christoph Glatt, 'Comparative issues in the formation of electronic contracts' (1998) 1/6 *International Journal of Law and Information Technology* 34

Christopher T. Poggi, 'Electronic Commerce Legislation: An Analysis of European and American Approaches to contract formation' 2000 (41) *Va. J. Int'l. L*. 224 272

Dan Puterbaugh 'Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation' March 2016 available at http://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/.

Dana van der Merwe Documentary evidence (with specific reference to hearsay) (1994) Obiter 67

D P van der Merwe Onlangse ontwikkelinge op die raakvlak tussen rekenaars en die reg (1991) 54 *THRHR* 96.

Eiselen “Elektroniese dataverwisseling (EDV) en die bewysreg” (1992) 55 *THRHR* 217

Jane Kaufman Winn & Michael Rhoades Pullen ‘Despatches from the Front: Recent Skirmishes Along the Frontiers of Electronic Contracting Law’ (1999) 55 Business Lawyer 455

J Hofman ‘Electronic Evidence in criminal cases,’ (2006) *SALJ* 257

J T Delport “Die Wet op Rekenaargetuienis” (1983) *Obiter* 140

Katherine S Williams & Indira Mahalingam Carr “The Singapore Computer Misuse Act – Better Protections for the Victims?” (1994) *Journal of Law and Information Science* Vol. 5 No. 2 215

Maria Angela Biasiotti, Mattia Epifani, Fabrizio Turchi ‘The Evidence Project: Bridging the Gap in the Exchange of Digital Evidence across Europe’ available at http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/The-EVIDENCE-Project-Bridging-the-Gap-in-the-Exchange-of-Digital-Evidence-Across-Europe.pdf (accessed 8 August 2016).

Mark Heyink ‘Extracts of comment made on the Electronic Communications and Transactions Bill submitted with the ‘Response to Notice 1537 of 2004: Notice Inviting Comment on Proposed Accreditation Regulations drafted in terms of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002

Mark Heyink ‘Response to Notice 1537 of 2004: Notice Inviting Comment on Proposed Accreditation Regulations drafted in terms of the Electronic Communications and Transactions Act, 2002’ (Act No. 25 of 2002)

MCJ Olmesdahl ‘Unheralded Demise of Wolmer versus Rees’ (1984) 100 *SALJ* 545 at 553.

P Roberts ‘Rethinking the Law of Evidence: A twenty-first Century Agenda for Teaching and Research’ 2002 (55) *Current Legal Problems* 297

Randolph A Kahn & Dianne J Silverberg ‘From Mount Sinai to Cyberspace: Making Good E-business Records’ (2001) 57 *Business Lawyer* 431

RIL Howland, ‘UNCITRAL Model Law on Electronic Commerce’ (1997) 32/6 *European Transport Law* 703.

S Papadopoulos ‘Electronic Wills with an Aura of Authenticity: Van der Merwe v Master of the High Court and Another’ (2012) 24 *SA Merc LJ* 93-106;

Safinaz Mohd Hussein, ‘The Malaysian Communications and Multimedia Act 1998 & its implications on the information technology (IT) industry’ (2000) 9/1 *Information & Communications Technology Law* 79

Saravuth Pitiyasak, ‘Electronic Contracts: Contract Law of Thailand, England and UNCITRAL Compared’ 2003 (9)1 *Computer and Telecommunications Law Review* 16

Stephen Mason, ‘Electronic evidence: A proposal to reform the presumption of reliability and hearsay’, *Computer Law and Security Review*, Volume 30 Issue 1 (February 2014), 80

Subhajit Basu & Richard Jones, ‘Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000’ paper delivered at *17th BILETA Annual Conference* held on 5-6 April 2002 at the Free University, Amsterdam, Netherlands;

Tana Pistorius ‘‘Nobody Knows You’re a Dog’ – The attribution of Data Messages’ 4 (2002) *SA Mercantile Law Journal* 737-747.

Tim Fletcher ‘Certification of electronic evidence – a powerful tool in South African litigation’.

Official Reports

South African reports

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

South African Law Reform Commission, *Review of the Law of Evidence (Hearsay and Relevance)* Discussion Paper 113, Project 126, (2008)

South African Law Reform Commission *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues* Issue Paper 27 (2010)

Foreign reports

European Union

Council of Europe *The Use of Electronic Evidence in Civil and Administrative Law Proceedings and its Effect on the Rules of Evidence and Modes of Proof: A Comparative Study and Analysis* (Council of Europe, European Committee on Legal Co-operation, 2015).

Ireland

Irish Law Reform Commission, Consultation Paper *Documentary and Electronic Evidence* (LRC CP 57 – 2009)

New Zealand

Ministry of Justice, New Zealand Appendix B 'A comparison of the inquisitorial and adversarial systems' in *Alternative Pre-trial and Trial Processes for Child Witnesses in New Zealand's Criminal Justice System* (Issues Paper 2010).

United States of America

United States Office of Legal Education Manual Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (2009) available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf Accessed 31 July 2012.

List of Cases

South African Cases

S v Swanepoel 1980 (1) SA 144 (NC);

S v Terrance Stephan Brown Case No: CC 54/2014) Western Cape High Court

S v Van Der Vyver (SS 190/06) [2007] ZAWCHC 69 (29 November 2007)

Seccombe v Attorney-General 1919 TPD 270

Sihlali v Broadcasting Corporation Ltd (2010) 31 ILJ 1477 (LC)

Spring Forest Trading 599 CC v Wilbury Ecowash and Others (725/13) [2014] ZASCA 178 (21 November 2014).

Trustees for the time being of the Delsheray Trust and Others v Absa Bank Limited 2014 High Court of South Africa (Western Cape Division) judgment delivered on 9 October

Van der Merwe v The Master and Another 2010 (6) SA 544 (SCA))

Wilberry (Pty) Ltd v Spring Forest Trading 559 CC (725/13) [2014] ZASCA (21 Nov 2014)

Foreign Cases

United Kingdom

Entores Ltd v Miles Far East Corporation [1955] All ER 493 (CA);

The Statute of Liberty [1968] 2 All ER 195

Thornton v Shoe Lane Parking [1971] 1 All ER 686;

United States of America

List of Legislation

South African legislation

Alienation of Land Act 68 of 1981

Bills of Exchange Act 34 of 1964

Civil Proceedings Evidence Act 25 of 1965

Computer Evidence Act 57 of 1983 (repealed by ECT Act)

Consumer Protection Act 68 of 2008

Copyright Act 98 of 1978

Criminal Procedure Act 51 of 1977

Cybercrime and Cybersecurity Bill

Electronic Communications and Transactions Act 25 of 2002 (ECT Act)

Cryptography Regulations (GN R216 in GG 28594 of 10 March 2006)

Accreditation Regulations (GN 504 in GG 29995 of 20 June 2007)

Electronic Communications and Transactions Amendment Bill (published in *Government Gazette* 35821, Notice 888 of 2012).

General Law Amendment Act of 1950.

Interpretation Act 33 of 1957

Law of Evidence Amendment Act 45 of 1988

National Credit Act 35 of 2005

Protection of Personal Information Act 4 of 2013

Stamp Duties Act 77 of 1968

Wills Act 7 of 1953

Foreign legislation

Argentina
Digital Signature Law, 25 506

Australia

Electronic Transactions Act 1999 (commenced by Proclamation on 15 March 2000)

Evidence Act 2006

Austria

Federal Electronic Signature Law

Belgium

Law determining some rules concerning the legal framework of electronic signatures and certification services (9 July 2001)

Bermuda

Electronic Transaction Act, 1999

Brazil

Provisional Measure 2200-2 of 24 August 2001

Canada

Federal law:

Evidence Act R.S.C. 1985

Personal Information Protection and Electronic Documents Act, SC 2000

Uniform Electronic Commerce Act 1999

Provincial legislation:

Alberta
Electronic Transactions Act S.O. 2001

British Columbia
Electronic Transactions Act S.B.C. 2001, c. 10

Manitoba
Electronic Commerce and Information Act, S.M. 2000, c.E55

New Brunswick
Electronic Transactions Act, S.N.B. 2001, c. E-55

Nova Scotia
Electronic Commerce Act S.N.S. 2000, c. 26

Ontario
Electronic Commerce Act 2000 C S.O. 2000, c. 17

Prince Edward Island
Electronic Commerce Act, S.P.E.I. 2001, c.31

Quebec
Act to Establish a Legal Framework for Information Technology S.Q. 2001, c. 31

Saskatchewan
Electronic Information and Documents Act, S.S. 2000, c.E-7.22

Yukon
Electronic Commerce Act S.Y. 2000, c. 10

Chile

Law 19.799 and Decree 181

China

Electronic Signature Law of the People's Republic of China (restrictions relate to marriage, adoption and inheritance)

Czech Republic

227/2000 Coll. ACT of 29 June 2000 on electronic signatures and on the amendment to certain acts (Electronic Signature Act)

Colombia

Law 527 of 1999; Law 1150 of 2007 (public procurement) Law 962 of 2005 (electronic invoice)

Denmark

Bill on Electronic Signatures

Finland

Act on Strong Electronic Identification and Electronic Signatures (617/2009)

France

Law No. 2000-230 of 13 March 2000 Adopting the Right of Proof to Information Technologies and Electronic Signatures modifying Civil Code 1316 and other laws related to signatures and records;

Germany

Law Governing Framework Conditions for Electronic Signatures and Amending other Regulations

Hong Kong

Electronic Transaction Ordinance

Hungary

ACT XXXV of 2001 Civil Code of the Republic of Hungary and Act IV of 1952 on Marriage, Family and Legal Custody

India

Information Technology Act 21 of 2000 (as amended in 2006 and 2008)

Ireland

Electronic Commerce Act, 27 of 2000

Israel

Electronic Signature Law 5761 – 2001

Italy

March 27, 2005 Legislative Decree No. 82

Japan
Law Concerning Electronic Signatures and Certification Services;

Malaysia

Digital Signature Act;

Mauritius

Electronic Transactions Act of 2000;

Netherlands

Electronic Signature Act;

New Zealand

New Zealand Evidence Act 2006

Norway

Electronic Signatures Act of 2001

Peru

Digital Certificates and Signature Law, Law No. 27269

Philippines

Electronic Communications Act of 2000

Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents

Poland

Act of 18 Sept. 2001 on Electronic Signature

Portugal

Decree-Law no.290-D/99, of 2 August,
Decree-Law no. 62/2003, of 3 April

Decree-Law no. 234/2000, of 25 September

Decree-Law no. 256/2003, of 21 October

Republic of Korea

Digital Signature Act

Romania

Law on the Electronic Signature 2001 and Law on Electronic Commerce 2002;

Russian Federation

Federal Law No. 63-FZ 'On Digital Signature (July 01 2011)

Federal Law No. 149-FZ 'On Information, Information Technology and Protection of Information (July 27 2006)

Part Four Civil Code of the Russian Federation (Art 016)

Singapore

Singapore Electronic Transactions Act 25 of 1998

Electronic Transactions Act, 2011

Spain

Ley 59/2003 de 19 de diciembre, de firma electronica;

Thailand

Electronic Transaction Act B.E. 2544 (2001)

Turkey

Electronic Signature Law No. 5070

United Arab Emirates

Electronic Transactions and Commerce Law No. 2 of 2002

United Kingdom

Criminal Justice Act 2003

Civil Evidence Act 1995

Electronic Communications Act 2000.

United States of America

Federal law:

Electronic Signatures in Global and National Commerce Act Pub. Law No. 106-229 114 Stat 465 (codified at 15 U.S.C. § § 7001-06, § 7021, § 7031 (2000)
Federal Rules of Civil Procedure

Federal Rules of Evidence

Uniform Electronic Transactions Act (4 August 1999 draft) (adopted at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23 30 1999 (UETA)

State law:

Illinois
Electronic Commerce Security Act (1998)

Massachusetts
Electronic Records and Signatures Act (1998)

Uruguay

Law No. 18.600 on Electronic Documents and Electronic Signatures

Electronic sources

A Barratt and P Snyman Researching South African Law (2005) available online at http://www.nyulawglobal.org/globalex/south_africa.htm

Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf

ITWeb 'The facts regarding advanced electronic signatures' available at http://www.itweb.co.za/index.php?=com_content&view=article&id=52249 accessed 5 March 2012

Mason et al The Convention on Electronic Evidence http://conventiononelectronicevidence.org/

UniForum "Submissions to the Parliamentary Committee on the Electronic Communications and Transactions Bill (ECT) http://co.za/UniForumECTBillSubmission.pdf

Namespace "Comments on the Electronic Communications and Transactions Bill Draft ECT bill submission - 2002-04-24"

Piete Brooks "Security: Privacy, Authenticity and Integrity" http://www.ac.uk.pgp.net/pgpnet/secemail/q4/node4.html

List of Regional and International Instruments

African Union

African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, 2015

Commonwealth Secretariat

Draft Model Law on Electronic Evidence 2002

European Union

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (EU Directive on Electronic Signatures)

Directive 2000/31/EC L178; [2000] (OJ 17 July) European Parliament and Council of 8 June, 2000 on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the internal market available at ‹http://europa.eu.int/comm/internal_market/en/media/eleccomm/com31en.pdf›

Electronic Commerce (EC Directive) Regulations 2002 (Statutory Instrument 2002/2013)

Commission Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for Member States cooperation on eID

Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services

Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means

INTERNATIONAL CHAMBER OF COMMERCE

ICC General Usage for International Digitally Ensured Commerce (GUIDEC)) drafted by the International Chamber of Commerce (ICC) Information Security Working Party, under the auspices of the ICC Electronic Commerce Project available at <http://www.iccwbo.org/home/guidec/guidec.asp>.

INTERNATIONAL TELLECOMMUNICATIONS UNION

ITU Electronic Evidence: Model Policy Guidelines & Legislative Texts (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013) https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-evidence_mpg.pdf

Southern African Development Community

SADC Model Law on Electronic Transactions and Electronic Commerce (2011)

SADC Model Law on Cybercrime

United Nations

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001

UNCITRAL Convention of Electronic Contracts

Executive Summary

1. The overall objective of the Electronic Communications and Transactions Act 25 of 2002 is to enable and facilitate electronic commerce. This is achieved by the legal recognition of data messages and electronic signatures. The ECT Act also regulates electronic transactions and provides for the protection of online consumers and thus creating public confidence in electronic transacting. The admissibility and evidentiary weight of electronic evidence plays a pivotal role in ensuring the protection of the rule of law and an environment within which e-commerce can flourish. The ECT Act represents a major step forward in the facilitation of electronic commerce in South Africa.

2. Some of the chapters of the ECT Act have stood the test of time whereas other chapters and or provisions have become obsolete or redundant due to technological or legislative developments. Although the focus of this report is on the adequacy of the e-evidence provisions of the ECT Act other issues including the definitions and the differentiation between electronic signatures and advanced electronic signatures are also examined.

3. The SALRC recommends the urgent review of the ECT Act to remove redundant provisions and to improve the regulatory framework inter alia for electronic signatures and advanced electronic signatures. The SALRC also recommends the adoption of the Electronic Evidence Bill to clarify the criteria for the admissibility of certain types of electronic evidence and the evidentiary weight thereof and to regulate matters related thereto.

4. In summary of the Commission's recommendations are:

A. Recommendations: The Electronic Communications Transactions Act

1. The SALRC recommends a review of the ECT Act. Many of the provisions of the ECT Act have never been implemented or have become obsolete. By and large, there seems to be consensus that the ECT Act should be reviewed as a matter of priority.

2. The definitions in the ECT Act should be amended. The ECT Act's definition of a data message includes 'voice, where the voice is used in an automated transaction'. The SALRC proposes deleting this from the definition of a data message. The SALRC proposes the expansion of the definition of a data message to embrace future technologies that are not 'electronic'. It is thus not necessary to define 'electronic'. The SALRC proposes the expansion of the definition of a data message to include 'digital, magnetic, optical and electromagnetic or similar means' by which data messages can be generated, sent, received or stored'.

3. Section 14 of the ECT Act is clear regarding what is deemed to be an 'original'.

4. The SALRC recommends that the scope of the ECT Act remain unaltered.

5. The SALRC recommends that the regulation of electronic signatures in the ECT Act should be amended in line with the European Union Regulation and the adoption of a three-tier approach.

6. The SALRC recommends that the ECT Act should be amended to provide for standards for the accreditation of foreign signatures.

7. It is furthermore recommended that the ECT Act be amended to link the national electronic identification scheme to access to public services; to introduce other electronic trust services related to electronic delivery service, electronic seals, electronic time stamps, and website authentication.

8. The SALRC recommends the establishment of an appropriate forum comprised of multiple stakeholders to conduct the review of the ECT Act.

9. The SALRC recommends that the forum should conduct regular reviews of the ECT Act.

B. Recommendations: Electronic Evidence

1. The SALRC recommends law reform, through the introduction of a single statute to regulate electronic evidence.

2. The SALRC supports the view that hearsay evidence made by a person in an electronic document should be treated in the same way as hearsay evidence in a paper-based document based on the principle of technological neutrality. On the interaction of the ECT Act with the CPEA, the CPA and the LEAA, the SALRC supports a less fragmented approach to the admissibility of documentary evidence and therefore proposes reform through amending and supplementing existing provisions.

3. The SALRC supports the maintenance of a distinction between automated data messages and data messages 'made by a person' and proposes statutory reform to guide the production and proof of both types of evidence in court.

4. The SALRC supports the development of a handbook or a Guide on obtaining and producing electronic evidence that will provide clarity, to practitioners and judicial officers, on the legal position and advice on technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

5. The SALRC does not recommend the adoption of a presumption of regularity in relation to mechanical devices in the law of evidence. The SALRC further recommends that the question of presumptions receive the attention of a standing committee/working group to be established

6. The SALRC recommends the adoption of a limited presumption (placing an evidential burden on the other party who did not object on notice) in civil proceedings.

7. The SALRC recommends the review and amendment of the Rules of Court and other related laws to clear conflicts and inadequacies and to align the law of evidence to the effective use of electronic evidence in courts.

8. The SALRC recommends that the Rules Board for Courts of Law (the Rules Board), perhaps assisted by a standing committee/working group with technical expertise be requested to consider amendments to the rules of court to provide for the discovery and inspection of electronic documents. The SALRC notes also that the Rules of Court may require amendment in the event of statutory reform that requires notice prior to trial to be given in respect of an intention to rely on electronic documentary evidence, as well as notice of any objections to the use thereof to enable parties to prepare for trial.

CHAPTER 1 INTRODUCTION

A Background to Project 126

1.1 This Report contains the final recommendations on the ongoing study by the SALRC on the review of evidence, specifically electronic evidence. This Report was preceded by Issue Paper 27 *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues*, which discussed a number of concerns about electronic evidence in criminal and civil proceedings; Issue Paper 27 was published for comment in 2010.

1.2 A review of the law of evidence was included in the SALRC's research 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. However, the Commission gradually realised the enormity of such an undertaking and abandoned the codification of the law of evidence. The Commission decided rather to ascertain which aspects of the law of evidence were unsatisfactory or did not meet current needs, and to formulate suggestions for their reform.

1.3 In 2003 in a preliminary study by the SALRC, Professor PJ Schwikkard identified several areas of law for possible reform and outlined these in Committee Paper 1024 titled Project 126 *Review of the Law of Evidence* (2003). The areas under discussion included the following:

- the principle of relevance;
- the approach to hearsay evidence; and
- various structural features of the court system (that is, the limited role of lay assessors and the adversarial nature of proceedings.)

1.4 Paper 1024 recognised that the function of the law of evidence differs in civil and criminal trials and that there are different policy considerations underlying each. Whereas civil trials are intended to resolve disputes to order relationships, criminal evidence and procedure is 'an applied branch of moral and political philosophy'[1] in which the rights and responsibilities

1 P Roberts 'Rethinking the Law of Evidence: A twenty-first Century Agenda for Teaching and Research' 2002 (55) *Current Legal Problems* 297 cited in South African Law Reform Commission, Discussion Paper 113, Project 126, *Review of the Law of Evidence (Hearsay and Relevance)* 2008 at 13.

of citizenship are articulated. As a point of policy therefore, the paper concluded that a more cautious approach should be taken to the admissibility of evidence in criminal trials.

1.5 That preliminary study was followed by Issue Paper 26 *Review of the Law of Evidence* and Discussion Paper 113 *Review of the Law of Evidence (Hearsay and Relevance)*. Both of these papers were published in 2008.

1.6 Issue Paper 26 identified several issues in theory and in practice for further investigation and review. These included issues related to the concepts of real evidence, documentary evidence and computer generated evidence. The Issue Paper asked the following questions (among others) which are relevant to the current Discussion Paper:

- To what extent (if any) should the rules regulating the admission of electronic recordings be clarified?
- Which rules (if any) regulating the admission of documentary evidence require reform?
- Are the provisions in the Electronic Communications and Transactions Act sufficient to regulate the admissibility of computer generated evidence?

These questions were expanded upon in 2010 in Issue Paper 27 *Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues*.

1.7 In Issue Paper 27 SALRC addressed the characteristics[2] of electronic evidence that raise concerns about its accuracy and authenticity. We also assessed the approach to electronic evidence in both civil[3] and criminal proceedings[4] in South Africa since the judgment in *Narlis v South African Bank of Athens*[5] first raised concerns about the admissibility of electronic evidence.

2 See Chapter 2 of Issue Paper 27 for a comprehensive discussion of the nature of electronic evidence.
3 See Chapter 4 of Issue Paper 27, which traces the admissibility of electronic evidence in civil proceedings prior to the enactment of the ECT Act. In particular the chapter discusses the provisions of the Computer Evidence Act 57 of 1983 (repealed by the ECT Act) and certain provisions of the Civil Proceedings Evidence Act 25 of 1965.
4 See Chapter 5 of Issue Paper 27 for a discussion of the admissibility of electronic evidence in criminal proceedings in terms of section 221 and section 236 of the Criminal Procedure Act. Chapter 5 discusses *S v Harper* 1981 (1) SA 88 (D) and the conflicting interpretations of the decision in *Harper* as it relates to the term 'document'. Subsequent decisions in *S v De Villiers* 1993 (1) SACR 574 (Nm) and *S v Mashiyi and Another* 2002 (2) SACR 387 (Tk) are also discussed.
5 1976 (2) SA 573 (A).

1.8 In 1982, after the decision in *Narlis*, the SALRC drafted the *Report on the Admissibility in Civil Proceedings of Evidence Generated by Computers*, Project 6, Review of the Law of Evidence (1982). This report ultimately resulted in the passing of the Computer Evidence Act 57 of 1983 applicable to civil proceedings. The SALRC's deliberations on the admissibility of computer generated evidence in criminal proceedings (Project 108) were superseded by the enactment of the ECT Act, which repealed the Computer Evidence Act and provided for the admissibility of electronic evidence in civil and criminal proceedings as follows:

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

1.9 Issue Paper 27 identified certain concerns that may arise out of the formulation of section 15 and related provisions of the ECT Act, and requested public comment. The Discussion Paper also raised a number of issues.

1.10 Commentators were invited to bear in mind the challenges that computer-related evidence presents to the law of evidence. One comment is that 'it has endeavour[ed] to force

the products of modern technology into the limited categories of either real or documentary evidence.'[6]

1.11 The digitisation of information and the rapid growth of the Internet have had a marked influence on society. The Internet is changing the way we communicate and do business. These changes have dramatically and irrevocably altered the needs of business and industry. The continuing development of the Internet and its associated applications has created a variety of new situations in which traditional legal principles should be applied.

1.12 Discussion Paper 131 has noted that *the* crucial concern, particularly where the evidence is derived from a computer that has performed a computational function, is the integrity (reliability) and authenticity (accuracy) of computers and computer systems. This concern is compounded by the fact that a computer 'no longer works with analogue data, but with data in a digital form, which makes it very susceptible to manipulation'.[7] Even if a computer served merely as a recording tool in compiling the piece of evidence, alteration of that electronic document may occur without detection – unlike alteration of a paper-based document. This scenario requires a new approach to addressing the question of authentication. It also raises questions about what constitutes best evidence and what constitutes an 'original' data message in the case of electronic evidence.

1.13 Discussion Paper 131 concluded that questions about integrity (reliability) and authentication are therefore critical considerations in deciding the way forward.

1.14 These concerns were reflected in the comments received by the SALRC on the questions poses in Discussion Paper 131. Together with the case law analysed and the comparative law studied in the preparation of this Report, such comments indicate a gap in South African law with regard to the admissibility of electronic evidence.

