Thesis
By
ODINGA
TAKOMBE

UNIVERSITY OF
SOUTH AFRICA

E-JUSTICE IN SOUTH AFRICA: LEGAL CHALLENGES SURROUNDINGELECTRONIC EVIDENCE AND PROCEDURE

JULY 2016

E-JUSTICE IN SOUTH AFRICA: LEGAL CHALLENGES SURROUNDING ELECTRONIC EVIDENCE AND PROCEDURE

By

ODINGA TAKOMBE

Submitted in accordance with the requirements

for the degree of

DOCTOR OF LAWS

at the

UNIVERSITY OF SOUTH AFRICA

PROMOTER: PROFESSOR SS NEL

JULY 2016

SUMMARY

The advent of information and communication technologies at the end of the twenty-first century constitutes a turning point in the history of humankind. Indeed these technologies have revolutionised the way one communicates, interacts, transacts, and does business as they allow information to be stored, managed, and transmitted rapidly and cheaply, and so create the rapid transformation of modes of social and economic organisation. Ways of governing and administrating the public domain are not immune to these changes, nor is the administration of justice, which is also a public service. Justice is strongly reliant on information; traditionally, such information was fixed on a physical medium such as a paper. With the electronic revolution, the nature of information has changed from a tangible to a digital form. This requires the justice system to adapt and transform itself into an electronic justice system or e-justice.

This thesis examines the challenges that the introduction of technology in the justice system raises from the perspectives of both the law of evidence and also the law of civil procedure. From a law of evidence point of view, the advancement of technology has created an entirely new source of evidence, namely electronic evidence. A comparative analysis of the law governing electronic evidence in England and South Africa reveals that the rules relating to real evidence, documentary evidence and hearsay in both jurisdictions are to a large extent able to deal with electronic evidence if they are complemented by rules specifically governing electronic evidence. In respect of civil procedure, the emphasis is on rules governing the filing and service of court documents or the discovery of documents. On these aspects South Africa is clearly lagging behind and needs to look at a more advanced jurisdiction from a technological point of view such as Singapore to reform its obsolete rules to accommodate the electronic filing and service of court documents and the electronic discovery of documents. England is also in advance of South Africa, and, so, South Africa can gain insight from that country as well.

KEY TERMS

E-justice, electronic evidence, electronic procedure, electronic discovery, Information and Communication Technologies, electronic signature, digital signature, documentary evidence, real evidence, hearsay, electronic filing, electronic service, Public-Key Infrastructure.

DECLARATION OF AUTHORSHIP

Student number: **4148-307-3**

I declare that **E-JUSTICE IN SOUTH AFRICA: LEGAL CHALLENGES SURROUNDING ELECTRONIC EVIDENCE AND PROCEDURE** is my own work, and that all the sources that I have used or quoted have been indicated and acknowledged by means of complete references.

_____ _____

Signature Date

Odinga Takombe

ACKNOWLEDGMENTS

Writing a thesis is not an easy task. It requires not only the personal efforts of the author but also the contributions of many other people. Beyond that there is an ingredient indispensable to the success of a project of such magnitude, the divine intervention. It is, therefore, right to pay tribute here to all who, in a way or another, have contributed to the successful completion of this thesis.

Above all, I would like to express my deepest gratitude to God Almighty for the graces and blessings he has granted to me throughout this research project. Without his love, strength, wisdom, guidance and inspiration, the achievement of this thesis would not have been possible.

I acknowledge in a special way the contribution of my promoter, Professor Sanette Nel, for her advisory role, guidance, valuable suggestions, and comments that have significantly enhanced the quality of the thesis. In addition, I thank her for her moral support expressed in her encouragement and her administrative support displayed whenever I have requested her to fill in a form or provide a reference letter. Appreciation is also extended to all members of the Department of Criminal and Procedural Law of the University of South Africa (UNISA), in particular Professor Hurter.

I am thankful to all the personnel of the UNISA Main Library for their assistance with research materials necessary to complete this thesis. I extend this gratitude to all my UNISA colleagues for the role they played in shaping this thesis, in particular former members of COSUSA and current members of UCOSA.

I also take this opportunity to recognise the work done by the Reverend David Swanepoel in respect of the editing of this thesis.

May my family also find here the expression of my immeasurable and deepest gratitude for their love, support and presence in my life, the conditions which are so important for a person to be able to focus on a project such as a thesis. My friends, you too, wherever you are, be acknowledged.

Finally, I would like to acknowledge the financial assistance received from UNISA and from the Council for the Development of Social Science Research in Africa (CODESRIA).

LIST OF ABBREVIATIONS

A.D	Appellate Division
ABA	American Bar Association
AIDE	Appalachian Institute of Digital Evidence
Art	Article
BAILII	British and Irish Legal Information Institute
BBM	BlackBerry Messenger
CD	Compact Disc
CD-ROM	Compact Disc Read-Only Memory
CEPEJ	European Commission for the Efficiency of Justice
CPA	Criminal Procedure Act 51 of 1977
CPEA	Civil Proceedings Evidence Act 25 of 1965
CPP	Court Process Project
CPU	Central Processing Unit
DNS	Digital Nervous System
DVD	Digital Versatile Disc or Digital Video Disc
ECT Act	Electronic Communications and Transactions Act 25 of 2002
EDRM	Electronic Discovery Reference Model
EPE	Electronic Presentation of Evidence
ESI	Electronic-stored Information
EU	European Union

FAT	File Allocation Table
FESA	Forum of European Supervisory Authorities for Electronic Signatures
FISH	Forensic Information System for Handwriting
Fn	Footnote
HM	Her Majesty
HMCTS	Her Majesty Courts and Tribunals Service
HMSO	Her Majesty's Stationary Office
HSM	Hardware security modules
ICRI	Interdisciplinary Centre for Law and Information Technology
ICT	Information and communication technologies
IJS	Integrated Justice System
ISAD	Information Society and Development
IT	Information Technology
JILT	Journal of Information, Law and Technology
LAN	Local area network
LQR	Law Quaterly Review
LSSA	Law Society of South Africa
MCOL	Money Claim Online
MP3	Digital audio format
OFS	Orange Free State
OPD	Orange Free State Provincial Division

PAN	Personal area network
PC	Personal computer
PD	Practice Direction
PDA	Personal Digital Assistant
PDF	Portable Document File
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PREMA	Preston E-mail Application Service
RAM	Random Access Memory
RSA	Rivest-Schamir-Adleman cryptosystem
S	Section
SAAA	South African Accreditation Authority
SACJ	South African Journal of Criminal Justice
SALJ	South African Law Journal
SALRC	South African Law Reform Commission
SAPO	South African Post Office
SFO	Serious Fraud Office
SMS	Short Message Service
SS	Subsection
T	Transvaal
TSO	The Stationary Office

UK	United Kingdom
UN	United Nations Organisation
UNCITRAL	United Nations Commission on International Trade Law
US	United States of America
USA	United States of America
VCD	Video Compact Disk
VoIP	Voice over Internet Protocol
VOL	Volume
WAN	Wide area network

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

1.1 Background

The end of the twentieth century has been marked by the appearance of information and communication technologies[1] which, in themselves, represent the start of a new era, the electronic age. The advent