1.15 Discussion Paper 131 has noted that the manner in which we address this gap is likely to be shaped by the common law origins and the adversarial nature of South Africa's legal

6 DP van der Merwe 'Appliances and Devices' in 'Evidence' by CWH Schmidt and DT Zeffert (updated by DP van der Merwe) *LAWSA* (LexisNexis Butterworths 2005) 8.4. The difference between evidence that is tendered 'circumstantially' and evidence that is tendered 'testimonially' therefore becomes important in determining how the courts should assess a particular piece of evidence.
7 Ibid.

system. The rules on the admissibility of evidence are notably lenient in inquisitorial systems,[8] such as those reflected primarily in civil law countries. However, this is not the case in the adversarial systems found in common law countries such as South Africa. Adversarial systems typically have well developed categories of inadmissible evidence – a feature that largely seems to be a response to the use of juries (which are less commonly used in inquisitorial systems) and a concern that juries 'don't have training on the weight that should be given to certain evidence.'[9]

2 Outline of the Report

1.16 The paragraphs above summarise the background to this Report and provide an introduction to the issues that will be discussed in the report.

1.17 Discussion Paper 131 requested comments on 11 issues. The eleven issues have been grouped into three broad themes. The report is structured around the three themes as follows:

- Chapter 2 discusses various issues related directly to the ECT Act (Issues 1-5).
- Chapter 3 discusses electronic evidence (Issues 6-11).
- Chapter 4 discusses the general proposals for law reform relating to the law of electronic evidence.
- Chapter five summarises the possibilities for law reform and the SALRC's provisional recommendations in this regard.

1.18 This report provides a short background to the issues raised, it provides an exposition of the comments received and concludes with an evaluation and recommendations.

8 Ministry of Justice, New Zealand 'Appendix B: a comparison of the inquisitorial and adversarial systems' in *Alternative Pre-trial and Trial Processes for Child Witnesses in New Zealand's Criminal Justice System* (Issues Paper 2010) available online at *http://www.justice.govt.nz/publications/global-publications/a/* Accessed 31 July 2012. See also Stephen Mason (ed) *International Electronic Evidence* (British Institute of International and Comparative Law 2008) and Mason's discussion of approaches from jurisdictions other than Commonwealth countries: see for example the chapter on 'Denmark' for a clear description of a very different approach to the law of evidence.

9 Ibid.

CHAPTER 2 THE ECT ACT

A Revision of the ECT Act

1 Background

Issue 1: Should the ECT Act be reviewed on a regular basis to take account of advances in technology?

- If so, what should such a review entail?
- When I how often should such a review take place?
- Who should undertake the review?

2.1 The advent of the use of electronic communications for commercial transactions posed unexpected and complex legal problems uncertainties. Electronic communications also spurned a host of illegal and fraudulent practices such phishing and payment fraud. Uncertainties regarding the admissibility and evidentiary value of electronic communications permeated these legal uncertainties.

2.2 In response to these developments the United Nations Commission on International Trade Law established a Working Group to draft legal rules on electronic commerce.[10] The UNCITRAL *Model Law on Electronic Commerce* was adopted in 1996 and aims to create a more secure legal environment for electronic commerce by providing a tool for states to enhance their legislation as regards paperless communication and storage of information.[11] In May 1997 the '*Guide to Enactment*' was published.[12] The *Guide* summarises the consensus of the discussions by the Commission and the Working Group and provides explanatory

10 Christoph Glatt, 'Comparative issues in the formation of electronic contracts' (1998) 1/6 International Journal of Law and Information Technology 34 at 57; Benjamin Wright, The Law of Electronic Commerce EDI, Fax and E-Mail: Technology, Proof, and Liability (1991) at 235; see also Toh See Kiat, Paperless International Trade: Law of Telematic Data Interchange (1992) at 10-11, 161-193.

11 Adopted on the 12th of June 1996.

12 The Guide to Enactment (1996) to Enactment (1996) was considered by the Working Group on Electronic Commerce see http://www.uncitral.org.

information aimed at assisting national governments when enacting legislation based on the Model Law.[13]

2.3 Other international developments include the adoption of the UNCITRAL Model Law on Electronic Signatures (MLES) in 2001 and the United Nations Convention on the Use of Electronic Communications in International Contracts[14] (here after the Electronic Communications Convention or UNECIC) prepared by the United Nations Commission on International Trade Law (UNCITRAL) in the field of electronic commerce and concluded in 2005.

2.4 The Model Law relies on the `functional equivalent approach', which is based on an analysis of the essential purpose and function of a traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.[15] It essentially involves the determination of the criteria which the equivalent electronic communication must meet in order to be given the same legal recognition as the corresponding paper-based document enjoys, where both the paper-based document and the electronic communication are performing the same function.[16]

2.5 It is also important to note that it is one of the objectives of Model Law that the adoption of the functional-equivalent approach should not result in imposing on users of electronic commerce more stringent standards of security (and the related costs) than in a paper-based environment.[17] The Model Law has adopted a technology-neutral solution.

2.6 Model Law adopted a flexible standard, taking into account the various layers of existing requirements in a paper-based environment: when adopting the `functional-equivalent' approach, attention was given to the existing hierarchy of form requirements, which provides

13 For a general discussion see RIL Howland, 'UNCITRAL Model Law on Electronic Commerce' (1997) 32/6 European Transport Law 703.
14 United Nations Convention on the Use of Electronic Communications in International Contracts www.uncitral.org/uncitral/en/uncitral_texts/electronic.../2005Convention.html which entered into force on 13 November 2013.
15 Id at par 16. It is noted in par 16 that paper documents fulfil the following functions: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met.
16 See Howland 'UNCITRAL Model Law on Electronic Commerce' (1997) 32/6 European Transport Law at 703.
17 See Guide to Enactment (1996) par 16.

distinct levels of reliability, tractability and inalterability with respect to paper-based documents.[18] For example, a data message cannot, in and of itself, be regarded as an equivalent of a paper document as it is of a different nature and does not necessarily perform all conceivable functions of a paper document. Furthermore, the requirement that data be presented in written form[19] is not to be confused with more stringent requirements such as `signed writing', `signed original' or `authenticated legal act'.[20] The Model Law influenced and shaped the e-commerce legislation adopted in many states[21] with the exception of its article 13 on attribution.[22] The European Union's E-Commerce Directive[23] is a notable exception as it was not influenced by the Model Law.

18 See the Guide to Enactment (1996) par 17.

19 This is regarded as a `threshold requirement'.

20 Ibid.

21 The US Uniform Electronic Transactions Act (4 August 1999 draft) (adopted at its Annual Conference Meeting in its One-Hundred-And-Eighth Year in Denver, Colorado (July 23B30 1999 (hereafter the UETA), has been closely modelled on arts 2(a) & (f), 4, 5, 6, 7, 8, 9, 10, 11, 14 & 15 of the Model Law whereas the federal Electronic Signatures in Global and National Commerce Act Pub. Law No. 106-229 114 Stat 465 (codified at 15 U.S.C. § § 7001-06, § 7021, § 7031 (2000) (hereafter referred to as the 'E-Sign Act') is not based on any model law. State law also emulates the Model Law – see the Illinois Electronic Commerce Security Act (1998) has adapted arts 2(a), 4, 5, 6, 7, 8, 9, 10 & 13 of the Model Law and Massachusetts' Electronic Records and Signatures Act (1998) have adapted articles 5, 6, 7, 8, 9 & 10 of the Model Law. In Australia the Electronic Transactions Act 1999 (commenced by Proclamation on 15 March 2000) (hereafter ETA)) was adopted in 1999; see also the Canadian Uniform Electronic Commerce Act 1999 (hereafter UECA) (available at ‹http://www.law.ualberta.ca/alri/ulc/acts/eUECA.htm›) (assented to 13 April 2000) statutes closely modelled on UECA has been adopted as a model for provincial electronic commerce laws see Ontario - Electronic Commerce Act 2000 C S.O. 2000, c. 17; Manitoba - Electronic Commerce and Information Act, S.M. 2000, c.E55; Saskatchewan - Electronic Information and Documents Act, S.S. 2000, c.E-7.22; Nova Scotia - Electronic Commerce Act S.N.S. 2000, c. 26; Yukon - Electronic Commerce Act S.Y. 2000, c. 10; British Columbia – Electronic Transactions Act S.B.C. 2001, c. 10; Price Edward Island - Electronic Commerce Act, S.P.E.I. 2001, c.31; New Brunswick -Electronic Transactions Act, S.N.B. 2001, c. E-55; Quebec Act to Establish a Legal Framework for Information Technology S.Q. 2001, c. 31; and Alberta Electronic Transactions Act S.O. 2001; Singapore has adopted the Electronic Transactions Act 25 of 1998 and it is based on the Model Law.

22 The Model Law's provisions on the attribution of data messages were not adopted by most countries as it was the one provision that was deemed to be out of sync with the functional equivalence and media neutrality principles – see Tana Pistorius ''Nobody Knows You're a Dog' – The attribution of Data Messages' 4 (2002) SA Mercantile Law Journal 737-747.

23 See Directive 2000/31/EC L178; [2000] (OJ 17 July) European Parliament and Council of 8 June, 2000 on Certain Legal Aspects of Information Society Services, in particular electronic commerce, in the internal market available at ‹http://europa.eu.int/comm/internal_market/en/media/eleccomm/com31en.pdf› (hereafter referred to as the E-Commerce Directive); the Electronic Commerce (EC Directive) Regulations 2002 (Statutory Instrument 2002/2013); the E-Commerce Directive was adopted in the United Kingdom in August 2002 – see Singleton supra note 4 at 1; Turner & Traynor supra note 4 at 19; Graham supra note 4 at 15 14; see also Smith & Hand supra note 4; Tim Kevan & Paul McGrath, E-mail, the Internet and the Law Essential Knowledge for Safer Surfing 2001 (Hertfordshire: EMIS Professional Publishing Ltd) at 209-214; For a critical discussion see See Christina Hultmark Ramberg, 'The E-Commerce Directive and Formation of Contract in a Comparative Perspective' (2001) 26 European Law Review 429 at 431 (also available at ‹http://www.juridicum.su.se›; See Christopher T. Poggi, 'Electronic Commerce Legislation: An Analysis of European and American Approaches to contract formation' 2000 (41) Va. J. Int'l. L. 224 at 272 at 270.

2.7 Chapter III of the ECT is also modelled on international best practice,[24] namely the UNCITRAL Model Law. The overall objective of the ECT Act is to enable and facilitate electronic transactions by providing for its enforceability and thus creating public confidence in electronic transacting. As drafted, the Act represents a major step forward in the facilitation of electronic commerce in South Africa. The impact of the Act is extensive as it amends traditional approaches to contract law are dramatic.

2.8 Key Issues addressed in this ECT Act include:

- Maximizing benefits – promotion of universal access, especially for members from previously disadvantaged communities, SMMEs and differently abled people
- Legal certainty – providing for the legally-binding effect of data messages
- Security – the regulation of cryptography and the accreditation of Authentication Service Providers; the protection of critical databases
- Protection of individuals – consumer and privacy protection
- E-government – ensuring electronic access to government and government services
- Illegal activities and enforcement – creation of new 'cyber offences' and cyber-inspectors
- Effective management of Internet-related issues – limitation of liability on the part of ISPs and national policy on the management of the domain name space.

24 See Assafa Endeshaw, 'The Singapore E-commerce 'code' (1998) 3/8 Information & Communications Technology Law 189 (hereafter Endeshaw E-commerce 'code'); Andrew Phang & Daniel Seng, 'The Singapore Electronic Transactions Act 1998 and the proposed art 2b of the Uniform Commercial Code' (1999) 2/7 International Journal of Law and Information Technology 103; see also in Assafa Endeshaw, 'Singapore gets to grips with the Internet' (1996) 7/2 Journal of Law and Information Science 208B222; Safinaz Mohd Hussein, 'The Malaysian Communications and Multimedia Act 1998 C its implications on the information technology (IT) industry' (2000) 9/1 Information & Communications Technology Law 79B88; see also Mauritius Electronic Transactions Act of 2000; Philippines Electronic Communications Act of 2000. Also based on the Model Law are Ireland's Electronic Commerce Act 27 of 2000, Bermuda's Electronic Transactions Act of 1999, India's Information Technology Act 21 of 2000 - see Subhajit Basu & Richard Jones, 'Legal Issues Affecting E-Commerce: A Review of the Indian Information Technology Act, 2000' paper delivered at 17th BILETA Annual Conference held on 5-6 April 2002 at the Free University, Amsterdam, Netherlands; see Thailand's Electronic Transactions Act 2001 (hereafter Thai ETA) – see Saravuth Pitiyasak, 'Electronic Contracts: Contract Law of Thailand, England and UNCITRAL Compared' 2003 (9)1 Computer and Telecommunications Law Review 16-30. Lastly, in South Africa, the Electronic Communications and Transactions Act 25 of 2002 (Proc R68 published in Government Gazette 23809 of 30 August 2002 (Reg Gaz 7449)) based its Chapter 3 dealing with e-contracting closely on the provisions of the Model Law.

2.9 Paper 27 raised the concern that new technologies, which are constantly being introduced, challenge existing legal concepts. The Paper asked a whether regular review of the ECT Act is desirable in light of the pace of technological development.

2 Exposition of comment

2.10 All comments expressed support for a regular review of the ECT Act 25 of 2002.

2.11 The Law Society of South Africa (LSSA) noted that the proposed standing committee should ensure harmonisation of our law with developments in other countries. It notes that in this regard, the ECT Act should only be amended with the greatest of care particularly where the sections are based on the UNCITRAL Model Law.

2.12 Mark Heyink notes that changes occur incredibly rapidly and citizens deserve the establishment of relative certainty in governing actions and also swift action to curb abuses that are always a feature of revolutionary times. Against this background, while he submits that to a large degree Chapter III of the ECT Act has stood the test of time, there are areas of amendment that are necessary. There are also many areas outside of Chapter III which have simply been bad law, have never been implemented and are now totally out of line with modern development.

2.13 Mark Heyink is not in support of regular reviews of 5 or 3 or 2 years as he notes that such reviews would be reactionary at best (bearing in mind that these reviews take significant time to actually be manifest in law, regulation or rules). He recommends the establishment of a standing committee that on a continuous and ongoing basis monitors developments, identifies areas of concern and engages with the appropriate actors in coordinating responses of the various parties.

3 Evaluation and recommendation

2.14 It has been noted that to have the greatest impact, legislation of this type must be future-proof and take into account the needs of the society it serves, especially if it is to help the expansion of small, medium and micro enterprises (SMME's). Furthermore, it should not

hinder economic growth by being too prescriptive or adding unnecessary regulatory burdens. It was predicted that the Act will have far-reaching implications for the way that South Africans will work, transact and share information.

2.15 However, whilst the Act does achieve its primary objective of facilitating electronic transactions, it also raises a number of serious questions, particularly in relation to some of the definitions used, the intention to regulate the provision of cryptography services, privacy of information, unsolicited communications and the protection of critical databases.

2.16 There is an apprehension that too much regulation will discourage private sector investment and will place an unnecessary burden on Government, which the taxpayer will ultimately have to pay for. The objective of the review of the ECT Act is not to introduce over-burdensome regulation but to amend poorly drafted legislation and to address legislative gaps. The current legal uncertainties place a huge burden on private and public sectors, especially the judiciary.

2.17 One overarching concern is the degree to which responsibility for much of the ensuing regulation is vested in the Department of Post and Telecommunications (DPST). Whilst we recognise the pivotal role that the DPST has to play because of its responsibility for managing telecommunications infrastructure, the ECT Act addresses diverse subject matter ranging from consumer protection, cryptography, the management of the .za domain name space, SPAM, the protection of personal information, electronic transactions, cyber inspectors, cybercrime to the limitation of liability of service providers. The ECT Act therefore impacts on a broad spectrum of government departments, including the Departments of Post and Telecommunication Services, Communications, Treasury, Home Affairs, Justice and Constitutional Affairs, Trade and Industry and State Security.

2.18 There is a need for a cross-cutting body to oversee legislation of this nature. Such an inter-departmental (and non- governmental) body need not place an additional burden on the tax-payer if its members are drawn from the existing establishment.

2.19 The SALRC recommends a review of the ECT Act. Many of the provisions of the ECT Act have never been implemented or have become obsolete. By and large, there seems to be consensus that the ECT Act should be reviewed as a matter of priority.

2.20 *Secondly, the SALRC recommends the establishment of an appropriate forum comprised of multiple stakeholders to conduct the review of the ECT Act.*

2.21 *The SALRC recommends that the forum should conduct regular reviews of the ECT Act.*

B Provisions of the ECT Act

1 Definitions

Issue 3: Should the current definition of 'data message' in the Act be revised? For consistency and clarity, **should the ECT Act or other legislation relevant to admissibility of electronic evidence in criminal proceedings include a definition of 'electronic', 'copy' and 'original'?**

(a) Background

(i) Data messages

2.22 The term 'data message' is defined in very wide terms: - a **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.

2.23 Data messages include all messages generated, sent, received or stored by electronic means. The phrase specifically includes any Internet messages and e-mail messages and it is wide enough also to include telefax, fax, SMS messages and instances where voice is used in conjunction with a voice recognition system on a computer or a mobile phone.

2.24 The notion of a 'data message' is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication. Thus, the notion of 'message' includes the notion of 'record'.

2.25 Clause 1(q) of the Electronic Communications and Transactions Bill (2012) proposes the amendment of the definition of a data message and as follows:

> ‘‘data message’ means [**data generated, sent, received or stored by electronic means and includes**] electronic communications including—
> (a) voice, where the voice is used in an automated transaction; and
> (b) any other form of electronic communications stored as a [**stored**] record includes the creation, storage and transmission of images scanned into a device;’

2.26 Clause 1(t) of the Electronic Communications and Transactions Bill provides that ‘electronic communications’ shall have the meaning given to it in the Electronic Communications Act 36 of 2005.

(ii) Other definitions

2.27 The Discussion Paper questions whether the ECT Act or other legislation relevant to admissibility of electronic evidence in criminal proceedings should include a definition of ‘electronic’, ‘copy’ and ‘original’?

2.28 The ECT Act does not define the concepts ‘electronic’ or ‘copy’.

2.29 The ECT Act does not define the concept ‘original’. The concept of originality is addressed in section 14 of the ECT Act as follows:

> 14. (1) Where a law requires information to be presented or retained in its original form, that requirement is met by a data message if—
>
> (a) the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection (2); and
>
> (b) that information is capable of being displayed or produced to the person to whom it is to be presented.
>
> (2) For the purposes of subsection 1(a), the integrity must be assessed—
>
> (a) by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
>
> (b) in the light of the purpose for which the information was generated; and
>
> (c) having regard to all other relevant circumstances.

(b) Exposition of comment

(i) Data message

2.30 The Banking Association South Africa noted that there is no need to amend the definition of a data message.

2.31 The Law Society of South Africa and the various submissions by Mark Heyink note that word '*message*' has an obvious long standing meaning in the English language related to a communication between two or more persons. This ordinary meaning is significantly departed from by the definition of a 'data message' in the ECT Act, which includes data records which are never communicated. The term '*data record*' is preferred to '*data message*', notwithstanding the use of the phrase '*data message*' in the UNCITRAL Model Law. Records of data communications will fit naturally within the meaning of a data record, as will data records which are not communicated. It is noted that the departure from the term used in the UNCITRAL Model Law will not serve as a problem to international legal harmonisation in any substantive way, particularly so given the broader reach of the ECT Act compared to the narrower commercial scope of the UNCITRAL Model Law.

2.32 Capitec Bank notes that the inclusion into the definition of 'voice, where voice is used in an automated transaction' has been explained by the drafters as being necessary to incorporate voice recordings that are analogue. With great respect the nature of analogue evidence is very different from digital evidence and its inclusion appears to reflect the drafter's deficiencies in understanding electronic or digital communications and records. In any event this becomes increasingly academic as audio and video recordings are almost exclusively digital.

2.33 The Law Society of South Africa and the various submissions by Mark Heyink endorse the Commission's proposal to amend the definition by either deleting subsection (a) from the definition or amending subsection (a) to include '*voice, where the voice was recorded in electronic form*'. The commentators note that, if the revised wording of subsection (a) was

introduced, it would mostly be beneficial for the avoidance of doubt, as anything recorded in electronic form would automatically constitute a data record.

2.34 Mark Heyink notes that while it is understood that the drafters may have included in the definition of 'data message' the concept of a stored record to assist in the understanding of the notion that a data message is not confined to communication between 2 persons or computers, it is less clear why they chose to include provisions relating to 'voice'. 'Voice' in digital form is identical in nature to text in digital form and as our telephone systems have moved from analogue to digital so voice records are increasingly being retained. Against this background the purpose of this inclusion and the move away from the recommended wording of the Electronic Commerce Model Law is not understood and, it is submitted, creates a restrictive approach which is totally unnecessary.

2.35 Mark Heyink also notes with great respect that the proposals made in the Electronic Communications and Transactions Amendment Bill shows a deficiency in understanding of the ECT Act and the underlying principles of the Electronic Commerce Model Law on which it was based. This is illustrated amply by the proposal to delete the definition of 'data' and replace it with the definition provided in the Electronic Communications Act.[25] The Electronic Communications Act does not even begin to address the same issues as are contemplated in the ECT Act as it deals specifically with electronic communications in a very different context to the way that data messages are dealt with in Chapter III of the ECT Act. He is of the opinion that the deletion of the term 'data' in the amendment of the definition of a 'data message' fatally undermines the foundations of the Electronic Commerce Model Law - therefore the ECT Act. This has been done without an appreciation of how the changes in this definition undermine the very principles on which this part of the Act is based.

(ii) Other definitions

2.36 The Banking Association South Africa noted that there is no need to define the terms 'copy', 'electronic' and 'original'.

25 It is important to note that an electronic communication is defined in the Electronic Communications Act as 'electronic communications' means the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electromagnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service'.

2.37 Mark Heyink notes that where a document is signed, often that is regarded as the original but it is also recognised that there may be more than one original and that originality is not necessary linked to uniqueness. He notes that in Deeds Office practice, an original is retained in the Deeds Office but equally a duplicate original is provided to the owner of the rights evidenced in the deeds. If one should differ from the other this may indicate that there has been tampering with one or the other.

2.38 He notes that the principle is identical in how the Electronic Commerce Model Law has chosen to deal with 'original' and is based on the integrity of the information from the time that it was first generated in its final form and that it is capable of being displayed or produced to a person to whom it is to be presented. From an evidential perspective it is the integrity of any further representation of a data message, by printout or otherwise, of how the data message was processed and displayed on the computer that is the determining factor for both best evidence and original.

2.39 Heyink notes that in considering the differences in form as opposed to function it has to be recognised that paper-based records are persistent. This means they are always evident. This is not the case with electronic records which are by nature pulses of electricity correlated to data and the data is then arranged by computer programmes into the information that constitutes the communication or record. They are not persistent and unlike paper, when the computer is switched off or when a particular document is not being processed by the computer it simply cannot be seen and in fact has no form.

2.40 He notes that the issue of 'original' is expressly addressed in the Model Law and has been incorporated into the ECT Act. Thus, when one considers a paper document from an evidential perspective, among the functions served by it is to provide that the information contained in the document would be legible to all, that it would be unaltered over time, allow for the reproduction of the document, allow for its authentication by means of signature and that it is in a form acceptable to public authorities and courts. With regard to the latter requirement there may also be additional information that will need to be provided to the document in certain instances. An example of this is that in some cases where copies of paper documents are used, it is sometimes necessary for them to be certified as true copies of the original.

2.41 Heyink correctly points out that with electronic evidence strictly the best evidence would be to take to court the computer or information system to display to the presiding officer the electronic evidence that is being led. He notes that this of course becomes absurd particularly if the information system includes extensive parts of the Internet, as so many information systems do today. Thus, printouts certified to accurately reflect the electronic information which has to be introduced in evidence are used and if they meet the criteria set out in Section 14 of the ECT Act dealing with originals, are regarded as originals and are therefore 'best evidence'.

2.42 With reference to 'electronic' and 'copy' Heyink notes that in dealing with 'copy document' and 'electronic document' in the context of a 'printout' the author of the Discussion Paper has not referred to the provisions in the ECT Act governing its original form. It is submitted that if this was done and properly understood that the definition of 'copy' is irrelevant in so far as it refers to an electronic record. Every time an electronic record is displayed or printed out it is in fact a copy. The issue of exactly what the original is, is irrelevant because the functions of the information (in particular its integrity) is what is important and not its form. Thus, as long as the definition of 'original' is adhered to in the ECT Act, representation of that information in whatever form is not a copy but in fact, by definition, an original. (See Section 14 in the ECT Act dealing with original and 17 with production of document or information.) He concludes that in dealing with section 15(4) (subject to the other limitations of the wording in that section itself) the printout is in effect an original for all purposes because the function of the original in paper form is served identically by the printout.

2.43 Against this background, and in so far as we are dealing with data messages, Heyink maintains that the word 'copy' should not be used and should in fact be deleted from Section 15(4) to ensure clarity in this regard.[26]

2.44 He also notes that moving to 'document', while the definition proposed by the author is dependent to some degree on the definition of 'copy' above, it is submitted that this change is

26 Heyick notes that the provisions of Section 15(4) needs to be revised. He argues:
'To clarify its purpose and remove the confusion between printouts of documents provided in the ordinary course of business and printouts provided for the sake of convenience where these printouts have to be made by virtue of the fact that an electronic record cannot be viewed by the party to whom it is produced. Because of the already enormous and increasing reliance on information in electronic form, where printouts are used to be adduced in evidence (which is really the purpose that the drafters had in mind when adding Section 15(4) to the provisions recommended in the Electronic Commerce Model Law). Further, it is submitted that an affidavit is not necessary in these circumstances. The reference to records in the ordinary course of business would then fall away in Section 15(4) but of course would apply the presumptions that our courts and our legislation already attribute to records of this nature. This would allow the functional equivalence principle to be applied consistently to electronic records.'

not necessary either. ‘Document’ itself requires no definition in its paper form as is well understood and judicial notice will be taken of that term where necessary.

2.45 Finally, Heyinnk notes that dealing with ‘electronic document’, the definition which is provided in the Discussion document does not add to the existing definitions of ‘data’ and ‘data message’ and unless it is intended that all of the ECT Act is amended to change verbiage, seems totally unnecessary. He submits that Chapter III of the ECT Act, if understood and interpreted against the Electronic Commerce Model Law, provides a sound basis for our law and, importantly, is harmonised with international law and development in this regard. He cautions against moving away from the wording of the ECT Act unless there are compelling reasons to do so. Certainly making wholesale changes to Chapter III of the ECT Act to deal with the narrower concerns relating to evidence, without properly understanding their background or the disciplines which inform the reliability and integrity of electronic evidence, should not be undertaken unless the whole of Chapter III is reconsidered and rewritten. He submits that in these circumstances it is highly likely that the principles on which such redrafting would be based would so closely reflect what is currently in the ECT Act as to render this exercise unnecessary.

(c) Evaluation and recommendation

(i) Data message

2.46 The UNCITRAL Model Law defines a ‘data message’ as 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;

2.47 The Electronic Communications Convention defines a data message as ‘information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or tele copy.[27]

27 See Article 4(c) of UNECIC.

2.48 The first issue to be considered under the definition of a data message in the ECT Act is the inclusion of 'voice' only where used in an automated transaction.

2.49 An 'automated transaction' means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment.

2.50 The definition specifically includes instances where voice is used in conjunction with a voice recognition system on a computer. What are clearly excluded are voice messages such as telephone conversations, even where the message is stored as a voice message. In the case of voice orientated 'automated transactions', the voice messages (compiled and decompiled into electronic impulses during the process) is recognised as the 'data message' component of that transaction.

(iii) Other definitions: electronic

2.51 The reference to 'similar means' in both the Model Law and UNECIC is intended to reflect the fact that this definition is not intended only for application in the context of existing communication techniques but also to accommodate foreseeable technical developments. It is noted that all means of communication and storage of information that might be used to perform functions parallel to the functions performed by the means listed 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 of the Model Law, the word 'similar' connotes 'functionally equivalent'.[28]

2.52 It is important to note that the Model Law's 'electronic, optical or similar means' is expanded to include 'electronic, magnetic, optical or similar means', The definition of a 'data message' is to encompass all types of messages that are generated, stored, or communicated in essentially paperless form. The addition of the word 'magnetic' as it expands the definition substantially.

2.53 The ECT Act defines 'data' as electronic representations of information of any kind. Electronic communication is defined to mean communication by means of data messages.

28 See Guide to Enactment par 31.

The meaning of the term ‘electronic’ is central to both the meaning of ‘data’ and the meaning of ‘data message’. ‘Electronic’ was defined in the ECT Act to mean digital or other intangible form. The definition of ‘electronic’ was inadequate and was deleted from the amended ECT Bill.[29]

2.54 ‘Electronic’ is defined in the UETA as relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.[30] The Canadian UECA's definition of electronic refers to storage in digital form or any other intangible form by electronic, magnetic or optical means.[31]

2.55 It is noted in the UETA comment on section 2 that not all the technologies included under the definition of electronic are technically `electronic' in nature (for example, optical fibre technology is not `electronic' in nature), but that the term `electronic' is the most apt to describe current technologies.

2.56 This wide definition adopted in the UECA has the advantage that future technologies will probably fall under this definition. For example, the development of biological and chemical processes for the communication and storage of data will fall within this technical definition as such processes that operate on electromagnetic impulses.[32] In a similar vein it is noted in the annotated text of the UECA that digital imaging relies on optical storage, which is technically not electronic, but which is generally regarded as proper subject matter for that Act.[33]

(iii) Other definitions: original

2.57 One of the pillars of commercial transacting is the sound knowledge that a transacting party will be entitled to enforce his bargain against a defaulting party. It is also a fundamental principle of procedural law that for litigation a party shall present the court with the ‘best evidence’ available to prove his claim. This age-old rule requires that authentic and original

29 See ECT Bill B8 of 2002 (as amended); Namespace op cit noted that the definition of electronic in the Bill was both too narrow and too broad. E.g., there are analogue (as opposed to ‘digital’) electronic signals that are part of voice, and voice is part of the definition of ‘data message’. See Namespace ZA ‘Comments on the Electronic Communications and Transactions Bill by Namespace ZA Draft ECT bill submission - 2002-04-24’ E.g., there are many intangible things that are not ‘electronic’ by any stretch of the imagination, e.g. a thought is intangible, a colour such as green is intangible, but no one would consider these to be ‘electronic’. Namespace ZA ‘Comments on the Electronic Communications and Transactions Bill by Namespace ZA Draft ECT bill submission - 2002-04-24’.

30 See UETA s 2(5).

31 See s 1(a) of the UECA.

32 See comment under s 2 of the UETA at 4.

33 See comment under s 1 of the UECA.

evidence be submitted such as an originally signed contract (as opposed to a copy). Whenever authentic or original material cannot be provided, a court requires oral evidence to convince it of the originality or authenticity. Besides hearsay, the question concerning best evidence, or the originality of the document concerned, remains. Source documents for document-specific rights and obligation can be called 'true' if reliable, only the latter can be called 'genuine' if reliable. Also keep in mind that the provision on 'original' was intended to deal with the rule in documentary evidence that copies of paper documents are not acceptable in court. This is because signs of any alterations, erasures etc. will be more obvious on the original document and because the 'wet' signature(s) may be subjected to forensic analysis.

2.58 It may be questioned whether it is appropriate to differentiate between a paper-based document which is replicated in digital format, and a document is from its point of origin in digital form. It has been noted that the difference is illuminated by the wording of Section 14(1)(a) '… when it was first generated in its final form as a data message or otherwise …'. [34] The Act does not distinguish between these respective original states of documentation for the purposes of originality. Meiring concludes that a scanned version of a paper-based document no longer in existence will fulfil evidential requirements as an original as much as a document generated with word-processing software, provided that the provisions of Section 14 are complied with.[35]

2.59. *Issue 3: there are two aspects:*

- *The first aspect (a) is the definition of a data message:*
  - *Concern has been expressed about the inclusion of 'voice, where the voice is used in an automated transaction' which does not appear in the UNCITRAL Model Law definition of a data message; the SALRC proposes deleting this from the definition of a data message.*
- *The second aspect (b) is the question of the need to define the terms 'electronic', 'original' and 'copy'.*
  - *The SALRC proposes the expansion of the definition of a data message to embrace future technologies that are not 'electronic'. It is thus not necessary to define 'electronic'. The SALRC proposes the expansion of*

34 See Ryk Meiring 'Electronic Transactions' *Cyberlaw @ SA II* at 89.
35 Ibid.

the definition of a data message to include 'digital, magnetic, optical and electromagnetic or similar means' by which data messages can be generated, sent, received or stored'.

- *Section 14 of the ECT Act is clear regarding what is deemed to be an 'original'.*
- *The term 'copy' has not been discussed (it is used in section 15(4)). The SALRC recommends that this term 'copy' should be deleted (see recommendations for law reform made in Chapter 3 infra).*

- *No further reform is proposed at this stage.*

2. Sphere of application

(a) Background

2.60 **Issue 4: The ECT Act's sphere of application does not extend to the Laws mentioned in Column A of Schedule 1** (i.e. the Wills Act; the Alienation of Land Act; the Bills of Exchange Act and the Stamp Duties Act. Should the ECT Act include the excluded transactions mentioned in Schedule 2 (i.e. agreements for the alienation of immovable property; agreements for long-term leases; the execution, retention and presentation of a will; and the execution of a bill of exchange?

2.61 Section 3 of the ECT Act addresses interpretation. It provides that the 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.

2.62 This section is extremely important in that it confirms that pre-existing (current) law also apply to the matters outlined in this Act.

2.63 The sphere of application of the ECT Act is addressed in section 4(1). It notes that subject to any contrary provision in this section, this Act applies in respect of any electronic transaction or data message. Section 4(2) provides that the Act must not be construed as—

(a) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form; or

(b) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

2.64 Section 4(3) notes that the sections of this Act mentioned in Column B of Schedule 1 do not apply to the laws mentioned in Column A of that Schedule.

2.65 Section 4(4) provides that the ECT Act must not be construed as giving validity to any transaction mentioned in Schedule 2.

2.66 Section 4(5) provides that the Act does not limit the operation of any law that expressly authorises, prohibits or regulates the use of data messages, including any requirement by or under a law for information to be posted or displayed in a specified manner, or for any information or document to be transmitted by a specified method.

2.67 Section 12 of the ECT Act refers to formalities. It provides as follows:

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.

2.68 Section 12 of the Act ensures that data messages are recognized as writing even where such a formality is required by statute. Formalities may be required either by the parties themselves[36] or by statute.[37] If information is contained in a data message in a manner that is accessible for future use, it will be recognized as writing.

2.69 This section is intended to define the basic standard to be met by a data message in order to satisfy a requirement that information be retained or presented 'in writing' or that it be contained in a 'document' or other paper-based instrument. The information in a data

36 For example the parties can provide that the contract must be in writing

37 For instance the assignment of copyright must be in writing and signed by the assignor in terms of the Copyright Act 98 of 1978; See also the General Law Amendment Act of 1950.

message must be accessible so as to be usable for subsequent reference. Here 'usable' includes human and/or computer use and 'accessible' is meant to imply that information in the form of computer data should be readable and interpretable, and that the software that might be necessary to render such information readable should be retained.

2.70 The legal recognition of electronic signatures and advanced electronic signatures is dealt with in section 13 of the ECT Act.

2.71 The Act defines an electronic signature as data which is attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature.

2.72 An advanced electronic signature is defined as an electronic signature which results from a process which has been accredited by the Accreditation Authority. Section 37 makes provisions for authentication service providers to register certain processes as advanced electronic signatures.

2.73 Where a signature is required by law an advanced electronic signature must be used.

2.74 However, as noted above, section 4 of the ECT Act makes provision for certain exclusions in the schedules to the Act. The provisions of the ECT Act are not applicable to the formalities (writing and signature) required in terms of the following:

- Alienation of Land Act 68 of 1981
- Wills Act 7 of 1953
- Bills of Exchange Act 34 of 1964
- Stamp Duties Act 77 of 1968
- a sales contract for the alienation of immovable property
- a long term lease (longer than 10 years) of immovable property
- a will
- a cheque or bill of exchange

(b) Exposition of comment

2.75 The Banking Association South Africa submitted that the question to extend the application of the ECT Act to other relevant legislation should be approached carefully and

with due consideration of the functional equivalence aspects. The Banking Association South Africa supported the formation of a dedicated body with adequate technological, legal and operational expertise to investigate extending the ECT Act application to legislation such as the Wills Act, Alienation of Land Act, Bills of Exchange Act and Stamp Duties Act.

2.76 The Law Society of South Africa notes that legal practitioners in general are distrustful of electronic documents and electronic signatures in particular. Although ante-nuptial contracts are generally reviewed at a time when persons are still alive and in a position to testify, some reservations have been expressed in relation to electronically executing any documents affecting the legal status of a person. Practitioners have also raised the question of whether affidavits should be capable of being signed in ink by a deponent (e.g. a client who might not have or need an advanced electronic signature) and then being scanned and signed electronically by a Commissioner of Oaths using an advanced electronic signature.

2.77 The Alienation of Land Act does not at first blush appear to present the same constraints as either the Wills Act or the Bills of Exchange Act. The Law Society of South Africa notes that there appears to be no practical reason why these agreements cannot be entered into by electronic means and as a matter of fact it appears that often faxed agreements of sale (notoriously insecure from a technology and information point of view) are accepted as valid evidence of sales of land by attorneys.

2.78 Mark Heyink notes that with regard to Wills and the issues of signature (the requirement that the testator or testatrix and the witnesses sign every page and that they are all present at the time of signature would have to be revised). He notes that an advanced electronic signature relates to the full record which will be signed only once and because of the nature of the identification elements of the provisions of advanced electronic signatures (which incorporates positive identification) the necessity for witnesses fall away.

2.79 He notes that it must be stated that levels of integrity which we seek to protect in a Will can be achieved and significantly exceeded in electronic form and using advanced electronic signatures. It is also important to recognise that the application of an advanced electronic signature provides the benefit of the presumption contained in Section 13(4) of the Act that the signature has been applied correctly. To some degree this may exclude disputes relating to the signature of Wills which currently come before the courts. Quite possibly this should be welcomed. It also opens the way for the signature of a digital or video recording of a Will.

2.80 Heyink notes that an advanced electronic signature will be as effective in 'locking' a digital video/audio recording and ensuring the integrity of the record as it is with a text record. In the case of video or audio digital Wills, while the integrity may be assured, the question of administration of these Wills may also beg some questions that legislation and regulation would require amendment, at least of the Administration of Estates Act.

2.81 Heyink notes that with regard to Bills of Exchange, it is submitted that one of the reasons that this was excluded is that the legislation governing bills of exchange contemplates bills of exchange in a paper format. The importance of signature in the negotiation of these bills is integral to the use of paper bills of exchange. However, the use of paper bills of exchange is reducing dramatically (considerably fewer cheques are written today than in years gone by) but they still exist and care will need to be taken to ensure that traditional negotiation of these bills of exchange in paper form are not adversely affected.

2.82 He notes that while traditional bills of exchange may become a dead letter in the future, different electronic transactions are replacing these and that this is definitely not something which needs to be dealt with in terms of the ECT Act save by reference in new legislation incorporating the legal principles relating to electronic communications, as may be deemed necessary.

2.83 Heyink notes that the Alienation of Land Act does not at first blush appear to present the same constraints as either the Wills Act or the Bills of Exchange Act. There appears to be no practical reason why these agreements cannot be entered into by electronic means and as a matter of fact it appears that often faxed agreements of sale (notoriously insecure from a technology and information point of view) are accepted as valid evidence of sales of land by attorneys.

2.84 Mark Heyink warns that caution needs to be sounded is that in certain instances it may be necessary for these documents to be lodged in a Deeds Office to protect one or other of the parties. There is no logical argument why a printout of an agreement transferring land cannot be dealt with by way of a printout in terms of section 15(4). Of course there may be arguments as to whether this is a record in the ordinary course of business if the current formulation of section 15(4) is maintained. It is suggested that, if this exclusion is removed, issues of administration of electronic documents in the Deeds Office would require

consideration and the Deeds Registries Act or its Regulations would have to be amended, alternatively Directives provided by way of Chief Registrars Circulars.

(c) Evaluation and Recommendation

2.85 The point of departure is that this Act applies to all common law as well as all legislation except where the application of the Act is specifically excluded. Party autonomy is retained, the Act merely facilitates e-communications, no-one may insist on the use of an electronic transaction and entities may lay down their own requirements where they are prepared to use electronic transactions including specific form, formats, standards etcetera be used. Section 12 and 13 of the ECT Act makes reference to the phrase 'in law'. Following the UNCITRAL Model Law, such term is likely to be interpreted to include reference not only to statutory, regulatory and common law, but also judicial precedent, procedural and subordinate law.[38] Reference is also made to 'law' in other sections of the ECT Act.[39]

2.86 Where the parties to an agreement require a written amendment of the agreement or a written notice in terms of the agreement, that requirement will be met by a data message.[40] This was confirmed in a recent decision of *Wilberry (Pty) Ltd v Spring Forest Trading 559 CC*[41] where the Supreme Court of Appeal held that an exchange of e-mail messages constituted a valid cancellation of a contract.[42]

2.87 Wills executed electronically have received legal recognition in South African courts.[43] There is no technological bar to the use of advanced electronic signatures to execute a will. Papadopoulos[44] correctly notes that:

38 Ryk Meiring 'Electronic Transactions' *Cyberlaw @ SA II* at 83.
39 See for example, Sections 12, 13(1), 14(1), 16(1), 17(1), etc.
40 Haupt op cit at 9 argues correctly that an agreement between two parties cannot be elevated to 'the law' – it merely has effect in law. Section 12 only affects statutory requirements of writing as the common law does not prescribe formality requirements.
41 (725/13) [2014] ZASCA (21 Nov 2014).
42 At par 17.
43 See *Macdonald v The Master and Others* 2002 (5) SA 64 (O); *Van der Merwe v The Master and Another* 2010 (6) SA 544 (SCA)); See also S Papadopoulos 'Electronic Wills with an Aura of Authenticity: Van der Merwe v Master of the High Court and Another' (2012) 24 SA Merc LJ 93-106; See also André R van Staden & Christa Rautenbach 'Enkele Gedagtes oor die Behoefte aan en die Toekoms van Elektroniese Testamente' (2006) 39 *De Jure* 586;
44 S Papadopoulos 'Electronic Wills with an Aura of Authenticity: Van der Merwe v Master of the High Court and Another' (2012) 24 SA Merc LJ 105-106.

> It has been argued that ECTA electronic signature provisions cannot meet the requirements for signature in terms of the Wills Act because this statute requires multiple signatures and parties need to sign in specific places within the document (ie, the testator must sign every page and witnesses must sign on the last page (Jamneck et al op cit at 66–7)). But I submit that this reasoning falls short of the functional equivalent approach of ECTA and the UNCITRAL Model Law as well as the inherent function of a signature in or on a document, whether it is electronic or paper-based
>
> …
>
> At a technological level, therefore, advanced electronic signatures have been designed to ensure the authenticity and integrity of a data message. Unlike handwritten signatures, once produced they cannot be copied or falsified. They can therefore fulfil the same functions as a handwritten signature, such as authentication, integrity and non-repudiation, and they attach to the electronic document, ie binary code, in its entirety (ie, every single page, word or letter (Fitzpatrick et al op cit at 557, 558, 560 and 570)). Furthermore, multiple electronic signatures can be attached to a single document, with each signatory being given a unique and secure electronic signature which will also record date and time stamps (see http:// www.docusign.com (visited on 26 October 2010)).

2.88 The limitation in the scope of application of the ECT Act i.e. the exclusion of agreements for the alienation of immovable property; agreements for long-term leases; the execution, retention and presentation of a will; and the execution of a bill of exchange did not arise due to any technological limitations.

2.89 The exclusion of certain transactions is not unique to South Africa. To the contrary, these provisions are mirrored in comparative provisions adopted in most jurisdictions for personal matters regarding death and family law;[45] real estate;[46] wills;[47] or the execution of a power of attorney[48] to name only a few. In a select few countries no restrictions apply.[49]

---

45 See Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf where the following are listed: See art 4 of Argentina's Digital Signature Law, 25 506; See Australia's ETA of 1999; Chile's Law 19.799 and Decree 181; the Electronic Signature Law of the People's Republic of China (restrictions relate to marriage, adoption and inheritance); See the Norwegian Electronic Signatures Act of 2001; United Arab Emirates' Electronic Transactions and Commerce Law No. 2 of 2002; Austria's Federal Electronic Signature Law; Finland's Act on Strong Electronic Identification and Electronic Signatures (617/2009); France's Law No. 2000-230 of 13 March 2000 Adopting the Right of Proof to Information Technologies and Electronic Signatures modifying Civil Code 1316 and other laws related to signatures and records; Germany's Law Governing Framework Conditions for Electronic Signatures and Amending other Regulations; In Hungary see ACT XXXV of 2001 which states in section 3(2) that restrictions apply to legal relationships referred to is sections 598-684 of the Civil Code of the Republic of Hungary and Act IV of 1952 on Marriage, Family and Legal Custody; and the United Kingdom's Electronic Communications Act 2000.

46 See Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf where the following are listed: See Australia's ETA of

2.90 *Issue 4: concerns about extending the scope of the application of the ECT Act to the transactions in Schedule 2 revolve around issues of authentication and reliability and the use of advanced electronic signatures. These issues are discussed below.*

2.91 *The SALRC recommends that the scope of the ECT Act remain unaltered.*

1999; Bermuda's Electronic Transaction Act, 1999; Canada's Personal Information Protection and Electronic Documents Act, SC 2000; the Electronic Signature Law of the People's Republic of China; Several laws in Colombia such as the Law 527 of 1999; Law 1150 of 2007 (public procurement) Law 962 of 2005 (electronic invoice); Hong Kong's Electronic Transaction Ordinance; India's Information Technology Act 2000 (as amended in 2006 and 2008); See also Japan – Law Concerning Electronic Signatures and Certification Services; Some real estate transactions are excluded in terms of Singapore's Electronic Transactions Act, 2011; ; United Arab Emirates' Electronic Transactions and Commerce Law No. 2 of 2002; See restrictions in the Unites States' Electronic Signatures in Global and National Commerce Act (E-Sign Act) and UETA; Uruguay's Law No. 18.600 on Electronic Documents and Electronic Signatures; Austria's Federal Electronic Signature Law; Czech Republic's 227/2000 Coll. ACT of 29 June 2000 on electronic signatures and on the amendment to certain acts (Electronic Signature Act); Finland's Act on Strong Electronic Identification and Electronic Signatures (617/2009); France's Law No. 2000-230 of 13 March 2000 Adopting the Right of Proof to Information Technologies and Electronic Signatures modifying Civil Code 1316 and other laws related to signatures and records; Germany's Law Governing Framework Conditions for Electronic Signatures and Amending other Regulations; See Ireland's Electronic Commerce Act, 2000; Poland's Act of 18 Sept. 2001 on Electronic Signature; and the United Kingdom's Electronic Communications Act 2000.

47 See Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf where the following are listed: See Australia's ETA of 1999; Canada's Personal Information Protection and Electronic Documents Act, SC 2000; India's Information Technology Act 2000 (as amended in 2006 and 2008); See also Japan – Law Concerning Electronic Signatures and Certification Services; United Arab Emirates' Electronic Transactions and Commerce Law No. 2 of 2002; Unites States' Electronic Signatures in Global and National Commerce Act (E-Sign Act) and UETA; Austria's Federal Electronic Signature Law; See Ireland's Electronic Commerce Act, 2000; Poland's Act of 18 Sept. 2001 on Electronic Signature; and the United Kingdom's Electronic Communications Act 2000.

48 See Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf where the following are listed: Canada's Personal Information Protection and Electronic Documents Act, SC 2000; Hong Kong's Electronic Transaction Ordinance; India's Information Technology Act 2000 (as amended in 2006 and 2008); Singapore's Electronic Transactions Act, 2011; See Ireland's Electronic Commerce Act, 2000;

49 See Abode Systems Incorporated *The Global Guide to Electronic Signature Law: Country by Country Summaries of Law and Enforceability* (2015) available at https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/adobe-global-guide-electronic-signatures.pdf where the following are listed: For example no restrictions are in the applicable in Brazil – see the Provisional Measure 2200-2 of 24 August 2001; Israel's Electronic Signature Law 5761 – 2001; Malaysia's Digital Signature Act; Peru's Digital Certificates and Signature Law, Law No. 27269; the Philippines' Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents; Republic of Korea Digital Signature Act; the Russian Federation's Federal Law No. 63-FZ 'On Digital Signature (July 01 2011) Federal Law No. 149-FZ 'On Information, Information Technology and Protection of Information (July 27 2006) and Part Four Civil Code of the Russian Federation (Art 016); Thailand's Electronic Transaction Act B.E. 2544 (2001); Tukey's Electronic Signature Law No. 5070; Belgium's Law determining some rules concerning the legal framework of electronic signatures and certification services (9 July 2001); Denmark's Bill on Electronic Signatures; Italy's March 27, 2005 Legislative Decree No. 82; the Netherland's Electronic Signature Act; Portugal's Decree-Law no.290-D/99, of 2 August, Decree-Law no. 62/2003, of 3 April, Decree-Law no. 234/2000, of 25 September and Decree-Law no. 256/2003, of 21 October; Romania's Law on the Electronic Signature 2001 and Law on Electronic Commerce 2002; Spain's Ley 59/2003 de 19 de diciembre, de firma electronica;

3. Electronic signatures

2.92 **Issues 5: The amendment of the ECT Act should be considered as far as electronic signatures are concerned.** The SALRC asked the following questions:

- Should the distinction between 'advanced electronic signature' and 'electronic signature' be abolished in the ECT Act?
- Should physiological features of biometrics (including fingerprint, iris recognition, hand, and palm geometry) be included in the ECT Act as a form of assent and electronic identity?

(a) Background

2.93 As noted above, an advanced electronic signature is defined as an electronic signature which results from a process which has been accredited by the Accreditation Authority. The compliance of various technical means with an 'advanced electronic signature' is important as in an electronic environment, the original of a message is indistinguishable from a copy, there is no hand written signature, and is not on paper. The potential for fraud is considerable, due to the ease of intercepting and altering information in electronic form without detection.

2.94 Accreditation is defined in section 33 to mean **recognition of an authentication product or service by the Accreditation Authority**. The term 'authentication products or services' is defined in section 1 to mean **products or services designed to identify the holder of an electronic signature to other persons**.

2.95 Section 38(1) of the ECT Act set out the criteria for accreditation. It provides that the Accreditation Authority may not accredit authentication products or services unless the Accreditation Authority is satisfied that an electronic signature to which such authentication products or services relate—

(a) is uniquely linked to the user;

(b) is capable of identifying that user;

(c) is created using means that can be maintained under the sole control of that user; and

(d) will be linked to the data or data message to which it relates in such a manner that any subsequent change of the data or data message is detectable;

(e) is based on the face-to-face identification of the user.

2.96 Section 38(4) provides that where the products or services are provided by a certification service provider, the Accreditation Authority may stipulate, prior to accrediting authentication products or services—

(a) the technical and other requirements which certificates must meet;

(b) the requirements for issuing certificates;

(c) the requirements for certification practice statements;

(d) the responsibilities of the certification service provider;

(e) the liability of the certification service provider;

(f) the records to be kept and the manner in which and length of time for which they must be kept;

(g) requirements as to adequate certificate suspension and revocation procedures; and

(h) requirements as to adequate notification procedures relating to certificate suspension and revocation.

(b)Exposition of comment

2.97 The Banking Association South Africa suggested that the distinction between 'advanced electronic signature' and 'electronic signature' as used in the ordinary sense be abolished as it will (inter alia) simplify the litigation process in obtaining provisional and summary judgments. The Banking Association South Africa supported the formation of a technical and expert body to consider the inclusion of biometric technology (such as

fingerprints, iris recognition, hand- and palm geometry) in the ECT Act, either in terms of the current provisions or by extending the current provisions.

2.98 The Law Society of South Africa and the representations made by Mark Heyink note that there is no physiological link between the electronic signature and the person making the signature. Therefore, the link between the signatory and the signature will be established through circumstantial evidence of the processes in place that are designed to provide this assurance. A tree-tiered approach is advocated, namely electronic signatures, digital signatures (which incorporate the concepts of 'reliable', 'secure' or 'advanced electronic signatures' as they are termed in other jurisdictions) and qualified electronic signatures.

2.99 Capitec Bank notes that the drafters of the ECT Act relied predominantly on the Electronic Commerce Model Law and applied its principles and its wording (only modified in a few circumstances) in Chapter III of the ECT Act, and the drafters relied on the EU Directive in dealing with electronic signatures.

2.100 Capitec Bank notes that the EU Directive (relied on by the drafters) was repealed on the 1st January 2016 and replaced by the EU Regulation, which provides more comprehensive guidance and formal governance to the use of electronic signatures in the European Union. The Regulation expands and enhances on the ambit of the Directive, providing a cross-border and cross-sector framework for secure and trustworthy electronic signatures and transactions, including the use of electronic signatures, which will be recognised by all states that are members of the European Union. The EU Regulation is significantly broader than the EU Directive and provides specifically for the legal effects of electronic signatures generally. It also establishes the requirements for advanced electronic signatures and qualified electronic signatures. The distinction between an advanced electronic signatures and an advanced electronic signature bearing a qualified certificate, is emphasised in the EU Regulation.

2.101 Capitec Bank maintains that the deviations from the principles stipulated in the Electronic Commerce Model Law and the Electronic Signature Model Law as well as a mis-understanding of the EU Directive has led to a mis-direction on the part of the drafters of the ECT Act. On a proper reading of the EU Directive it is also clear that what is intended is that

where an accreditation or qualification by a public body was required that an advanced electronic signature could be qualified by such public body. This is where the confusion has arisen. The ECT Act attributes the term 'advanced electronic signature' to an electronic signature which is accredited by the Accreditation Authority (this being the same as a qualified electronic signature defined in the EU Regulation). Thus even though we have taken this terminology from the EU Directive the ECT Act does not treat advanced electronic signatures in the same manner that it is treated in the EU Directive or now in the EU Regulation

2.102 Capitec Bank maintains that this is made abundantly clear by the EU Regulation (which will repeal the EU Directive) which clearly recognises advanced electronic signatures as signatures that do not require any qualification or accreditation. It is also recognised that advanced electronic signatures created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures in conformity with the requirements of a supervisory body, will be regarded as qualified electronic signatures.

2.103 Capitec Bank notes that the EU Regulation contemplates, in the same manner as we have dealt with accreditation in South Africa, that a public supervisory body confirms that the provider of qualified electronic signatures meets all of the requirements of the EU Regulation. Thus, the EU Regulation contemplates the broad scope of electronic signatures, within that scope the concept of advanced electronic signatures is defined in the EU Regulation, and within the scope of advanced electronic signatures the potential for qualification of those signatures by a public supervisory body is also recognised.

Capitec Bank provides the following illustration:

Figure 1 – South Africa

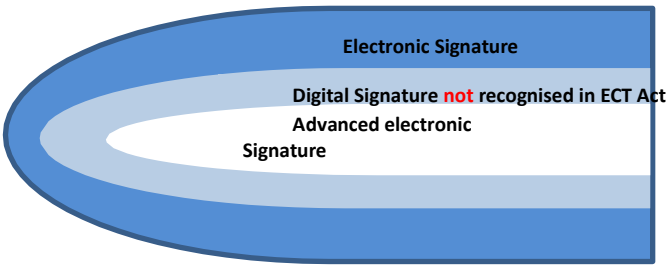
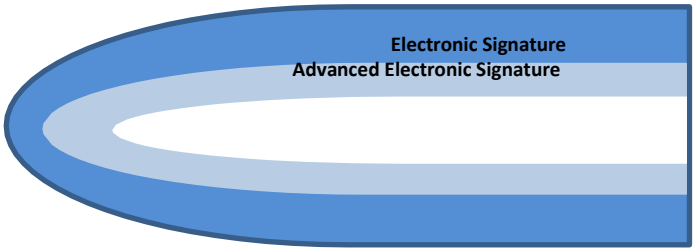


Figure 2 – European Union



2.104 Capitec Bank notes that this has resulted in our law on electronic signatures being 'out of step' with international development and not least of which the EU Directive on which our law of electronic signatures is based. Therefore the ECT Act is in serious need of review and, where necessary, revision. Failure to address the mis-directions of the drafters of the ECT Act will continue to create barriers to electronic communications and the use of electronic signatures. It will also lead to a perpetuation of the difficulties that we currently experience relating to electronic evidence, its admissibility and assessment of its weight in legal proceedings.

2.105 Capitec Bank notes that a further consequence of the misalignment will be difficulty in the recognition of foreign electronic signatures in South Africa as well as the potential disqualification of South African electronic signatures from recognition in other jurisdictions.

2.106 Capitec Bank notes that an electronic signature is by definition a 'data message' and therefore the principles relating to electronic evidence, developed and established in the Electronic Communications Model Law, adopted in the ECT Act and also stipulated in the EU Directive, relating to both the admission and the weight of evidence of data messages, apply equally to evidence relating to electronic signatures. These principles include the assessment of the weight of evidence, regard being had to the reliability of the manner in which the signature (constituted by a data message) was generated, stored or communicated, the reliability of the manner in which the integrity of the data message (signature) is maintained, the manner in which the originator was identified (a critical element in the case of digital and advanced electronic signatures), and any other relevant factor.

2.107 Capitec Bank notes that the vast majority of communications signed electronically are signed using electronic signatures, which have no inherent security and no defined process of linking the signature to a particular person. These signatures are not reliable signatures as defined in the Electronic Signatures Model Law nor are they advanced electronic signatures as defined in the EU Directive. However, in the absence of the signature

being disputed, our courts will, and have, afforded legal recognition to these 'insecure' signatures.[50]

2.108 Capitec Bank notes that the intention to sign in the context of an electronic signature may be evidenced in many ways. Section 13(5) of the ECT Act allows for an 'expression of intent' where an electronic signature is not necessarily required, but nonetheless allows that the intent of the signature can be inferred. Therefore where a person accepts associated writing by clicking an 'I ACCEPT' button on a digital display, this is a positive action from which intent can be inferred. Similar principles would apply to the manner in which electronic signatures may be applied to electronic records in an electronic online environment from which the intent of the signatory may be inferred. From an evidentiary perspective if a signatory asserts lack of intent, the court may take into account all relevant circumstantial evidence in this regard. This is no different from any dispute as to whether intent was present where intent is required in law.

2.109 Capitec Bank notes that in the case of a digital or advanced electronic signature the application of the signature requires certain active steps required to use the technology necessary for their application to a writing. In this regard, unless the signatory can positively show a clear lack of understanding of the technologies used to apply an advanced electronic signature, it is highly unlikely that a defence, on the part of the signatory that there was no intention to use the signature, will be sustained.

2.110 Capitec Bank notes that both the concept of 'reliable signature' in the Electronic Signature Model Law and 'advanced electronic signature' in the EU Directive are defined to incorporate all of the criteria that apply to digital signatures based on asymmetric encryption provided in PKI. Both asymmetric encryption (used in digital signatures) and PKI are subject to internationally recognised standards.

2.111 Capitec Bank recommends the implementation of a 3 tier system, which recognises:

(a) electronic signatures;

50 See *Spring Forest Trading 599 CC v Wilbury Ecowash and Others* (725/13) [2014] ZASCA 178 (21 November 2014).

(b) secure electronic signatures meeting the criteria which are materially similar in their definition of advanced electronic signatures in the European Union and reliable signatures in the Electronic Signature Model Law; and
(c) signatures which are accredited by a public supervisory body.

2.112 Capitec Bank notes that another fact which should be taken into account in considering the electronic signature framework in South Africa is that the new South African ID card is capable of facilitating the issue of advanced electronic signatures to South African citizens. The ability to link the stringent identification processes applicable to the issue of an identity document to advanced electronic signatures, facilitated by smart identity cards should also be taken into account in considering potential benefits of each citizen having an advanced electronic signature. The importance to South Africa's information economy and to the e-government initiatives that are contemplated in the ICT Policy are obvious.

2.113 Capitec Bank notes that in this scenario the Department of Home Affairs will not only become the Certification Authority for advanced electronic signatures (incorporating the Registration Authority function confirming the identity of signatories which is currently part of its identity process) but these advanced electronic signatures will then be capable of being used for online identification in instances where the identity of signatories needs to be established without the necessity for face-to-face identification.

2.114 Capitec Bank submits that the effort that is made in identifying and verifying the physical identity of citizens could synergistically provide the same certainty to the identity of digital citizens in their online communications and transactions.

2.115 Mark Heyink rejects the notion of abolishing the distinction between electronic signatures and advanced electronic signatures. He notes that the result of merely abolishing the distinction between advanced electronic signatures and electronic signatures without establishing a framework for reliable signatures (and possibly even advanced or qualified electronic signatures for use in limited circumstances) would be reckless. It would not advance the cause of secure electronic commerce (in fact it would be a regressive step) and is totally out of line with modern thinking on information security, cybersecurity and the protection of personal information. It will result in fertile ground for fraud and unnecessary litigation.

2.116 On the issue of biometrics Mark Heyink notes that Biometrics relate to the physiology of a person. In the context of signature, handwritten signatures are biometric in nature as they can be linked to the physiology of a person. The link between a person and the signature made by a person can be established by appropriate forensic testing of the signatures. This link is therefore a physiological link and falls under the category of 'biometric identification'. He notes that the physiological link that exists between the signatory and the signature with handwritten signatures, is absent in electronic signatures by their very nature.

2.117 Heyink notes that what must also has to be recognised in addressing this issue, is that biometrics, immediately they are captured and used in digital form, are nothing more than a data message and are susceptible to amendment, as is any other data message, unless allied to secure encryption technologies. Biometrics, as it is hoped is demonstrated in the examples below, are nothing more than one of the factors of authentication of the identity of a person. They should not be seen in themselves to be a solution to the issue of signatures although it must be recognised that with the advance of technology and the ever and quickly decreasing cost of using biometrics, their promise to fulfil some of the functions that we attribute to signatures is good. This having been said, biometric technologies have not advanced sufficiently, nor has the cost of their use been decreased sufficiently for it to be feasible for biometric technologies to be used on their own as reliable signatures.

(b) Evaluation and recommendation

2.118 'Signature' is a wide concept. The Guide to the Model Law provides in par 53 that the following functions of a signature may be noted:

- to identify a person,
- to provide certainty as to the personal involvement of that person in the act of signing,
- to associate that person with the content of a document.
- to attest to a person's intent to be bound by the contents of a signed contract,
- to endorse authorship of a text, or
- to confirm physical presence, namely that at a certain time that party was physically present at a certain place.

2.119 It may be noted that, alongside the traditional handwritten signature, there exist various types of procedures (e.g., stamping, perforation), that are sometimes also referred to as 'signatures', which provide various levels of certainty, exist alongside the handwritten signature. The concept of a signature has been adapted so that in certain contexts a stamp, perforation or even a typewritten signature or a printed letterhead might be regarded as sufficient to fulfil the signature requirement. At the other end of the spectrum, there exist requirements that combine the traditional hand written signature with additional security procedures such as the confirmation of the signature by witnesses or the function of notaries in certifying a signature.[51]

2.120 The intention of the person applying the electronic signature may thus be to fulfil any of these functions. The Act gives legal recognition to any method of signing an electronic documents or message, namely anything from a password to a scanned 'wet' signature, as long as the person applying it intends the data to fulfil the function of a signature and she applies it in the form of data in or attached to, or logically associated with other data.

2.121 Electronic signatures can take a variety of forms and, depending on the nature of the transaction, could range between simply writing your name at the end of an email to the use of complex biometric-identification technologies. Alongside 'advanced electronic signatures' based on public key cryptography, there are various other devices which may currently be used, or considered for future use, with a view to fulfil in one or more of the functions of a handwritten signature. For example, certain techniques would rely on authentication through a biometric device. Where samples of the identifier would have been previously analysed and stored by the biometric device.

2.122 The Act makes provision for 'electronic signatures' and 'advanced electronic signatures'. A technology-neutral approach has been adopted. The two concepts, namely 'electronic signatures' and 'digital signatures', should not be confused. Remember that although a 'digital signature' is an 'electronic signature', the latter concept is much wider.

51 See Guide par 54.

2.123 Electronic signatures include all technologies for replacing handwritten signatures in the electronic environment, namely by use of a digital pen, PIN-codes, scanned signatures and digital signatures. Digital signature is the name for a method of signing electronically by using public-key infrastructure (PKI)[52] encryption systems. A digital signature is thus one way in which an electronic signature may be created.

2.124 Biometric techniques can be based on physiological or behavioural identifiers. Examples of physiological identifiers include fingerprint, finger geometry, hand geometry, iris recognition, retina pattern, face recognition (geometry and thermal imaging), palm pattern, voice recognition, vein pattern and DNA. Examples of behavioural identifiers include signature verification and keystroke dynamics.

2.125 However, where law requires the signature of a person 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.[53] For example, where a law (such as the Copyright Act) requires a signature, only an advanced electronic signature will be valid. Advanced electronic signatures are presumed to be a valid electronic signature and to have been applied properly, unless the contrary is proved.[54] Some confusion exists whether the term 'required by law' should be interpreted widely – meaning statutes and their enabling regulations and forms.[55] Where the term is capable of a wider interpretation it would mean that safety records, medical records and the like must be accompanied by an advanced electronic signature to comply with the requirements of the ECT Act.[56]

2.126 An advanced electronic signature has a higher evidential value than electronic signatures. Should the signatory dispute the validity of his or her advanced electronic

52 Public Key Infrastructure (PKI) is a set of policies and procedures to establish a secure information exchange see https://docs.oracle.com/cd/B10501_01/network.920/a96582/pki.htm.
53 See s 13(1).
54 See s 13(4).
55 See Mark Heyink 'Response to Notice 1537 of 2004: Notice Inviting Comment on Proposed Accreditation Regulations drafted in terms of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002) at page 2-3.
56 See Mark Heyink 'Extracts of comment made on the Electronic Communications and Transactions Bill submitted with the 'Response to Notice 1537 of 2004: Notice Inviting Comment on Proposed Accreditation Regulations drafted in terms of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002

signature, he or she bears the onus of proving that in court. In the case of an electronic signature, the normal rules of attribution apply, and a party relying thereon must prove that the signatory validly applied the signature

2.127 Section 13(3) provides that parties may sign a contract electronically. Where the parties to an electronic transaction have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if—

- a method is used to identify the person and to indicate the person's approval of the information communicated; and
- 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.

2.128 Section 13(3) is based on article 7 of the UNCITRAL Model Law on Electronic Commerce. One major difference between section 13(3) and article 7, however is that article 7 of the Model Law applies where the law requires a signature, whereas section 13(3) of the ECT Act apply where the parties require an electronic signature for an electronic transaction and the parties have not agreed on the form or type of electronic signature to be used.

2.129 Aashish Srivastava and Michel Koekemoer[57] have examined the electronic signature regime in South Africa and have noted several flaws in the provisions of the ECT Act. The authors submit:

> Section 13(3)(b) is clearly vague and ambiguous, making it difficult to attribute a precise meaning to its provisions. Such language in the ECTA gives an opportunity to a party to a transaction that required a signature to attempt to escape its obligations by denying that any of the parties' signatures were valid on the ground that the method of signature employed was not as reliable as appropriate in the circumstances. Moreover, if such a dispute was referred to court, the entire contract may get invalidated on the ground that the electronic signature was not appropriately reliable in such circumstances. The appropriateness of an electronic signature may also fail to be the same for a day-to-day transaction as it is for complex business transactions involving large sums of money. Note that after adopting the MLEC in 1996, the UNCITRAL decided to examine the issue of electronic signatures exclusively. This led to the development of the Model Law on Electronic Signatures (hereinafter referred to as the 'MLES') in 2001. Article 6 of the

57 See 2.118 Aashish Srivastava and Michel Koekemoer 'The Legal Recognition of Electronic Signatures in South Africa: A Critical Overview' *African Journal of International and Comparative Law* 21.3 (2013): 427–446.

MLES, which is a replication of article 7 of the MLEC (on which section 13(3) of the ECTA is based) provides guidance on where an electronic signature will be considered reliable and appropriate for the purpose of a specific document. Article 6(3) states that an electronic signature is considered to be reliable if:

(a) the signature creation data are linked to the signatory;

(b) the signature creation data were, at the time of signing, under the control of the signatory;

(c) any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

It is interesting to note that the provisions in article 6(3) of the MLES are similar to section 38(1)(a)–(d) of the ECTA discussed above. Section 38(1) of the ECTA lays down the criteria for the accreditation of products and services in support of advanced electronic signatures.

Thus, if the reliability clause laid down in section 13(3) of the ECTA is interpreted with the help of article 6(3) of the MLES, which is similar to section 38(1)(a)–(d) of the ECTA, one comes to the conclusion that the electronic signature used under section 13(3) must be an advanced electronic signature. The only difference would be that the identification of the user need not necessarily be face to face, the requirement under section 38(1)(e). Thus, implicitly, section 13(3) of the ECTA makes provision for digital signatures because no other form of electronic signature technology can presently satisfy the reliability test. In other words, prima facie the ECTA seems to be a two-pronged approach legislation similar to the ES Directive; however, when examined in detail, it is a technology-specific legislation that mandates the use of digital signatures for legally enforceable electronic transactions in South Africa.[58]

2.130 Article 9(3) of the Electronic Communications Convention provides where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and

(b) The method used is either:

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above, by itself or together with further evidence.

58 See Srivastava and Koekemoer op cit at 432-433.

2.131 Srivastava and Koekemoer[59] maintain that while article 9(3) of the Electronic Communications Convention contains fairly similar provisions to article 7 of the Model Law and section 13(3) of the ECT Act, it includes one new provision, namely, article 9(3)(b)(ii). They note:

> This new provision in the Convention helps it retain a technology-neutral approach and also resolves the anomaly associated with the reliability test as it validates a signature method – regardless of its reliability in principle – whenever the method used is proven in fact to have identified the signatory and indicated the signatory's intention in respect of the information contained in the electronic communication.[60]

2.132 The ECT Act differentiates between a certification-service-provider and an authentication service provider. In terms of section 1 of the ECT Act an authentication service provider provides authenticated and accredited products, and a certification service-provider provides authenticated (but not accredited) advanced electronic signatures. Nevertheless, section 38(4), by referring to section 38(1), does permit certification-service-providers to issue accredited advanced electronic signatures.[61]

2.133 The voluntary accreditation of certification-service-providers is also inconsistent with international best practice.[62]

2.134 Apart from the drafting criticisms that can be directed at the provisions of the ECT Act, we need to take note of important international developments. The most important development in the regulation of electronic signatures is the EU Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation) that was adopted in July 2014.[63] This is an important development as it introduces various new ways in which trust in online services can be enhanced.

2.135 Substantively, eIDAS is in two parts. The first section deals with government-recognized electronic identification systems and establishes a legal framework that will allow all EU member states to mutually recognize each other's identification systems. This section

59 See Srivastava and Koekemoer op cit at 442.
60 Ibid.
61 See Srivastava and Koekemoet op cit at 434.
62 Ibid.
63 See 910/2014 and also Commission Implementing Decision (EU) 2015/296 of 24 February 2015 on procedural arrangements for Member States cooperation on eID; Commission Implementing Regulation (EU) 2015/806 of 22 May 2015 on the form of the EU Trust Mark for Qualified Trust Services; Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means

targets the public sector and requires Member States to permit citizens from other member states to use their own electronic IDs to access their online services.

2.136 The second section of eIDAS deals with electronic signatures. It clarifies existing rules, but also introduces a new legal framework for electronic signatures and seals. The Regulation provides for the admissibility of all electronic signatures and verification services as evidence in legal proceedings.[64] This includes electronic signatures, seals, time stamps, registered delivery services and certificates for website authentication.

2.137 eIDAS also includes a definition of the service companies that provide these electronic signatures, seals and stamps – Trust Services, namely qualified and non-qualified Trust Services.

2.138 The definition of electronic signature remains the same as under the 1999 Directive[65] and there is a provision for the legal recognition of electronic signatures their admissibility as evidence in legal proceedings. Advanced Electronic Signatures (AES) allows for the unique identification and authentication of the signer of a document and enables the verification of the integrity of the signed agreement. The signer's certificate is cryptographically bound to the document using the private key uniquely held by the signer, and also produces the effect of a tamper-evident seal protecting the integrity of the document. During the validation process, the reciprocal public key is extracted from the signature and used to both authenticate the signer's identity through the trusted issuing CA and to confirm that no changes were made to the document since it was signed. Although these certificates have existed for many years, eIDAS enables the signer to use the latest technologies, like mobile devices, to accomplish this.[66]

2.139 A new and third type of signature defined under eIDAS is the Qualified Electronic Signatures (QES) based on Qualified Certificates issued by CAs which have been accredited and supervised by authorities designated by the EU member states and meet the

64 See Regulation 25.
65 Directive 1999/93/EC.
66 See Dan Puterbaugh 'Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation' March 2016 available at http://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/.

requirements of eIDAS. Qualified Certificates must also be stored on a qualified signature creation device such as a smart card, a USB token, or a cloud based trust service.[67]

2.140 eIDAS also introduced the recognition of electronic seals and Qualified electronic seals. These are similar to electronic signatures but only available to legal persons such as corporate entities. This raises the interesting prospect of minimizing the importance of the 'authorized signer' for a particular entity.[68]

2.141 *Issue 5: the SALRC recommends that a three-tier approach be adopted for the regulation of electronic signatures in line with the European Union Regulation.*

2.142 *The SALRC recommends that the ECT Act should be amended to provide for standards for the accreditation of foreign signatures.*

2.143 *It is furthermore recommended that the ECT Act be amended to link the national electronic identification scheme to access to public services; introduce other electronic trust services related to electronic delivery service, electronic seals, time stamps, and website authentication.*

B Evidence and the ECT Act

1. Admissibility of electronic evidence in criminal and civil proceedings

(a) Background

2.144 Issue 2: Are the provisions in the ECT Act adequate to regulate the admissibility of electronic evidence in criminal and civil proceedings?

67 See Dan Puterbaugh 'Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation' March 2016 available at http://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/.

68 See Dan Puterbaugh 'Understanding eIDAS – All you ever wanted to know about the new EU Electronic Signature Regulation' March 2016 available at http://www.legaltechnology.com/latest-news/understanding-eidas-all-you-ever-wanted-to-know-about-the-new-eu-electronic-signature-directive/.

2.145 Section 15(1) essentially removes the barriers that have been created by an interpretation of best evidence and the hearsay rules to allow for the admission of evidence and section 15(2) stipulates that such evidence must be given due evidential weight.

2.146 Section 15(3) provides the guidance and framework to approach the assessment of the weight of electronic evidence with due regard to circumstantial evidence (the electronic records themselves, the reliability of the information systems processing the information and the integrity of the information).

(b) Exposition of comment

2.147 The Banking Association South Africa submitted that the ECT Act should be the prevailing legislation to provide for evidence provisions relating to the use and admissibility of electronic evidence in criminal and civil proceedings.

2.148 Advocate IM Bredenkamp notes that the ECT Act is a fairly recent legislative development and that it is best to leave it to the courts to clarify, and alert the authorities should problems arise with the interpretation and application thereof.

2.149 The Law Society of South Africa supports the amendment of existing provisions rather than the repeal of these provisions and the introduction of a new statute to regulate documentary evidence or hearsay and documentary evidence. It notes that the initial objection by our courts was that all computer evidence constituted hearsay evidence and this led to the untenable situation where a vast majority of important and relevant evidence was not automatically admissible. This is what the ECT Act - our law for already 12 years and under which huge tracts of electronic evidence have been introduced into our courts as evidence without material difficulty - had sought to address.

2.150 The issue of whether poor programming of computers or failures in operation by administrators of computers or information systems may pervert evidence is more than adequately dealt with in section 15(3) of the ECT Act, which deals with the reliability of the computer itself and the integrity of evidence produced using computers. It is in this sphere that - due to the general lack of understanding by attorneys, advocates and presiding officers of

the principles of information security that inform the reliability and integrity of data messages (electronic communications and records) and the assessment of the weight of electronic evidence - the difficulties occur.

2.151 Mark Heyink notes that there seems to be no reason why the framework which will be informed by other factors relating to information security should be any different in criminal or civil proceedings. Regardless of what proceedings are contemplated, assessing the weight of evidence goes to an assessment essentially of the integrity of the information. To the best of my understanding we do not make any distinctions in this process in criminal and civil proceedings save for the higher thresholds that apply in criminal law relating to proof.

2.152 He notes that there appears to be no cogent reason for removing section 15 from the ECT Act. Subject to the comments made on this issue, he agrees that striving to attain consistency in approach and harmonising the provisions dealing with hearsay and best evidence is important.

(c) Evaluation and recommendation

2.153 *Issues surrounding electronic evidence and especially the adequacy of the provisions in the ECT Act is discussed in detail in Chapter 3 below.*

2.154 The SALRC recommends law reform, through the introduction of a single statute to regulate electronic evidence as set out in Annexure A.

CHAPTER 3 ELECTRONIC EVIDENCE

A Hearsay evidence

1. The interrelationship between section 15 of the ECT Act and other statutory exceptions

(a) Background

3.1 Issue 6: Should section 15 of the ECT Act prescribe that a data message is automatically admissible as evidence in terms of section 15(2) and a court's discretion merely relates to an assessment of evidential weight based on the factors enumerated in section 15(3)?

3.2 Should a 'data message' constitute hearsay within the meaning of section 3 of the Law of Evidence Amendment Act?

3.3 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) of the Criminal Procedure Act; and Part VI (documentary evidence) of the Civil Proceedings Evidence Act?

(b) Exposition of comment

3.4 The Banking Association South Africa agreed that electronic evidence, such as data messages, should not be exempt from the hearsay rule and that the question of the production and admissibility of automated electronic evidence should be clarified.

3.5 The Law Society of South Africa recognises that there is some confusion amongst members of the profession in relation to:

- hearsay as it applies to electronic evidence;
- the authentication of electronic evidence;
- the admissibility of business records in terms of Section 15(4) of the ECT Act;
- the interaction between (and applicability of) the various laws that regulate exceptions to the hearsay rule; and
- obtaining and producing electronic evidence.

3.6 Mark Heyink notes that in dealing with the issue of hearsay evidence, what must be understood is that from the perspective of electronic evidence, initially all evidence emanating from a computer was regarded as hearsay evidence. Judgments in this regard led to practical difficulties relating to electronic evidence. This motivated the drafting of the Computer Evidence Act, the provisions of which, while possibly being workable in the context of a computer in a computer room with a 'white-coated' programmer being able to provide evidence, became redundant immediately computers became networked. Even at the time that the Computer Evidence Act was promulgated its application was extremely limited and would be regarded as absolutely absurd in the interconnected world. This has been remedied by the repeal of that Act in the Electronic Communications and Transactions Act ('ECT Act').

3.7 He notes that the ECT Act (particularly Chapter III which defines the legal requirements of data messages) is materially identical in form to the Electronic Commerce Model Law on Electronic Commerce, which is the basis of the development of legislation relating to the admission of electronic records in many jurisdictions globally. The interpretation that normal rules of hearsay, governing the exclusion of evidence based on the credibility of another who is not 'in court' and capable of being cross-examined, appears from reported cases to have been more than adequately dealt with by our courts to date.

3.8 The Law Society of South Africa submits that the evidentiary provisions in Section 15 of the ECT Act are adequate and do not require any material amendment or replacement by other provisions, save for section 15(4).[69] Concern is expressed that this section may be

69 The following alternative formulation of Section 15(4) is suggested:

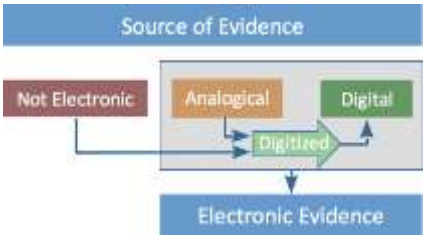
interpreted to automatically elevate certain data messages to constitute proof of facts in dispute. In addition, it is not clear whether all data messages made by a person in the ordinary course of business require certification, or only copies, printouts or extracts from such data messages.

(c) Evaluation and recommendation

3.9 Electronic evidence is comprised of data that has potential probative value and that is generated, processed, stored on or transmitted by any electronic or digital device. Digital evidence is evidence which has been generated or converted to a numerical format. Electronic evidence comprises of both evidence that has been 'born digital' and evidence that has not been 'not born digital' but that became digitised during their life-cycle.[70]

3.10 The Sources of electronic evidence in aptly illustrated in Figure I below.

Figure 1: From Sources of Evidence to Electronic Evidence[71]



3.11 Importantly for litigators, the ECT Act provides a simple but powerful procedure for the certification of electronic evidence, making it firstly admissible in evidence and secondly rebuttable proof of the facts it contains. It is simply required that 'an officer' in the service of

---

A data record adduced by a person, or a copy or printout of or an extract from such data record, certified to be correct by that person or by another person duly authorised by the adducer to do so, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible as rebuttable evidence of the information contained in such record, copy, printout or extract.

70 Maria Angela Biasiotti, Mattia Epifani, Fabrizio Turchi 'The Evidence Project: Bridging the Gap in the Exchange of Digital Evidence across Europe' available at http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/The-EVIDENCE-Project-Bridging-the-Gap-in-the-Exchange-of-Digital-Evidence-Across-Europe.pdf (accessed 8 August 2016).

71 Maria Angela Biasiotti, Mattia Epifani, Fabrizio Turchi 'The Evidence Project: Bridging the Gap in the Exchange of Digital Evidence across Europe' available at http://sadfe2015.safesocietylabs.com/wp-content/uploads/2015/10/The-EVIDENCE-Project-Bridging-the-Gap-in-the-Exchange-of-Digital-Evidence-Across-Europe.pdf (accessed 8 August 2016).

the person who entered or created the data message certifies as correct a data message which is either 'made by a person in the ordinary course of business' or which is a copy, printout or extract from such data message in order for such evidence to be best evidence.

3.12 It has been noted that Section 15(4) counters a potential gap in South African law upon the repeal of the Computer Evidence Act 1983[72] any differences between the wording of Section 15 and Article 9 of the UNCITRAL Model Law are stylistic in nature. The intention behind this section is to ensure the admissibility of data messages in legal proceedings, and to establish their evidential value.

3.13 The Johannesburg High Court was asked to consider electronic evidence not certified as correct in terms of the ECT Act, highlighted the value of the certification procedure. In *Ndlovu v The Minister of Correctional Services*[73] concerned a delictual claim for wrongful imprisonment.[74] Electronic evidence was led regarding parole violations which had been recorded on a computer program by more than one person. The court held that unless the person who entered the data on the computer was called as a witness, the computer printout constituted hearsay evidence. It was also held that data messages must comply with the same requirements as paper-based evidence namely, they must be relevant and otherwise admissible, their authenticity must be proved and the original document must normally be produced (unless it is the best evidence that the party presenting it could reasonably be expected to obtain).

3.14 In addition to the normal rules of evidence, the court applied section 15(3) of the ECT Act which requires it to consider 'the reliability of the manner in which the data message was generated, stored or communicated... the reliability of the manner in which the integrity of the data message was maintained; the manner in which its originator was identified; and any other relevant factor'.

3.15 The learned judge commented that on his reading of the ECT Act, electronic evidence certified in accordance with Section 15(4) stands as evidence without further qualification unless it is rebutted by the opposing party and in particular, is not required to be assessed in

72 See Ryk Meiring 'Electronic Transactions' *Cyberlaw @ SA II* at 89; also refer to section 92 of the ECT Act.
73 2004 JDR 0328 (W) judgement delivered May 19, 2004,
74 See Annexure 'D' for a synopsis of the issues dealt with by the court.

terms of the additional four aspects set out in Section 15(3). While the judge's comments do not form a part of the reasoning for his decision and are accordingly not binding, they do serve to highlight the benefits of the certification procedure. The procedure immediately relieves the party presenting the electronic evidence of a substantial evidential burden and transfers that burden to the opposing party, which is then required to present evidence (if the evidence is to be rebutted).[75]

3.16 The Western Cape High Court recently addressed this issue. In *S v Terrance Stephan Brown*[76] a trail within a trail was held to determine the admissibility of three photographs that was found of the accused on a phone which was found at the scene of a crime. The admissibility of the photographs would then be used to offer proof, or render it more probable, that the phone, Exhibit 1, on which they were found, belonged to the accused and must have been dropped by him at the scene of the crime.

3.17 The court noted that the ECT Act follows an inclusionary rather than an exclusionary approach to the admission of electronic communications as evidentiary material.[77] The court noted that it agrees with the observation of Gautschi AJ in *Ndlovu v Minister of Correctional Services and another*[78] that section 15(1)(a) does not render a data message admissible without further ado. The provisions of section 15 certainly do not exclude our common law of evidence. This being the case the admissibility of an electronic communication will depend, to no small extent, on whether it is treated as an object (real evidence) or as a document.[79] The court noted that section 221(5) of the CPA provides that a document includes any device 'by means of which information is recorded or stored'. [80]

3.18 In *Seccombe and others v Attorney-General* [81] it was noted that the word document 'is a very wide term and includes everything that contains the written or pictorial proof of something. It does not matter of what material it is made'.[82] The court in *S v Terrance Stephan*

75 Tim Fletcher 'Certification of electronic evidence – a powerful tool in South African litigation'.
76 (Case No: CC 54/2014) Western Cape High Court.
77 See par 17.
78 [2006] 4 All SA 165 (W) at page 172.
79 See *S v Terrance Stephan Brown* par 18.
80 See *S v Terrance Stephan Brown* par 19.
81 1919 TPD 270.
82 See *Seccombe and others v Attorney-General* 277.

Brown concurred that graphics, audio and video that are in a data message form should be treated in the same way as documents.[83]

3.19 The court noted that the images at issue were vulnerable to potential mutability and that the transient nature in which images of this nature are generated, stored and transmitted by an electronic device dictates that they should more appropriately be dealt with as documentary evidence rather than *'real evidence'*. The court concurred with the approach followed in *S v Ndiki and others*[84] where Van Zyl J expressed the view[85] that the first step in considering the admissibility of documentary evidence is to examine the nature of the evidence in issue in order to determine what kind of evidence one was dealing with and what the requirements for its admissibility are.[86]

3.20 The images in question were downloaded from the phone, reproduced in hard copy (paper) form and enlarged. There was no suggestion that either the devices or the software which were used to produce or enlarge the images was unreliable or that he manipulated the data or electronic communication in any way.[87]

3.21 The court then addressed the various other objections to the admissibility of the images raised on behalf of the accused. Firstly, it was contended that the data message or images amounted to hearsay.[88] The court noted that section 3(4) of the Law of Evidence Amendment Act[89], defines hearsay evidence as evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence.[90] The court noted that the three images which the State seeks to introduce as evidence are photographs, apparently of the accused, and, subject to proof of his identity and bearing in mind the limited purpose for which they are tendered, their probative value stands or falls by that simple fact.[91] In this sense, at least, the images are more akin to

83 See *S v Terrance Stephan Brown* par 19 where the court referred to J Hofman 'Electronic Evidence in criminal cases,' (2006) *SACJ* 257 at page 268.
84 [2007] 2 All SA 185 (CK)
85 At paragraph [53]
86 See *S v Terrance Stephan Brown* par 18.
87 See *S v Terrance Stephan Brown* par 21-22.
88 Ibid at par 25.
89 45 of 1988
90 See *S v Terrance Stephan Brown* par 25.
91 Idem.

being 'real evidence' but, however they are classified, they do not constitute hearsay evidence.[92]

3.22 The integrity of the chain from the time that the phone was allegedly picked up by Cronje to the time that it was handed to the police was also questioned by the counsel for the accused. [93] The court conceded that there was a four hour window period during which any number of persons could have tampered with the phone, but noted that it was a short period of time and there was no evidence that the phone or the images had been tampered with.[94] The court noted that any form of interference or tampering would have to have involved the manipulation of pre-existing images on the phone, a much more unlikely scenario than the placing of such images on the phone in the four hour window period.[95] The court noted that tampering with the images required no small degree of technical skill and that it was important that Linnen's evidence was that the images in question had been transmitted to the phone on 7 March 2014 was undisputed. The court held that in light of the evidence as a whole it considered the lack of proof of the integrity of the phone for the four hour period as insufficient to justify the exclusion of the evidence. [96]

3.23 The court held that the three images were admissible as evidence.[97] In conclusion the court observed that it is worth noting that the process envisaged by section 15(2)-(3) of the ECT Act, namely to assess the evidentiary weight of the electronic communication sought to be introduced in evidence will only be addressed after all the evidence has been heard.[98]

3.24 One may conclude that the hearsay rule is very much alive, that section 15 did not take away a court's discretion to determine the evidentiary weight of evidence and that for section 15(4) to apply, and the correct certification procedure should be followed.

3.25 Issue 6: in line with the principle of technological neutrality, the SALRC supports the view that hearsay evidence made by a *person in an electronic document should be treated in the same way* as *hearsay evidence in* a *paper-based document. On the*

92 Idem.
93 Section 15(3)(b) of the ECT Act provides that in assessing the evidential weight of a data message, regard must be had to – the reliability of the manner in which the integrity of the data message was maintained.
94 See *S v Terrance Stephan Brown* par 26.
95 Idem.
96 Idem.
97 See *S v Terrance Stephan Brown* par 34.
98 S v Terrance Stephan Brown par 33.

interaction of the ECT Act with the CPEA, the CPA and the LEAA, the SALRC supports a less *fragmented approach to the admissibility of documentary evidence and therefore proposes reform: through amending and supplementing existing provisions.*

2. Hearsay and mechanically produced evidence

(a) Background

3.26 Issue 7: Should the ECT Act or other relevant legislation) make a clear distinction between *mechanically produced evidence without the intervention of the human mind* (akin to real evidence) and *mechanically produced evidence with the intervention of the human mind* (hearsay)?

(b) Exposition of comment

3.27 The Banking Association South Africa agrees with the proposition by the SALRC to maintain a distinction between automated data messages and data messages 'made by a person' and support statutory reform to guide the production and proof of both types of evidence in court.

3.28 The Banking Association South Africa submits that a handbook should be developed that will provide clarity and guidance to legal practitioners and judicial officers on the legal position and advice on technical aspects of producing electronic evidence in court.

3.29 The Law Society of South Africa notes that the *Ndlovu* case[99] interprets this issue correctly. The correct interpretation of Section 15 allows for the distinction between hearsay

99 Where Gautschi AJ expressed the following view: *'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.'*

and real evidence to be easily made. The purposes of Section 15(1) and (2) do not intend doing away with the hearsay rule but are rather aimed at ensuring that it is not used to disqualify the admission of data messages in evidence. The Law Society of South Africa maintains that sub-section 15(3) of the Act provides a more than adequate balance in dealing with so called 'real evidence' in allowing for evidential weight of a data message to be dependent upon 'the reliability of the manner in which the data message is generated, stored or communicated'. Regardless of the categorisation of the evidence as hearsay or real, the integrity of the evidence is dependent upon the reliability of the computer processing the information.

3.30 Mark Heyink notes that In so far as the distinction between real and documentary evidence is concerned, in the former instance it is accepted that this is information which is generated without human intervention. In the latter instance it is information where the input of the information and its processing is influenced by humans. If the main issue underlying evidence is the integrity of the evidence that is placed before a court, both of these issues are addressed in Section 15(3) of the ECT Act. In the case of direct evidence, it is the reliability of the computer processing the information which has to be evidenced.

3.31 He notes that while the fact is that the computer generates this information without input from a human being, in doing so it is nonetheless 'acting' on the instructions of the programmer of the software which initiates this automatic processing. It must be recognised that software is far more complex than purely mechanical solutions that our courts have previously dealt with. It must also be recognised that this programming, although automatic, may fail for various reasons. For instance malware or a virus may influence operation of the software, rendering the automatic processing of supposedly 'real' evidence unreliable. Thus, reliability and presumptions of reliability are an important factor in assessing the weight of evidence, whether it is real or documentary. Turning to documentary evidence, again it is submitted that Section 15(3) of the ECT Act adequately deals with this in addressing the assessment of the weight of evidence. The second element of ensuring the integrity of the information processed is properly addressed by this provision.

(c) Evaluation and recommendation

3.32 In certain instances a party will communicate with the world through an automated website which requires a minimum of actual human input, but where the system will automatically generate responses to messages received from customers. For instance a website may be programmed to receive orders which have been electronically completed by customers. Once received, the system will generate an acknowledgment of receipt of the order, check the levels of stock ,check the payment details of the buyer (for instance with the credit card company) and if sufficient stock is available and payment is cleared, generate a message to the dispatch department to send the item to the buyer.

3.33 Human intervention will only take place where the goods are physically removed from the store and sent to the buyer. Where electronic goods are ordered this may not even be necessary as the goods can be sent electronically without human intervention. For instance if you buy software on the Internet, the software is usually sent without any human intervention. In terms of section 20 where electronic agents are used, the offer or acceptance generated by the electronic agent will be regarded as a declaration of will of the party on whose behalf that computer and electronic agent has been programmed.

3.34 An automated transaction therefore is a transaction where one or both of the parties make use of automated systems, i.e. a program that communicates with or responds to third parties without any human intervention. The offer or acceptance is made by the computer program without referring any decision for actual human input. In this case the computer and computer program constitutes an electronic agent. A typographical or grammatical error in section 20(d) should be corrected and section 20 should be reworded so that it can be more easily understood.

3.35 Attribution should also be considered. Attribution concerns whether an electronic event may be related to a person, thus a key issue in the licensing of intellectual property on the Internet. To be more specific, in e-commerce, attribution refers to the manner in which one determines whether a data message (electronic communication) originates from a specific person, or machine (for automated communication systems). Attribution deals with whether a data message was actually sent by the person who is indicated as its originator, and with the circumstances in which one may assume that it actually originated from that

person. With a paper-based communication, the problem usually concerns forged signatures, or the unauthorized use of a person's letterhead. In the e-commerce environment, similar problems may arise. For example, an unauthorized person may have sent a message from another's e-mail account; or, a person may fraudulently have used another's authentication code, encryption, or the like.

3.36 'Attribution' should not be confused with 'authentication', which term is sometimes as an alternative for 'electronic signature'.[100] We are addressing the rules and presumptions relating to the attribution of electronic events, but not with the attribution of authenticated messages (such as an advanced electronic signatures).[101]

3.37 Specific rules for the creation, recognition, and control of authentication products and services have been enacted. The legal force of an otherwise attributable message is limited by the formal authentication and certification requirements.[102]

3.38 At common law, where a message or action is sought to be attributed to a person in court, the person who alleges attribution shoulders the burden of proof. A person who wants to produce a document has to prove that it is authentic.[103]

3.39 Whether a person created a document or signed it, or both, is solved by leading the evidence of the maker, the signatory, or the witnesses, and sometimes a handwriting specialist, and of other surrounding circumstances[104] In *CRC Engineering (Pty) Ltd v JC Dunbar & Sons (Pty) Ltd*[105] the court held that when the authenticity or the execution of a document is put in issue, the burden of proof is on the party seeking to rely on that document, and that she proves such authenticity by calling the person who signed it, or someone who saw her sign it.[106]

---

100 Randolph A Kahn & Dianne J Silverberg 'From Mount Sinai to Cyberspace: Making Good E-business Records' (2001) 57 Business Lawyer 431 at 432; Jane Kaufman Winn & Michael Rhoades Pullen 'Despatches from the Front: Recent Skirmishes Along the Frontiers of Electronic Contracting Law' (1999) 55 Business Lawyer 455 at 462.

101 See s 13(4) of the ECT Act.

102 General Usage for International Digitally Ensured Commerce (GUIDEC)) drafted by the International Chamber of Commerce (ICC) Information Security Working Party, under the auspices of the ICC Electronic Commerce Project available at <http://www.iccwbo.org/home/guidec/guidec.asp>.

103 *S v Swanepoel* 1980 (1) SA 144 (NC); see also Vivienne Lawack-Davis (*Aspects of Internet Payment Instruments* (unpublished LLD thesis University of South Africa, 2000) 296.

104 See *Policansky Bros Ltd v L & H Policansky* 1935 AD 89 at 90-91; LH Hoffmann & DT Zeffertt South African Law of Evidence 3rd ed (1981) 308-309.

105 1977 (1) SA 710 (W) at 711-712.

106 See also *Annama v Chetty* 1946 AD 142 at 150.

3.40 The actions of a machine are normally attributed to the person who instructed or programmed it to perform a specific function (see, for example, the definition of the 'author' of a computer-generated work).[107] It has been suggested that where mistakes occur in electronic communications through the malfunction of machines, the party that installed the malfunctioning machine must assume the risk of any defects or delays in the transmission.[108]

3.41 In terms of article 13(1) of the Model Law, a data message is the originator's if it was sent by her. It is deemed to have been sent by her if it was sent by a person who had the authority to act on her behalf in respect of that data message, or by an information system programmed by, or on behalf of, the originator to operate automatically.[109] An addressee may regard a data message as the originator's and act on that assumption if the addressee properly applied a procedure previously agreed to by the originator for that purpose (to ascertain whether the data message was the originator's), or the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or any agent of her agents enabled that person to gain access to a method used by the originator to identify data messages as her own.

3.42 Paragraph (3) does not apply as of the time when the addressee has received notice from the originator that the data message is not hers, and has reasonable time to act accordingly; or, in the second instance in paragraph (3), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not the originator's.[110] It will be very difficult to know that the notice is actually from the originator if the authentication procedure did not work properly vis-á-vis the previous message.[111]

---

107 s 1(1) sv 'author' of the Copyright Act 98 of 1978; *Entores Ltd v Miles Far East Corporation* [1955] All ER 493 (CA); *Thornton v Shoe Lane Parking* [1971] 1 All ER 686; Michael Chissick & Alistair Kelman Electronic Commerce Law and Practice 2nded (2000) 77).

108 See AJ Kerr *The Principles of Law of Contract* 5 ed (1998) 110-111; for a discussion of 'electronic wizardry', and fault on the part of the offeror and the equipment used by her, see also MCJ Olmesdahl 'Unheralded Demise of Wolmer versus Rees' (1984) 100 *SALJ* 545 at 553.

109 Art 13(2).

110 Art 13(4).

111 See Arno R Lodder 'Electronic Contracts and Signatures: National Civil Law in the EU Will Change Drastically Soon', paper delivered at 15th BILETA Conference 'Electronic Datasets and Access to Legal Information', held on 14 April 2000 at the University of Warwick (available at <http://www.bileta.ac.uk/00papers/lodder.html>).

3.43 Where a data message is the originator's, or deemed to be hers, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee may regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee may not do so when she knew or should have known, had she exercised reasonable care or used any agreed procedure that the transmission resulted in any error in the data message as received.[112] Paragraph (5) has been interpreted as a rule relating to mistake or error in the electronic environment that conflicts with national laws. The addressee may rely on an electronic record as long as she acts in good faith and is unaware of any mistake.[113]

3.44 The purpose of article 13 is not to assign responsibility. Rather, it deals with the attribution of data messages by establishing a presumption that under certain circumstances a data message is considered to be as the originator's, and qualifies that presumption where the addressee knew or ought to have known that the data message was not the originator's. Earlier drafts of the Model Law contained an additional provision to the effect that the attribution of authorship of a data message to the originator should not interfere with the legal consequences of that message, which should be determined by other applicable national law. It was later felt that it was not necessary to express that principle in the Model Law but that it should be mentioned in the Guide.

3.45 Some countries have adopted article 13 in national law. They include Bermuda[114] Mauritius[115] the Philippines[116] and Singapore.[117] Countries that have rejected the Model Law approach have done so because mainly because article 13 creates rules that conflict with the principle of functional equivalence. Their approaches range from making no provision for on attribution to adopting a limited version of article 13.

3.46 The ECT is in line with international best practices as far as attribution is concerned. Section 25 states that a data message is the originator's if it was sent by

- the originator personally;

112 See art 13(5).
113 Art 13(5) read with art 13(4); see Christina Hultmark Ramberg 'The E-commerce Directive and Contract Formation in a Comparative Perspective' 22, available at <http://www.juridicum.su.se>.
114 See s 10 of the Electronic Transactions Act of 1999.
115 See s 11 of the Electronic Transactions Act of 2000.
116 See s 18 of the Electronic Communications Act of 2000.
117 See s 13 of the Electronic Transactions Act.

- a person who had authority to act on the originator's behalf in respect of that data message; or
- an information system programmed by or on behalf of the originator to operate automatically, unless it is proved that the information system did not properly execute such programming.

We support this approach for several reasons.

3.47 It is in line with our common law.

- The principle of functional equivalence dictates this: it will be wrong to adopt rules that create disparity between paper-based and electronic-based transactions.
- International best practices dictate it.
- The standards and allocation of risk adopted in article 13 have their origin in a provision relating to another, more specialized type of electronic communication – article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order.

3.48 This Model Law drew substantially on the attribution procedures in article 4A of the Uniform Commercial Code relating to fund transfers. These standards were developed in the specialized context of high-value electronic fund transfers. This is perhaps the main reason why the provisions of article 13 have not been accepted or adopted universally.

3.49 The final phrase in Section 25(c) ' … unless it is proved that the information system did not properly execute such programming' was inserted when the ECT Act was being considered before the Portfolio Committee on Communications, and can possibly be viewed as a helpful but strictly unnecessary reference to the rebuttable nature of these provisions.[118] Similarly, had the person referred to in Section 25(a) not personally transmitted the data message, or had the person referred to in Section 25(b) not been appropriately authorized to act on behalf of the originator (and subject to the rules associated with estoppel), that originator will be able to lead evidence of such fraud, and should be able to prove any agreement concluded on the basis of such misrepresentation void *ad initio*.[119]

118 See Meiring 'Electronic Transactions' *Cyberlaw @ SA II* at 100.
119 See Meiring 'Electronic Transactions' *Cyberlaw @ SA II* at 100; Christie op cit at 330.

3.50 Issue 7: the SALRC supports the maintenance of a distinction between automated data messages and data messages 'made by a person' and proposes statutory reform (see Annexure A) to guide the production and proof of both types of evidence in court.

3.4. In addition, the SALRC supports the development of a handbook or a Guide on obtaining and producing electronic evidence that will provide clarity, to practitioners and judicial officers, on the legal position and advice on technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

3. Authentication of electronic evidence

(a) Background

3.51 Issue 8: 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?

(b)Exposition of comment

3.52 The Banking Association South Africa notes that whilst Section 15(3) of the ECT Act provides valuable guidelines for assessing the evidential weight of a data message, it sees value in statutory reform as there may be growing uncertainty with technological advances regarding certain aspects addressed/or not addressed in the ECT Act.

3.53 The Banking Association South Africa submits that reform along the lines as suggested by the SALRC will go a long way to achieve clearer articulation of both statutory and non-statutory guidelines for the authentication and weight of documentary evidence, including electronic evidence. We support the repeal of existing provisions and the introduction of a unitary statute containing provisions articulated in clauses 7 and 8 of Annexure A of the paper.

3.54 The Law Society of South Africa is of the opinion that a review is not necessary at present, and that the Court should be allowed to test the aspect of authenticity further.

(c) Evaluation and recommendation

3.55 Issue 8: the SALRC supports the clearer articulation of both statutory and non-statutory (in the form of a handbook/manual) guidelines for the authentication (and weight) of documentary evidence, in particular electronic evidence, and in addition proposes that the court be expressly vested with the discretion to exclude unfairly prejudicial evidence.

3.56 The SALRC proposes reform through amending and supplementing existing provisions such as those articulated in clauses 7 and 8 of Annexure A.

4. Admissibility of business records

(a) Background

3.57 Issue 9: The admissibility of business records:

- 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 Jaw on reverse onus provisions?

(b) Exposition of comment

3.58 The Banking Association South Africa supports the repeal of Section 15(4) and the provision of legislative amendments that will provide for the admissibility of business records. The Banking Association South Africa also supports the introduction of a unitary statute to regulate documentary evidence or hearsay and documentary evidence. The Banking Association South Africa is of the opinion that certificates may well be used to confirm business records as hearsay or otherwise.

3.59 The Law Society of South Africa is of the opinion that the proposed amendment would do away with a special statutory dispensation for business records only. The following alternative formulation of Section 15(4) is suggested: A data record adduced by a person, or a copy or printout of or an extract from such data record, certified to be correct by that person or by another person duly authorised by the adducer to do so, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible as rebuttable evidence of the information contained in such record, copy, printout or extract.

(c) Evaluation and recommendation

3.60 The SALRC proposes reform through amending and supplementing existing provisions of the ECT Act (see in particular clause 6 of Annexure A).

5. Presumptions for mechanical devices

(a) Background

3.61 Issue 10: A presumption of regularity:

- In the Discussion Paper the SALRC provisionally recommended that the law of evidence should not prescribe a presumption of regularity in relation to mechanical devices but should include, in civil proceedings, a limited presumption (placing an evidential burden on the other party who did not object on notice). The question remains whether the law of evidence should prescribe a presumption of regularity in relation to mechanical devices (involving automated operations such as speedometers and breath-testing devices).

(b) Exposition of comment

3.62 Mark Heyink agrees with the SALRC recommendation for the most part. However, he notes that this recommendation fails to take into consideration the presumptions which should apply in uncontested matters. He notes that the practicalities of the administration of justice demand that certain "presumptions of reliability" and "presumptions of regularity" are recognised.

3.63 The LSSA draws attention to the persuasive judgment in the matter of the *Trustees for the time being of the Delsheray Trust and Others (as appellants) and Absa Bank Limited (as respondent)*.[120]

3.64 The LSSA notes that although the judges dealt with the common-law as opposed to the provisions of the ECT Act, the comments of the learned judges are particularly pertinent to the assessment of the weight of evidence in terms of Section 15(3)(a) being the reliability of the manner in which the data message was generated, stored or communicated.[121] In this regard, the judges indicate that generally the presumption of reliability has not been applied in South African law under that name but that the underlying principles of the presumption are established in our law. It exists by virtue of the doctrine of judicial notice and that these principles are firmly established in our law.

3.65 The judges quote Corbett JA in the matter of the *State v Mthimkulu*,[122] where Corbett noted "The extent to which the court will insist upon, or relax, the standards of proof which theoretically apply when evidence involving the use of scientific instruments is presented to it will very much depend upon (a) the nature of the process and the instrument involved in the particular case, (b) the extent, if any, to which the evidence is challenged, and (c) the nature of the enquiry and the facta probanda in the case. No hard and fast rule can, or should, be laid down. Much will depend on the facts and circumstances of each individual matter."[123]

---

120 (A504/13) [2014] ZAWCHC 152; [2014] 4 All SA 748 (WCC) (9 October 2014).
121 See paragraphs 37 to 43 and paragraphs 49 to 51.
122 1975 (4) SA 759 (A).
123 At 765 A – B. See also *Gamede and Othes v S* (AR 434/08) [2009] ZAKZPHC 40 (4 September 2009).

3.66 The LLSA notes that considering the complexity of computers and at this stage the relevant ignorance of most lawyers and jurists as to the workings of a computer, the wisdom of Corbett JA (even though the matter was decided in 1974) resonates today.

3.67 The LSSA notes that judicial notice is to a large degree subjective and may vary from judge to judge. However, one of the overriding issues that needs to be considered in the interests of the administration of justice is that, when evidence is not challenged and there are no clear reasons to doubt the evidence which is put before the court, judicial officers should presume reliability.

3.68 In its consideration of the facts, the learned judges referred to an extract from *Ex Parte Rosch*:[124] a court would be failing in its duty if it ignored the realities of modern science and technologies in the production of evidence. In 1997 courts are entitled to accept that computers are ubiquitous in the society in which we live. The process by which these instruments record and print information is no less commonplace than the operation of motor vehicles and cameras. It is not necessary that there should be evidence as to how each computer works as a prerequisite to the admissibility of evidence produced by such computer, if what has been produced has been done so automatically."[125]

3.69 The LLSA notes that the sentiments expressed in this judgment are trite and should be even more compelling in our world some 18 years after the judgment was delivered. However, the LSSA cautions that sight must not be lost of the fact that there are continuous and rapid developments in technologies and their use. Sometimes these developments are not necessarily matched by the safeguards of the integrity of information which may be processed.

3.70 The learned judges in the *Delsheray* case then go on to base the presumption of reliability on four factors. The first of these is credence given to a large commercial bank in the assumption that its computer systems are as sophisticated as other financial institutions. The LSSA notes that the assumption is more supportive of a presumption of reliability. The second factor is the employment of appropriate personnel filling the responsibility to ensure operation of the computer system is "proper". The LSSA notes

[124] [1998] 1 or SA 319 [W].
[125] At par 42.

that these are issues which are based on information security principles and the same presumptions as apply to the first factor would be more appropriate.

3.71 The third factor relates to the nature of the evidence itself. In this regard, whether the evidence is challenged or not is a critical determinant. It is however submitted that in uncontested matters the presumption should be that the person providing a certificate in terms of Section 15(4) has not acted fraudulently.

3.72 The fourth factor is that in this matter the respondent's computer records with respect to the account in dispute are accessible to the client. This is an important determinant as in the majority of cases (certainly not all), by virtue of modern technologies, customers or clients generally have an insight into the processing of their information, whether it be personal or financial.[126] Thus obvious errors would in many cases be evident to clients or customers well in advance of any legal action being taken.

3.73 The learned judges go on to deal with the issue of human input as hearsay evidence. They note that this may be overcome by reference to Section 3(1)(c) read with Section 3(4) of the Law of Evidence Amendment Act. The court noted that one of the issues which must be borne in mind is that, by the nature of computer evidence, in many cases the input to records is provided from difference sources. This may result in a plethora of witnesses having to be called if the hearsay rule was strictly applied.

3.74 The LSSA notes that an alternative to the application of the statutory exception of hearsay evidence as referred to above is the "presumption of regularity". The court has found that this has been applied in our law[127] before and that there is a significant degree of overlap between the "presumption of reliability" and the "presumption of regularity". On that basis the court found in the particular case that the arguments in favour of the application of the presumption of reliability applied equally to the "presumption of regularity".

3.75 In conclusion, LSSA notes that the court found that computer-generated information, although it may contain evidence which was input by different parties, was

[126] It was noted that laws such as the Protection of Personal Information Act 4 of 3013, the National Credit Act 35 of 2005 and the Consumer Protection Act 68 of 2008 are predicated on the principles of transparency.
[127] *R v Minors*; *R v Harper*.

sufficient for a person relying on the accuracy of the records to depose to an affidavit, verifying the information in the records relied upon and enforcing a claim (this matter related to an application for summary judgment and therefore reliance was placed on an affidavit).

3.76 The LSSA notes that with regard to Section 15(4) the provision of a certificate where a matter is uncontested will achieve the same function as an affidavit. Indeed, in this particular instance an affidavit is required in terms of the rules of court as the application was for summary judgment. The same requirement is not necessary in applications for default judgment.

3.77 Legal Aid maintains its previous position, namely that insofar as criminal cases are concerned, a presumption of regularity in respect of speedometers and breath testing devices "would have the effect of placing at the very least an evidential burden on an accused person who would normally not have the resources to meaningfully rebut as it would involve the leading of expert evidence". For this reason we opposed a presumption of regularity in criminal cases. This remains our position. In any event, the onus is on the state to prove its case beyond a reasonable doubt.

3.78 Legal Aid notes that insofar as civil cases are concerned, if the plaintiff were to give notice in terms of clause 6 of the Draft Bill and the defendant failed to object thereto, or the court dismissed his objection, then in terms of clause 6(4)(b) the document attached to the notice would "be presumed, in the absence of evidence to the contrary, (to be correct in respect of) the nature, origin and contents of the document as shown on its face". If the defendant were to object, he would have the onus of proving the mechanical device not to have been properly functioning, despite a certificate of calibration provided by the plaintiff. There appears to be no objection thereto.

3.79 Legal Aid reiterates that the threshold requirements would be that the plaintiff would have to attach to his notice a copy of the report generated by the mechanical device concerned. In addition he would have to attach a certificate of calibration and also a certificate of competence in respect of the operator.

(c) Evaluation and recommendation

3.80 Some have proposed the adoption of a presumption of the integrity of a computer. The presumption has a limited scope namely (i) where evidence is adduced supporting the finding that the computer was operating properly, (ii) where the electronic record was recorded or stored by a party who has opposite interest to the party who seeks to introduce it in a proceedings, or (iii) where the electronic record was recorded or stored by whom is not a party to a proceedings or whom did not record or store the electronic record under control of a party seeking to introduce it. In short, such presumption applies where there is evidence on the proper operation of a computer or where there is no conflicting or suspicious interest of the party who seeks to introduce the electronic record in a proceeding.[128]

3.81 This is a sound approach for electronic record systems.

3.82 *Issue 10: the SALRC provisional recommends that the law of evidence should not prescribe* a *presumption of regularity in relation to mechanical devices.*

3.83 *The SALRC recommends the adoption of* a *limited presumption (placing an evidential burden on the other party who did not object on notice) in civil proceedings.*

3.84 *The SALRC recommends the adoption of a limited presumption of integrity for electronic record systems.*

3.85 *The SALRC further recommends that the question of presumptions receive the attention of* a *standing committee/working group established in terms of the recommendations of this Report.*

[128] See the comments on the ITU Model Law on article 6(2) -- *ITU Electronic Evidence: Model Policy Guidelines & Legislative Texts* (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013) https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Documents/FINAL%20DOCUMENTS/ENGLISH%20DOCS/e-evidence_mpg.pdf.

6. Admissibility of computer generated evidence

(a) Background

3.86 Issue 11: In general, are the provisions in the ECT Act sufficient to regulate the admissibility of computer generated evidence?

(b) Exposition of comment

3.87 The Banking Association South Africa cautions against a presumption of regularity which includes that 'in the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time'.

3.88 The Banking Association South Africa agrees with the SALRC recommendation that the question of presumptions should be dealt with by a standing committee/working group to be established in terms of the recommendations of the discussion paper.

3.89 The Law Society of South Africa notes that in *the Trustees for the time being of the Delsheray Trust and Others v Absa Bank Limited*[129] the court held that while the presumption of reliability has not been established in our law under that name, it exists by virtue of the doctrine of judicial notice and that these principles are firmly established in our law.

3.90 With regard to Section 15(4) and comments previously made relating to the additional overhead of affidavits as opposed to certificates, the Law Society of South Africa submits that the provision of a certificate where a matter is uncontested will achieve the same function as an affidavit. Indeed, in this particular instance an affidavit is required in terms of the rules of court as the application was for summary judgment. The same requirement is not necessary in applications for default judgment.

3.91 The Banking Association South Africa submits that the ECT Act provisions in general have proven to be effective but we support the notion to explore the development of new measures to assist courts in the discovery and inspection of electronic documents. The

129 2014 High Court of South Africa (Western Cape Division) judgment delivered on 9 October.

Banking Association South Africa appreciates the opportunity to be part of any committees/forums to be created in the reform process.

3.92 Advocate IM Bredenkamp notes that on face value the provisions of section 15 of Act 25 of 2002 is sufficient to regulate the admissibility of computer generated evidence. The LSSA is also of the view that the ECT Act is sufficient to regulate the admissibility of computer generated evidence.

3.93 However, the LSSA also supports the recommendation that the Rules Board consider amendments to the rules of court to provide for the discovery and inspection of electronic documents and submits that such revisions would greatly promote the administration of justice.

3.94 It is clear that the admissibility and evidential weight of disputed data message (including ordinary emails, attached electronic files and electronically stored records) depend on an 'integrity' assessment.

3.95 It is also clear that the 'integrity' of a disputed electronic document cannot be properly assessed from a paper printout of that electronic document, but only from an electronic copy of the document containing file metadata, i.e. information contained in the electronic copy that typically evidences when, and by whom, an electronic document was originally created, whether it was revised or edited, to whom it may have been sent and when it was received.

3.96 Accordingly, should the admissibility or evidential weight of a paper printout of an electronic document be challenged in contentious litigation, it results in significant wasted costs and delays that could otherwise have been avoided had electronic copies of those documents been produced.

3.97 Internationally, civil procedure rules have been amended to address these issues by catering for the proper discovery and production of electronic documents before trial. For example, in the United Kingdom, the importance of electronic file metadata was recognized by an amendment to the civil procedure rules relating to discovery in October 2005 which revised the definition of a 'document' in the UK's civil procedure rules to now specifically include 'additional information stored and associated with electronic documents known as 'metadata'. If the rules are not amended as above, it will be difficult for a Court, in possession of only a paper copy of, for example, an email, and faced with admissibility challenge in respect of that

email (irrespective of whether the challenge is bona fide or deliberately obstructive), to find good cause for allowing the disputed paper version to be used at trial because: (i) the 'best evidence' of that email would not have been produced in terms of Section 15(1)(b) of the ECT Act if the original electronic copy could have been produced, (ii) the 'integrity' of that email would not easily be capable of passing assessment in terms of Section 15(3) of the ECT Act and (iii) the 'original' of that email would not have been made available for inspection or produced at Court in terms of Rules 35(6) and (10) read in the light of Section 14 of the ECT Act.

3.98 If the rules were amended as outlined above, then not only would the rules regarding production of documents be more closely aligned with Sections 14 and 15 of the ECT Act but the process of obtaining copies of electronic documents would also become significantly more cost-efficient for litigants and their legal representatives. In addition, parties would also be in a proper pre-trial position to evaluate evidence and to consequently make informed, time-saving concessions during pre-trial conferences as to which documents may, without any further proof, serve as evidence of what they purport to be in terms of Rule 37(6)(k).

3.99 For the reasons outlined above, the Law Society of South Africa submits that Rules 35(2) and (6) should be amended and further submissions will be made directly to the Rules Board in this regard.

(c) Evaluation and recommendation

3.100 This matter was dealt with in a recent judgment in *S v Terrance Stephan Brown.*[130] This was a trail within a trail held to determine the admissibility of three photographs that was found of the accused on a phone which was found at the scene of a crime. The court addressed the question of originality. The court noted that section 14 of the ECT Act provides that a data message satisfies the requirements of original form if the integrity of the information from the time when it was first generated in its final form as a data message has passed assessment in terms of sec 14(2) and, secondly, that information is capable of being

130 (Case No: CC 54/2014) Western Cape High Court.

displayed or produced to the person to whom it is to be presented. The second requirement is clearly met (the images were downloaded and printed).

3.101 As regards the first requirement, sec 14(2) provides that integrity must be assessed

(a) by considering whether the information has remained complete and unaltered;

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

(c) having regard to all other relevant circumstances.'[131]

The State tendered evidence that the images could be traced back to a certain phone or phones which transmitted them to Exhibit 1.[132] Linnen testified that the software he used precluded him from tampering with the images. The court noted that there was no evidence or even a suggestion that any person tampered with the phone or, more accurately, the images stored thereon, although the phone was in unknown hands for at most four hours that night before being handed over to Major Muller.[133] Furthermore, what evidence there is indicates that the phone was in the hands of lay persons in the four hour period and it is thus improbable that any tampering with the images in question took place.[134] The court held that it was most significant that Linnen's evidence was that the data downloaded revealed that the images in question had been transmitted to the phone two days before the shooting at a stage when, on the available evidence, the phone was in the hands of the original owner or possessor.[135]

3.102 As regards the images being in their original form the court held:

> In my view, on a conspectus of this evidence, the requirements of original form and of sec 14 of the ECTA have been met. In any event sec 15(1)(b) of the ECTA gives data messages a further exemption from the requirement of original form *'if it is the best evidence that the person adducing it could reasonably be expected to obtain'*. In the light of the lack of any evidence as to who originally transmitted the images to the phone, ***Exhibit 1,*** and the limited purposes for which the evidence was tendered, namely, to prove that the phone belonged to the accused, I consider that the State could not reasonably be expected to have produced better evidence of these images. Finally, as regards authenticity, I consider that, seen as a whole, Linnen's evidence establishes the authenticity of the images in question which, in any event, was not disputed by the accused, the apparent subject of the images.[136]

131 See section 14(2)(a)-(c) of the ECT Act.
132 Ibid at par 22.
133 Idem.
134 Idem.
135 Idem.
136 See *S v Terrance Stephan Brown* par 23.

3.103 *Issue 11: the SALRC recommends that the Rules Board for Courts of Law (the Rules Board), perhaps assisted by a standing committee/working group with technical expertise be requested to consider amendments to the rules of court to provide for the discovery and inspection of electronic documents. The SALRC notes also that the Rules of Court may require amendment in the event of statutory reform that requires notice prior to trial to be given in respect of an intention to rely on hearsay or documentary evidence, as well as notice of any objections to the use thereof to enable parties to prepare for trial.*

CHAPTER 4 LAW REFORM

A Recommendations for law reform

(a) Background

4.1 In considering these and related issues in the current Discussion Paper, the SALRC highlights several areas of confusion, and considers three broad options or possible approaches to law reform that may be pursued.

4.2 **Option 1:** Retention of the current regulatory landscape (possible minor reform). This approach would result in the retention of the current regulatory framework, possibly with the introduction of minor statutory reform (for example the substitution of current definitions in the CPA and the CPEA).

4.3 The advantage of such an approach is that relatively few changes to the current regulatory framework would be required, which would cause minimal disruption to the legal profession and would most likely be introduced fairly rapidly. However, this conservative approach would mean that multiple laws would still apply.

4.4 The disadvantages of this scenario include the likelihood that confusion would continue to exist about certain laws and principles, including the following:

- hearsay as it applies to automated electronic evidence (and the seeming hesitance to treat electronic evidence as real evidence);
- the authentication of electronic evidence;
- the admissibility of business records in terms of section 15(4) of the ECT Act; and
- the interaction between (and applicability of) the various laws that regulate exceptions to the hearsay rule.

4.5 Option 2: Introduction of Electronic Evidence specific legislation or guidelines: This option would also largely retain the current regulatory framework (with possible minor statutory reform) but in addition would introduce legislation[137] more detailed than section 15 of the ECT Act, specifically to address the admissibility of electronic evidence. The question of admissibility would focus on issues such as the authentication and reliability of electronic evidence. The content of such legislation may be informed by the provisions of the Draft Model Law on Electronic Evidence[138] commissioned and published in 2002 by the Commonwealth Secretariat.

4.6 The Model Law was published to assist Commonwealth jurisdictions grappling with legislative reform in the context of electronic evidence, and was endorsed by the Commonwealth Law Ministers as a Commonwealth model of good practice.

4.7 Option 2 would provide greater clarity on the admissibility and production of electronic evidence than Option 1. However, Option 2 would not resolve the potential confusion – and possible deviation from a functional equivalence approach[139] – caused by the multiple sources of law that would still apply to hearsay and documentary evidence.

4.8 Option 3: Reform of the current regulatory landscape: The third option involves a more extensive overhaul of the regulatory framework for hearsay and certain types of documentary evidence. This approach would include two aspects:

- The repeal of existing provisions on the admissibility of hearsay evidence and certain types of documentary evidence (primarily business records, including banking records) in terms of the CPA, CPEA, LEAA and the ECT Act.
- The introduction of a single statute to regulate the admissibility of such evidence, in terms of authentication, and the best evidence rule.

4.9 Option 3 would require the enactment of legislation along the lines of that set out in Annexure A. Option 3 would achieve the objectives of both Options 1 and 2, and would also reduce the opportunity for confusion that arises from the current multiple sources of law regulating the admissibility of such evidence.

137 Or possibly Regulations in terms of the ECT Act.
138 Draft Model Law on Electronic Evidence (2002) available at *http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BE9B3DEBD-1E36-4551-BE75-B941D6931D0F%7D_E-evidence.pdf* Accessed 31 July 2012.
139 On the meaning of 'functional equivalence' see n **Error! Bookmark not defined.**.

(b) Exposition of comment

4.10 The Banking Association of South Africa notes that the current legislative framework dealing with hearsay evidence and admissibility of electronic evidence is uncertain and is dealt with in different statutes, for example the Criminal Procedure Act, the Civil Proceedings and Evidence Act, the Law of Evidence Amendment Act and the ECT Act.

4.11 The Banking Association of South Africa prefers Option 3 which deals with the reform of the current regulatory landscape.[140] It must be noted that such a reform will have a huge impact on the systems and processes that banks use, which should be taken into account during the review process.

4.12 An important development is the first draft Convention on Electronic Evidence as proposed by Mason.[141] The main objective of the draft convention is to pursue a common policy towards electronic evidence, taking into account the differences in the treatment of evidence in individual jurisdictions. Secondly, the aim is to encourage judges and lawyers to more fully understand the concept of electronic evidence in the interests of providing for fairness in legal proceedings; to promote adequate procedures in legal proceedings, to implement appropriate legislation where necessary, and to promote international co-operation. The text, reproduced in Annexure B, draws on several key resources.[142] These resources were considered in the preparation of the Draft Bill.

(c) Evaluation and recommendation

4.13 The SALRC recommends the adoption of a law on electronic commerce.

---

140 See p 87 of the Discussion Paper.

141 See http://conventiononelectronicevidence.org/ (accessed 10 August 2016).

142 Stephen Mason, *Electronic Evidence* (3rd ed, LexisNexis Butterworths, 2012), 4.21; Commonwealth Draft Model Law on Electronic Evidence; Electronic Evidence: Model Policy Guidelines & Legislative Texts (Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean, International Telecommunication Union Telecommunication Development Bureau, Geneva, 2013); Stephen Mason, 'Electronic evidence: A proposal to reform the presumption of reliability and hearsay', *Computer Law and Security Review*, Volume 30 Issue 1 (February 2014), 80 – 84; Council of Europe *The Use of Electronic Evidence in Civil And Administrative Law Proceedings and its Effect on the Rules of Evidence and Modes of Proof: A Comparative Study and Analysis* (Council of Europe, European Committee on Legal Co-operation, 2015).

CHAPTER 5

RECOMMENDATIONS AND PROPOSALS FOR LEGISLATIVE REFORM

A. Recommendations: The ECT Act

5.1 The SALRC recommends a review of the ECT Act. Many of the provisions of the ECT Act have never been implemented or have become obsolete. By and large, there seems to be consensus that the ECT Act should be reviewed as a matter of priority.

5.2 The definitions in the ECT Act should be amended. The ECT Act's definition of a data message includes 'voice, where the voice is used in an automated transaction'. The SALRC proposes deleting this from the definition of a data message. The SALRC proposes the expansion of the definition of a data message to embrace future technologies that are not 'electronic'. It is thus not necessary to define 'electronic'. The SALRC proposes the expansion of the definition of a data message to include 'digital, magnetic, optical and electromagnetic or similar means' by which data messages can be generated, sent, received or stored'.

5.3 Section 14 of the ECT Act is clear regarding what is deemed to be an 'original'.

5.4 The SALRC recommends that the scope of the ECT Act remain unaltered.

5.5 The SALRC recommends that the regulation of electronic signatures in the ECT Act should be amended in line with the European Union Regulation and the adoption of a three-tier approach.

5.6 The SALRC recommends that the ECT Act should be amended to provide for standards for the accreditation of foreign signatures.

5.7 It is furthermore recommended that the ECT Act be amended to link the national electronic identification scheme to access to public services; to introduce other electronic trust services related to electronic delivery service, electronic seals, electronic time stamps, and website authentication.

5.8 The SALRC recommends the establishment of an appropriate forum comprised of multiple stakeholders to conduct the review of the ECT Act.

5.9 The SALRC recommends that the forum should conduct regular reviews of the ECT Act.

B. Recommendations: Electronic Evidence

5.10 The SALRC recommends law reform, through the introduction of a single statute to regulate electronic evidence as set out in Annexure A.

5.11 The SALRC supports the view that hearsay evidence made by a person in an electronic document should be treated in the same way as hearsay evidence in a paper-based document based on the principle of technological neutrality. On the interaction of the ECT Act with the CPEA, the CPA and the LEAA, the SALRC supports a less fragmented approach to the admissibility of documentary evidence and therefore proposes reform through amending and supplementing existing provisions.

5.12 The SALRC supports the maintenance of a distinction between automated data messages and data messages 'made by a person' and proposes statutory reform (see Annexure A) to guide the production and proof of both types of evidence in court.

5.13 The SALRC supports the development of a handbook or a Guide on obtaining and producing electronic evidence that will provide clarity, to practitioners and judicial officers, on the legal position and advice on technical aspects of producing electronic evidence in court to avoid unnecessary confusion.

5.14 The SALRC does not recommend the adopt ion of a presumption of regularity in relation to mechanical devices in the law of evidence. The SALRC further recommends that the question of presumptions receive the attention of a standing committee/working group established in terms of the recommendations of this Report.

5.15 The SALRC recommends the adoption of a limited presumption (placing an evidential burden on the other party who did not object on notice) in civil proceedings (see Annexure A).

5.16 The SALRC recommends the review and amendment of the Rules of Court and other related laws to clear conflicts and inadequacies and to align the law of evidence to the effective use of electronic evidence in courts.

5.17 The SALRC recommends that the Rules Board for Courts of Law (the Rules Board), perhaps assisted by a standing committee/working group with technical expertise be requested to consider amendments to the rules of court to provide for the discovery and inspection of electronic documents. The SALRC notes also that the Rules of Court may require amendment in the event of statutory reform that requires notice prior to trial to be given in respect of an intention to rely on electronic documentary evidence, as well as notice of any objections to the use thereof to enable parties to prepare for trial.

C. Proposals for Legislative Reform

5.18 It is clear that legislative reform is both necessary and desirable to address the current difficulties surrounding electronic evidence in our courts.

5.19 The draft legislation proposed in Annexure A draws on several authoritative sources, namely (a) the first draft Convention on Electronic Evidence as proposed by Mason;[143] (b) the Commonwealth Draft Model Law on Electronic Evidence;[144] and (c) the ITU's Electronic Evidence: Model Policy Guidelines & Legislative Texts[145] and the proposal made in Discussion Paper 131.

5.20 The term 'authentication', which is defined to mean the process by which any electronic record, document or other thing is proven to be what it claims to be was adopted from the Draft Convention.

[143] Hereinafter Draft Convention.
[144] Hereinafter Commonwealth Convention.
[145] Hereinafter ITU Model Law.

5.21 The definitions of the terms ‘business’, ‘business records’ and ‘computer system’ were adopted from the proposal for legislation in Discussion Paper 131.

5.22 The term ‘computer’ which is defined as any electronic or digital device capable of performing mathematical or logical instructions was adopted from the Draft Convention.

5.23 The definition of contents data is any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form. This definition was adopted from the ITU Model Law. The definition of content data refers both to processed and to unprocessed forms of data. It encompasses not only “raw” contents aimed to be transformed in the course of data processing, but also the different data generated as outputs of such a processing activity. Content data also includes a second layer of data, containing “data about data” (metadata). Metadata is a central element of content data.

5.24 Similarly the definition of ‘data’ which means any representation of facts, information or concepts including information in a form suitable for processing in a computer, a computer system or a device. The definition of data also includes the content data (and therefore also metadata). It was adopted from the ITU Model Law. The scope of the proposed Bill is limited to electronic evidence. It thus only includes facts, information, and concepts which have been represented by binary digits.

5.25 The definition of a ‘device’, namely any electronic or digital apparatus or tool operating alone or connected to other apparatus or tools, that process information or data in digital form was adopted from the Draft Convention.

5.26 The definition of ‘digital’, namely anything that relies on technology based on a binary system or any future development or replacement technology was also adopted from the Draft Convention.

5.27 The definition of ‘electronic evidence’, namely evidence derived from data has been adopted from the Draft Convention. Note, however, that only the first part of the definition was adopted. The definition in the Draft Convention were deemed superfluous.

5.28 The definitions of ‘electronic record’ and ‘electronic records system’ were adopted from the Commonwealth Convention.

5.29 The definition of ‘metadata’, namely data that describes other data was adopted from the Draft Convention.

5.30 The definition of a ‘record’, namely anything in which information of any description is recorded was adopted from the Bill proposed in Discussion Paper 131.

5.31 Clause 2 on the scope was adopted from the Bill proposed in Discussion Paper 131.

5.32 Clause 3 is an enabling provision on the admissibility of electronic evidence. It is based on Article 2(1)-(2) of the Draft Convention as well as Clause 2.2 of the Bill proposed in Discussion Paper 131.

5.33 Clause 4 deals with the authenticity of electronic evidence. This clause was drafted with due reference to Article 3(1)-(2) of the Draft Convention and Clause 7.1 proposed in the Bill in Discussion paper 131. The clause is also partly based on Clause 9 of the ITU Model Law as well as Article 5 of the Commonwealth Convention.

5.34 Clause 5 deals with the application of the best evidence rule. It provides that in any legal proceeding, subject to sub-clause (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored. Sub-clause 2 provides that where an electronic record in the form of a printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule. This clause 5 was drafted with reference to an adaptation of Article 4 of the Draft Convention. It is also based on Article 6(1)-(2) of the Commonwealth Convention. Subsection 2 is also based on Clause 8 of the ITU Model Law.

5.35 Clause 6(2) deals with the admissibility of business records and it establishes a limited presumption. It is partly based on Clause 4 of the draft Bill proposed in Discussion Paper 131. Clause 6(2) deals with a presumption of integrity of an electronic records system. This is modelled on Article 7 of the Commonwealth Convention and Article 6(2) of the ITU Model Law.

5.36 Clause 7 deals with standards relating to the preservation of records for the purpose of determining under any rule of law whether an electronic record is admissible. This clause is based on Clause 8 of the Commonwealth Convention and it is also partly based on Clause 10 of the ITU Model Law.

5.37 Clause 8 deals with the proof of matters related to print outs; business records and standards by affidavit. It is based on Clause 9 of the Commonwealth Convention.

5.38 Clause 9 refers to parties' right to cross examination a deponent of an affidavit.

5.39 Clause 10 deals with agreements on the admissibility of electronic records. This clause is based on Article 5 of the Draft Convention. It is also based on Article 11(1)-(2) of the Commonwealth Convention.

5.40 The admissibility of electronic signatures is provided for in clause 11 of the Bill. Clauses 11(1)-(2) are based on Article 12(1)-(2) of the Commonwealth Convention.

5.41 Clause 12 provides that parties must give notice of intention to produce electronic evidence. This clause is partly based on Clause 6 of the Bill proposed in Discussion Paper 131. It should be noted that Clause 6(4) of the Bill proposed in Discussion Paper 131 was not adopted.

5.42 The court has a discretion to exclude or limit the use of electronic evidence or to admit such evidence provisionally. These issues are addressed in clauses 13-14. They are based on Clauses 9 and 10 of the Bill proposed in Discussion Paper 131.

5.43 Clauses 15-17 on the admissibility of electronic evidence from other jurisdictions; the recognition of foreign electronic evidence and signatures and interpretation were adopted from Clauses 8(1), Clause 9(1)-(2) and clause 10(1) of the Draft Convention.

Annexures

ANNEXURE A: DRAFT LAW OF EVIDENCE BILL

REPUBLIC OF SOUTH AFRICA

LAW OF EVIDENCE BILL

(As *introduced)*

(MINISTER FOR JUSTICE AND CONSTITUTIONAL DEVELOPMENT)

[B - 2016]

REPUBLIEK VAN SUID-AFRIKA

WETSONTWERP OP BEWYSREG

(Soos *ingedien)*

(MINISTER VAN JUSTISIE EN STAATKUNDIGE ONTWIKKELING)

[W- 2016]

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

Words underlined with a solid line indicate insertions in existing enactments.

BILL

To regulate the admissibility of evidence so as to provide for the admissibility of hearsay evidence, and for the admissibility and proof of business records and evidence produced by processes, machines and other devices in all legal proceedings; and to provide for matters connected therewith.

BE IT ENACTED by the Parliament of the Republic of South Africa, as follows:

Preamble[204]

1. Definitions

'**authentication**' means the process by which any electronic record, document or other thing is proven to be what it claims to be;

'**business**' includes any activity regularly carried on, whether for profit or not, by the state, any organ of state, any organisation or person;

'**business records**' includes those records created or received in the ordinary course of business;

'**computer**' means any electronic or digital device capable of performing mathematical or logical instructions;

'**computer system**' means a device or a group of interconnected or related devices, which perform functions pursuant to computer programs;

'**content data**' means any data whether in digital, optical, or other form, including metadata, that conveys essence, substance, information, meaning, purpose, intent, or intelligence, either singularly or when in a combined form, in either its unprocessed or processed form.

[204] The Act is intended to clarify, consolidate and align the rules for the admissibility of business records and evidence produced by processes, machines and other devices, while leaving intact existing legislation on (for example) the admissibility of official and public documents.

‘**data**’ means any representation of facts, information or concepts and includes information in a form suitable for processing in a computer, a computer system or a device and it includes the content data;

‘**device**’ means any electronic or digital apparatus or tool operating alone or connected to other apparatus or tools, that process information or data in digital form;

‘**digital**’ means anything that relies on technology based on a binary system or any future development or replacement technology;

‘**electronic evidence**’ means evidence derived from data;

‘**electronic record**’ means data, that is recorded or stored on any medium in or by a computer or other similar device and that can be read or perceived by a person or by computer or any device, and it includes a display, print out or other output of that data and includes business records;

‘**electronic records system**’ includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records.

‘**metadata**’ means data that describes other data;

‘**record**’ means anything in which information of any description is recorded;

2. Application

This Act applies to all criminal and civil proceedings or the legal proceedings before any tribunal in which the rules of evidence apply.

3. Admissibility of electronic evidence

(1) Evidence in electronic form shall be admitted into legal proceedings.

(2) Section 3(1) does not modify any rule that applies to the admissibility of evidence, except in relation to the rules relating to authenticity and best evidence.

4. Authenticity of electronic evidence

(1) The party seeking to introduce electronic evidence in any legal proceeding has the burden of proving its authenticity.

(2) The authenticity shall be established by

(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.

(3) When assessing the authenticity of evidence in electronic form referred to in sub-section (2), the following factors to be considered include but shall not be limited to:

(a) Whether the data (both the content and associated metadata) relied upon in any legal proceedings is an accurate representation of the prevailing and existing state of the data at the time relevant to the legal proceedings.

(b) If the data has changed, for whatever reason, there is an accurate and reliable method of documenting the changes, including the reasons for any such changes from the moment they were identified (and or possibly seized) as potential evidence in legal proceedings.

(c) If the necessary continuity of the data between the moment the data was obtained for legal purposes and its submission as evidence in legal proceedings can be demonstrated.

(d) Any techniques that were used to obtain, secure and process the data should be available to verification and testing.

(e) The technical and organizational evidence must demonstrate that the integrity of the data is trustworthy, and is therefore considered to be reliable and complete, insofar as the data can be complete, which in turn will depend on the circumstances surrounding the data at the time it was identified as of being potentially relevant in legal proceedings.

5. Application of Best Evidence Rule

(1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of an electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of a printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.

6. Business records

(1) Data in the form of business records made by or on behalf of a person in the ordinary course of business, or a copy or printout of or an extract from such data certified to be correct, is admissible 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, as electronic evidence of the facts contained in such a business record, copy, printout or extract against any person, provided:

(a) an affidavit is made by the person who was in control of the information system at the time when the data message was created;

(b) the affidavit contains sufficient information on the authenticity of the electronic evidence as set out in section 4(3) above.

(2) In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances.

(b) where it is established that the electronic record was recorded or stored by a [an opposing] party to the proceedings [who is adverse in interest to the party seeking to introduce it]; or

(c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

7. Standards

For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

8. Proof by Affidavit

The matters referred to in sections 5(2), 6, and 7 may be established by an affidavit given to the best of the deponent's knowledge or belief.

9. Cross Examination

(1) A deponent of an affidavit referred to in section 8 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court, cross examine a person referred to in section 8.

10. Agreement on Admissibility of Electronic Records

(1) Unless otherwise provided in any other statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by an attorney.

11. Admissibility of Electronic Signature

(1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

(3) The signature, execution, or attestation of a document, whether electronic or otherwise, that is required by law to be attested may be proved by any satisfactory means, provided that an attesting witness need not be called to prove that the document was signed, executed or attested if it was signed, executed, or attested by an advanced electronic signature.

12. Notice of intention to produce electronic evidence

(1) Notice of an intention to produce electronic evidence in terms of subsections 3, 4 or 5 must be given-

(a) in writing to every other party to the proceeding, and must include the contents of the electronic evidence and (where applicable) the originator of the data; and if the electronic evidence is to be produced, a print out or a copy of the data including any related metadata must be attached to the notice; and

(b) in sufficient time before the hearing to provide all other parties to the proceeding with a fair opportunity to prepare to inspect the electronic evidence.

(2) A party to the proceeding who is given notice in terms of subsection (1) must, if that party objects to the admission of the electronic evidence, give notice of objection as soon as practicable to the party proposing to offer the statement.

(3) Subsections (1) and (2) may be excluded by agreement of the parties, or by waiver of the party to whom notice is required to be given; or the presiding officer may dispense with the requirement to give notice under subsections (1) or (2)-

(a) if having regard to the nature and contents of the electronic evidence, no party is substantially prejudiced by the failure to give notice under subsection (1); or

(b) if giving notice was not reasonably practicable in the circumstances; or

(c) in the interests of justice.

(4) In any civil proceedings, where the notice in terms of subsection (1) relates to documentary evidence and no party objects to the notice in terms of subsection (1), or if the court dismisses an objection on the ground that no useful purpose would be served by requiring the party concerned to call a witness to produce the electronic evidence,-

(a) the electronic evidence, if otherwise admissible, may be admitted in evidence; and

(b) it will be presumed, in the absence of evidence to the contrary, that the nature, origin, and contents of the electronic evidence are as shown by the content data.

(5) Provision may be made by the Rules of Court specifying the manner in which the duties imposed by this section are to be complied with, including the time allowed for such compliance.

(6) A failure to comply with this section or any Rules of Court provided in terms of subsection (5) does not affect the admissibility of the evidence, but may be taken into account by the court-

(a) in considering the exercise of its powers over the proceedings and in respect of costs; and

(b) as a matter that might adversely affect the weight to be given to the evidence.

(7) In any civil proceeding where a party is permitted under the Rules of Court relating to discovery to inspect a document –

(a) the requirement to prove the authenticity and integrity of the electronic evidence may be dispensed with in circumstances described in those Rules; and

(b) the procedure to be adopted by a party seeking to require proof of the authenticity and integrity of the electronic evidence is set out in those Rules; and

(c) the production of secondary evidence to prove the authenticity and integrity of the Electronic evidence may be permitted in circumstances described in those Rules.

13. Discretion to exclude or limit the use of electronic evidence

The court may refuse to admit electronic evidence or may limit the use to be made of such evidence; if a particular use of the evidence might be unfairly prejudicial to a party or might be misleading or confusing.

14. Provisional admission of evidence

If a question arises concerning the admissibility of any electronic evidence, the court may admit the electronic evidence in question, subject to further evidence being offered later on to establish its relevance and evidentiary weight.

15. Admissibility of electronic evidence from other jurisdictions

(1) Where electronic evidence originates from another jurisdiction, its admissibility is not impaired if the electronic evidence is proven in accordance with Article 4 or the authenticity of the evidence is otherwise demonstrated.

16. Recognition of foreign electronic evidence and signatures

(1) In determining whether or not, or to what extent, data in electronic form is legally effective, no regard shall be had to the geographical location where the data was created or used or to the place of business of its creation, provided the electronic record or document is located in South Africa.

(2) Where the electronic record or document is located in a foreign jurisdiction, sub-section (1) does not apply unless –

(a) the party who adduces evidence of the contents of the electronic record or document has, not less than 14 days before the day on which the evidence is

adduced, served on each other party a copy of the electronic record or electronic evidence proposed to be tendered;

(b) the court directs that it is to apply; or

(c) there is an international treaty in effect establishing recognition of electronic records or documents or of electronic signatures located in the foreign jurisdiction.

17. Interpretation

(1) The provisions of this Act may be interpreted and enforced in light of the internationally accepted principles of technological neutrality and of functional equivalence.

18. Repeal of sections of statutes

Repeals: section 15(4) of the ECT Act

Sections 27 – 38 of the Civil Proceedings Evidence Act (notwithstanding these provisions the Electronic Evidence Act shall apply to electronic evidence)

Sections 221, 222, and 236 of the Criminal Procedure Act (notwithstanding these provisions the Electronic Evidence Act shall apply to electronic evidence)

ANNEXURE B: DRAFT ELECTRONIC EVIDENCE CONVENTION

Part I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

‘attribution’ means the assigning of responsibility for or tracing the origin of an act purported to have been performed or committed using or through a computer device, system or network;

‘authentication’ means the process by which any electronic record, document or other thing is proven to be what it claims to be;

‘computer’ means any electronic device capable of performing mathematical or logical instructions;

‘electronic evidence’ means evidence derived from data contained in or produced by any device the functioning of which depends on a software program or from data stored on or communicated over a computer system or network;

‘electronic record’ means data that is recorded or stored on any medium in or by a device programmed by software code and that can be read or perceived by a person or any such device, and includes a display, print out or other output of that data;

‘data’ means data in digital form;

‘device’ means any electronic apparatus or tool operating alone or connected to other apparatus or tools, that process information or data in digital form;

‘digital’ means anything that relies on technology based on a binary system or any future development or replacement technology of the same;

‘digital evidence specialist’ means a person who is appropriately qualified, and where the law requires, authorized, and capable of investigating and examining evidence in electronic form;

‘legal proceeding’ means before any statutory arbitral or other tribunal, board or commission according to national law and charged with legally defined duties and obligations, or any other formal legal process;

‘metadata’ means data that describes other data;

‘software program’ means any set of instructions that will cause a device to perform a function;

‘tool’ means any device or software program that can be used to identify, secure, examine and analyse electronic evidence.

Part II – Status of electronic evidence

Article 2 – Admissibility of electronic evidence

(1) Evidence in electronic form shall be admitted into legal proceedings.
(2) Article 2(1) does not modify any rule that applies to the admissibility of evidence, except in relation to the rules relating to authenticity and best evidence.

Article 3 – Authenticity of electronic evidence

(1) The party seeking to introduce electronic evidence in any legal proceeding has the burden of proving its authenticity.
(2) The following tests are to be considered when assessing the authenticity of evidence in electronic form:
(a) The data (both the content and associated metadata) relied upon in any legal proceedings are an accurate representation of the prevailing and existing state of those data at the time relevant to the legal proceedings.
(b) If the data have changed, for whatever reason, there is an accurate and reliable method of documenting the changes, including the reasons for any such changes from the moment they were identified (and possibly seized) as potential evidence in legal proceedings.
(c) It is necessary to demonstrate the continuity of the data between the moment the data were obtained for legal purposes and their submission as an exhibit in legal proceedings.
(d) It should be possible to test any techniques that were used to obtain, secure and process the data.
(e) The technical and organizational evidence demonstrates the integrity of the data is trustworthy, and is therefore considered to be reliable and complete, insofar as the data can be complete, which in turn will depend on the circumstances surrounding the data at the time it was identified as of being potentially relevant in legal proceedings.

Article 4 – Best evidence

In any legal proceeding, where any printout, document or other physical manifestation of the result or output or appearance of any electronic process, record or any other representation of that process or record has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purpose of the best evidence rule and shall be admitted as evidence subject to satisfactory proof of its integrity.

Article 5 – Agreement on admissibility of electronic evidence

(1) Unless otherwise provided in any law, an electronic record or document is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at a time provided for in domestic law that its admissibility may not be disputed.
(2) Notwithstanding the provisions of Article 5(1), an agreement between the parties on the admissibility of an electronic record or document does not render the record admissible in a criminal proceeding if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a lawyer.

Part III – Investigation and examination of electronic evidence

Article 6 – Digital evidence specialist

(1) Provision should be given to the formal education and training of digital evidence specialists. Such specialists are required to make judgements about the appropriateness of the tools and techniques they use to interrogate devices and seize evidence in electronic format.
(2) A digital evidence specialist must provide an analysis of their findings, setting out the basis upon which their judgement is formulated. In addition, it is necessary for a practitioner to identify any data that appear to be inconsistent with their assessment.
(3) The primary duty of the digital evidence specialist is to the court.

Article 7 – The use of good practice guidelines for electronic evidence

(1) The Parties shall establish a Forum for the development of good practice and guidelines in the acquisition, handling and otherwise processing of electronic evidence in the form of Standard Operating Procedures.
(2) The forum shall
(a) Include participation from at least two thirds of all Parties to the Convention.
(b) Establish its own rules of procedure and may establish subcommittees to consider specific issues.
(c) Be funded by contributions from the Parties on a basis to be agreed.
(d) Submit the first edition of its Standard Operating Procedures within two (2) years of this Convention coming into force.
(e) Produce updates and amendments to the Standard Operating Procedures as deemed desirable and necessary by the forum and in any case every two years.
(3) Except where incompatible or inconsistent with national legislation, codes or procedure, Parties to this Convention shall implement Standard Operating Procedures on the acquisition, obtaining, packaging, processing and examination of electronic evidence.
(4) The Standard Operating Procedures shall be:

(a) Drafted by reference to the standards and guidelines established by the Forum.

(b) Adopted within 18 months of accession to this Convention or within 18 months of the publication of the first version of the Standard Operating Procedures by the Forum, wherever is the sooner.

(c) Implemented by all national and government departments charged with legal duties and obligations involving the use, handling or processing of electronic evidence.

(5) Any authority responsible for investigating a matter involving the criminal law shall apply and follow the Standard Operating Procedures unless there are exceptional or extenuating circumstances where they cannot be followed.
(6) Where, under Article 7(5) above, the Standard Operating Procedures have not been complied with for exceptional circumstances, those circumstances and the reasons shall be recorded in writing at the time of the departure from the Standard Operating Procedures and the written record shall be admissible in legal proceedings.

Part IV – General provisions

Article 8 – Admissibility of electronic evidence from other jurisdictions

(1) Where electronic evidence originates from another jurisdiction, its admissibility is not impaired if the electronic evidence is proven in accordance with Article 3 or the authenticity of the evidence is otherwise demonstrated.
(2) Parties to this Convention shall adopt legislation whereby Internet Service Providers or Commercial Service Providers in the business of telecommunications who operate within the territory of the Party shall comply with any and all legislative provisions and judicial or prosecutorial notices and orders regarding the data relevant to the use of those services, no matter where the data are held or processed, as if those data were held or processed within the Party's territory.

Article 9 – Recognition of foreign electronic evidence and signatures

(1) In determining whether or not, or to what extent, data in electronic form is legally effective, no regard shall be had to the geographical location where the data was created or used or to the place of business of its creation, provided the electronic record or document is located in the domestic jurisdiction.
(2) Where the electronic record or document is located in a foreign jurisdiction, Article 9(1) above does not apply unless –
(a) the party who adduces evidence of the contents of the electronic record or document has, not less than 14 days before the day on which the evidence is adduced, served on each other party a copy of the electronic record or document proposed to be tendered;
(b) the court directs that it is to apply; or
(c) there is an international treaty in effect establishing recognition of electronic records or documents or of electronic signatures located in the foreign jurisdiction.
(3) Notwithstanding the provisions of Article 9(2) above, an adjudicator may admit data in electronic form that is located in a foreign jurisdiction if domestic law so provides.

Article 10 – Interpretation

(2) The provisions of this Convention shall be interpreted and enforced in light of the internationally accepted principles of technological neutrality and of functional equivalence.
(3) Where the meaning of a word or phrase in this Convention differs from the meaning of a word or phrase defined in any information technology literature, the adjudicator shall interpret the meaning in accordance with the domestic law on the interpretation of words and phrases.

Article 11 – Entering into force

(1) The Convention shall enter into force on the thirtieth day following the date of deposit with the Secretary-General of the United Nations.
(2) For each State ratifying or acceding to the Convention after the deposit of the twentieth instrument of ratification or accession, the Convention shall enter into force on the thirtieth day after the deposit by such State of its instrument of ratification or accession.

ANNEXURE C: COMMONWEALTH MODEL LAW

ELECTRONIC EVIDENCE MODEL LAW

AN ACT to make provision for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings.

BE IT ENACTED by the Parliament [name of legislature] of …… [name of country] as follows:

Short Title

1. This Act may be cited as the Electronic Evidence Act, 2002

Interpretation

2. In this Act,

‘data’ means representations, in any form, of information or concepts;

‘electronic record’ means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, print out or other output of that data.

‘electronic records system’ includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records.

‘legal proceeding’ means a civil, criminal or administrative proceeding in a court or before a tribunal, board or commission.

General Admissibility

3. Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

4. (1) This Act does not modify any common law or statutory rule relating to the admissibility or records, except the rules relating to authentication and best evidence.

Scope of Act

A court may have regard to evidence adduced under this Act in applying any common law or statutory rule relating to the admissibility of records.

Authentication

5. The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

Application of Best Evidence Rule

6. (1) In any legal proceeding, subject to subsection (b), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored.

(2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule.

Presumption of Integrity

7. In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record.

(b) where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

Standards

8. For the purpose of determining under any rule of law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour that used, recorded or preserved the electronic record and the nature and purpose of the electronic record.

Proof by Affidavit

9. The matters referred to in sections 6, 7, and 8 may be established by an affidavit given to the best of the deponent's knowledge or belief.

Cross Examination

10. (1) A deponent of an affidavit referred to in section 9 that has been introduced in evidence may be cross-examined as of right by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

(2) Any party to the proceedings may, with leave of the court, cross examine a person referred to in subsection 7(c).

Agreement on Admissibility of Electronic Records

11. (1) Unless otherwise provided in any other statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a solicitor.

Admissibility of Electronic Signature

12. (1) Where a rule of evidence requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences.

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a

transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the person.

ANNEXURE D: EXTRACTS FROM the ITU MODEL LAW ON ELECTRONIC COMMERCE (HIPCAR PROJECT)

PART II – ADMISSIBILITY

3. Amendment to Authentication and Best Evidence Rules

This Act does not modify any common law or statutory provision relating to the admissibility of records, except those relating to authentication and best evidence.

4. Common Law and Statutory Rules

In applying any common law or statutory provision relating to the admissibility of records, the Court may have regard to the principles guiding the admissibility of electronic records as prescribed by this Act.

5. General Admissibility of Electronic Evidence

Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the sole ground that it is an electronic record.

6. Application of the Best Evidence Rule

(1) In any legal proceeding, subject to subsection (2), where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the computer in or by which the data was recorded or stored.

(2) In the absence of evidence to the contrary, the integrity of the computer in which an electronic record is recorded or stored is presumed in any legal proceeding:

(a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record;

(b) where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

7. Integrity of Information, and Specific Admissibility Rules

(1) A statement contained in an electronic record produced by a computer which constitutes hearsay shall not be admissible in any proceedings as evidence of any fact stated therein unless the integrity of the computer is presumed under subsection 2.

(2) In the absence of evidence to the contrary, the integrity of the computer in which an electronic record is recorded or stored is presumed in any legal proceeding if the transaction record:

(a) has remained complete and unaltered, apart from:

(i) the addition of any endorsement; or

(ii) any immaterial change;

which arises in the normal course of communication, storage or display;

(b) has been electronically certified or has been electronically signed, by a method provided by accredited certification entities;

(c) which integrity and content has been notarized;

(d) has been recorded in a non-rewritable storage device, or any other electronic means that does not allow the alteration of the electronic records;

(e) has been examined and its integrity confirmed by an expert appointed by the court; or

(f) relating to which:

(i) evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to doubt the integrity of the record.

(ii) it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or

(iii) it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record.

(3) Where a statement contained in an electronic record produced by a computer does not constitute hearsay, such a statement shall be admissible if the conditions specified in subsection (2) are satisfied in relation to that electronic record.

8. Print-outs

(1) In any legal proceeding, where an electronic recording in the form of a printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout may be deemed to be the record for the purpose of the best evidence rule.

(2) A printout or record of a data message, certified to be a correct representation of the data message as it is displayed on a computer or information system by a person authorised by an entity wishing to have the printout admitted as evidence, is, on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law or the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence as rebuttable evidence of the information contained in the record or printout.

9. Burden to Prove the Authenticity of Electronic Evidence

The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be. In the event there is special legislation protecting more vulnerable persons, including consumers and children, and establishing allocation of burden of proof more beneficial to those persons, such legislation shall have precedence over this section.

10. Standards

For the purpose of determining under any other law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business or endeavour used, recorded or preserved the electronic record and the nature and purpose of the electronic record. Public authorities in charge of development or approval of relevant technical standards or security procedures shall issue guidelines providing orientation on the applicable criteria to be followed for compliance with this section.

11. Affidavits

Where it is intended to adduce an electronic record as evidence, it is permissible to have that record adduced in the form of an affidavit.

12. Agreement on Admissibility of Evidence

(1) Unless otherwise provided in any statute, an electronic record is admissible, subject to the discretion of the court, if the parties to the proceedings have expressly agreed at any time that its admissibility may not be disputed.

(2) Notwithstanding subsection (1), an agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not legally assisted or represented.

ANNEXURE E: CPEA, CPA, LEAA and the ECT Act

Extract from:

CIVIL PROCEEDINGS EVIDENCE ACT 25 OF 1965

PARTV

DOCUMENTARY EVIDENCE (SPECIAL PROVISIONS AS TO BANKERS' BOOKS) (ss 27-32)

27 Definition of 'bank'

in this Part 'bank' means a 'banking institution' as defined in the Banks Act, 1965, and includes the Land and Agricultural Bank of South Africa, and a building society.

28 Entries in bankers' books admissible in certain cases

The entries in ledgers, day-books, cash-books and other account books of any bank, shall be admissible as *prima facie* evidence of the matters, transactions and accounts therein recorded, on proof being given by affidavit in writing of a director, manager or officer of such bank, or by other evidence that such ledgers, day-books, cash-books or other account books are or have been the ordinary books of such bank, and that the said entries have been made in the usual and ordinary course of business, and that such books are in or come immediately from the custody or control of such bank.

29 Examined copies of entries in bankers' books admissible

Copies of all entries in ledgers, day-books, cash-books or other account books used by any bank, may be proved as evidence of such entries without production of the originals, by means of the affidavit of a person who has examined the same, stating the fact of the examination and that the copies sought to be put in evidence are correct.

30 Notice of intention to adduce evidence relating to entries in bankers' books

(1) No ledger, day-book, cash-book or other account book of any bank, and no copies of entries therein contained, shall be adduced or received in evidence under this Part, unless at least ten days' notice in writing, or such other notice as may be ordered by the person presiding at the proceedings concerned, containing a copy of the entries proposed to be adduced in evidence, has been given by the party proposing to adduce the same in evidence to the other party.

(2) On the application of any party who has received such notice, the person presiding at the proceedings may order that such party be at liberty to inspect and take copies of any entry in the ledgers, day-books, cash-books or other account books of the bank concerned, relating to the matters in question, and such order may be made in the discretion of the person so presiding, either with or without summoning before him such bank or the other party, and shall be intimated to such bank at least three days before such copies are required.

(3) On the application of any party who has received such notice, the person presiding at the proceedings may order that the entries and copies mentioned in the notice shall not be admissible as evidence of the matters, transactions and accounts recorded in such ledgers, day-books, cash-books or other account books.

31 Bank not compelled to produce books unless ordered to do so

No bank shall be compelled to produce its ledgers, day-books, cash-books or other account books in any civil proceedings unless the person presiding at such proceedings orders that they shall be so produced.

32 This Part not to apply to proceedings to which bank is a party

Nothing in this Part contained shall apply to any civil proceedings to which any bank whose ledgers, day-books, cash-books or other account books are required to be produced in evidence, is a party.

PART VI

DOCUMENTARY EVIDENCE (MISCELLANEOUS PROVISIONS) (ss 33-38)

33 Definitions

In this Part, unless the context otherwise indicates-

'document' includes any book, map, plan, drawing or photograph;

'statement' includes any representation of fact, whether made in words or otherwise.

34 Admissibility of documentary evidence as to facts in issue

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

(a) the person who made the statement either-

(i) had personal knowledge of the matters dealt with in the statement; or

(ii) where the document in question is or forms part of a record purporting to be a continuous record, made the statement (in so far as the matters dealt with therein are not within his personal knowledge) in the performance of a duty to record information supplied to him by a person who had or might reasonably have been supposed to have personal knowledge of those matters; and

(b) the person who made the statement is called as a witness in the proceedings unless he is dead or unfit by reason of his bodily or mental condition to attend as a witness or is outside the Republic, and it is not reasonably practicable to secure his attendance or all reasonable efforts to find him have been made without success.

(2) The person presiding at the proceedings may, if having regard to all the circumstances of the case he is satisfied that undue delay or expense would otherwise be caused, admit such a statement as is referred to in subsection (1) as evidence in those proceedings-

(a) notwithstanding that the person who made the statement is available but is not called as a witness;

(b) notwithstanding that the original document is not produced, if in lieu thereof there is produced a copy of the original document or of the material part thereof proved to be a true copy.

(3) Nothing in this section shall render admissible as evidence any statement made by a person interested at a time when proceedings were pending or anticipated involving a dispute as to any fact which the statement might tend to establish.

(4) A statement in a document shall not for the purposes of this section be deemed to have been made by a person unless the document or the material part thereof was written, made or

produced by him with his own hand, or was signed or initialled by him or otherwise recognized by him in writing as one for the accuracy of which he is responsible.

(5) For the purpose of deciding whether or not a statement is admissible as evidence by virtue of the provisions of this section, any reasonable inference may be drawn from the form or contents of the document in which the statement is contained or from any other circumstances, and a certificate of a registered medical practitioner may be acted upon in deciding whether or not a person is fit to attend as a witness.

35 Weight to be attached to evidence admissible under this Part

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

(2) A statement admissible as evidence under this Part shall not, for the purpose of any rule of law or practice requiring evidence to be corroborated or regulating the manner in which uncorroborated evidence is to be treated, be treated as corroboration of evidence given by the person who made the statement.

36 Proof of instrument to validity of which attestation is necessary

In any civil proceedings an instrument to the validity of which attestation is requisite may, instead of being proved by an attesting witness, be proved in the manner in which it might be proved if no attesting witness were alive: Provided that nothing in this section contained shall apply to the proof of wills or other testamentary writings.

37 Presumptions as to documents twenty years old

There shall in any civil proceedings, in the case of a document proved or purporting to be not less than twenty years old, be made any presumption which on the fifteenth day of March, 1962, would have been made in the case of a document of like character proved or which purported to be not less than thirty years old.

38 Savings

Nothing in this Part shall-

(a) prejudice the admissibility of any evidence which would apart from the provisions of this Part be admissible; or

(b) render admissible documentary evidence as to any declaration relating to a matter of pedigree, if that declaration would not have been admissible as evidence if this Part had not been enacted.

Extract from

CRIMINAL PROCEDURE ACT 51 OF 1977

221 Admissibility of certain trade or business records

(1) In criminal proceedings in which direct oral evidence of a fact would be admissible, any statement contained in a document and tending to establish that fact shall, upon production of the document, be admissible as evidence of that fact if-

(a) the document is or forms part of a record relating to any trade or business and has been compiled in the course 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 is 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 has 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.

(2) For the purpose of deciding whether or not a statement is admissible as evidence under this section, the court may draw any reasonable inference from the form or content of the document in which the statement is contained, and may, in deciding whether or not a person is fit to attend as a witness, act on a certificate purporting to be a certificate of a registered medical practitioner.

(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 the facts.

(4) No provision of this section shall prejudice the admissibility of any evidence which would be admissible apart from the provisions of this section.

(5) In this section-

'business' includes any public transport, public utility or similar undertaking carried on by a local authority, and the activities of the Post Office and the Railways Administration;

'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.

222 Application to criminal proceedings of certain provisions of Civil Proceedings Evidence Act, 1965, relating to documentary evidence

The provisions of sections 33 to 38 inclusive, of the Civil Proceedings Evidence Act, 1965 (Act 25 of 1965), shall *mutatis mutandis* apply with reference to criminal proceedings.

236 Proof of entries in accounting records and documentation of banks

(1) The entries in the accounting records of a bank, and any document which is in the possession of any bank and which refers to the said entries or to any business transaction of the bank, shall, upon the mere production at criminal proceedings of a document purporting to be an affidavit made by any person who in that affidavit alleges-

(a) that he is in the service of the bank in question;

(b) that such accounting records or document is or has been the ordinary records or document of such bank;

(c) that the said entries have been made in the usual and ordinary course of the business of such bank or the said document has been compiled, printed or obtained in the usual and ordinary course of the business of such bank; and

(d) that such accounting records or document is in the custody or under the control of such bank,

be *prima facie* proof at such proceedings of the matters, transactions and accounts recorded in such accounting records or document.

(2) Any entry in any accounting record referred to in subsection (1) or any document referred to in subsection (1) may be proved at criminal proceedings upon the mere production at such proceedings of a document purporting to be an affidavit made by any person who in that affidavit alleges-

(a) that he is in the service of the bank in question;

(b) that he has examined the entry, accounting record or document in question; and

(c) that a copy of such entry or document set out in the affidavit or in an annexure thereto is a correct copy of such entry or document.

(3) Any party at the proceedings in question against whom evidence is adduced in terms of this section or against whom it is intended to adduce evidence in terms of this section, may, upon the order of the court before which the proceedings are pending, inspect the original of the document or entry in question and any accounting record in which such entry appears or of which such entry forms part, and such party may make copies of such document or entry, and the court shall, upon the application of the party concerned, adjourn the proceedings for the purpose of such inspection or the making of such copies.

(4) No bank shall be compelled to produce any accounting record referred to in subsection (1) at any criminal proceedings, unless the court concerned orders that any such record be produced.

(5) In this section-

'document' includes a recording or transcribed computer printout produced by any mechanical or electronic device and any device by means of which information is recorded or stored; and

'entry' includes any notation in the accounting records of a bank by any means whatsoever.

Extract from
LAW OF EVIDENCE AMENDMENT ACT 45 OF 1988

3 Hearsay evidence

(1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless-

(a) each party against whom the evidence is to be adduced agrees to the admission thereof as evidence at such proceedings;

(b) the person upon whose credibility the probative value of such evidence depends, himself testifies at such proceedings; or

(c) the court, having regard to-

(i) the nature of the proceedings;

(ii) the nature of the evidence;

(iii) the purpose for which the evidence is tendered;

(iv) the probative value of the evidence;

(v) the reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends;

(vi) any prejudice to a party which the admission of such evidence might entail; and

(vii) any other factor which should in the opinion of the court be taken into account,

is of the opinion that such evidence should be admitted in the interests of justice.

(2) The provisions of subsection (1) shall not render admissible any evidence which is inadmissible on any ground other than that such evidence is hearsay evidence.

(3) Hearsay evidence may be provisionally admitted in terms of subsection (1) *(b)* if the court is informed that the person upon whose credibility the probative value of such evidence depends, will himself testify in such proceedings: Provided that if such person does not later testify in such proceedings, the hearsay evidence shall be left out of account unless the hearsay evidence is admitted in terms of paragraph *(a)* of subsection (1) or is admitted by the court in terms of paragraph *(c)* of that subsection.

(4) For the purposes of this section-

'hearsay evidence' means evidence, whether oral or in writing, the probative value of which depends upon the credibility of any person other than the person giving such evidence;

'party' means the accused or party against whom hearsay evidence is to be adduced, including the prosecution.

Extract from:

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT 25 OF 2002

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.

14 Original

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

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

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

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

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

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

(c) having regard to all other relevant circumstances.

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 its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

16 Retention

(1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if-
(a) the information contained in the data message is accessible so as to be usable for subsequent reference;
(b) the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
(c) the origin and destination of that data message and the date and time it was sent or received can be determined.

(2) The obligation to retain information as contemplated in subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

17 Production of document or information

(1) Subject to section 28, where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if-
(a) considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and
(b) at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection (1), the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for-
(a) the addition of any endorsement; or
(b) any immaterial change, which arises in the normal course of communication, storage or display.

18 Notarisation, acknowledgement and certification

(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 to, incorporated in or logically associated with the electronic signature or data message.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy thereof and the certification is confirmed by the use of an advanced electronic signature.

19 Other requirements

(1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time, is satisfied by the submission of a single data message that is capable of being reproduced by that addressee.

(2) An expression in a law, whether used as a noun or verb, including the terms 'document', 'record', 'file', 'submit', 'lodge', 'deliver', 'issue', 'publish', 'write in', 'print' or words or expressions of similar effect, must be interpreted so as to include or permit such form, format or action in relation to a data message unless otherwise provided for in this Act.

(3) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed by electronic means, that requirement is met if the document indicates that It is required to be under seal and it includes the advanced electronic signature of the person by whom it is required to be sealed.

(4) Where any law requires or permits a person to send a document or information by registered or certified post or similar service, that requirement is met if an electronic copy of the document or information is sent to the South African Post Office Limited, is registered by the said Post Office and sent by that Post Office to the electronic address provided by the sender.

List of Respondents to the Issue Paper

- Adv GTS Eiselen (In re Nedbank);
- The National Commissioner, South African Police Service (SAPS);
- Roux Krige of the National Prosecuting Authority (NPA);
- Raj Daya, CEO of the Law Society of South Africa (LSSA);
- Legal Aid, South Africa;
- Infology, an information management service provider with a specialised focus on legal risk management;
- Mark Heyink of Information Governance (Pty) Ltd; and
- Stephen Mason, general editor of the comparative law volumes *Electronic Evidence: Disclosure, Discovery & Admissibility* (2007) and *International Electronic Evidence* (2008).

List of Respondents to the Discussion Paper

- Banking Association of South Africa
- Capitec Bank
- Law Society of South Africa (LSSA);
- Legal Aid, South Africa;
- Mark Heyink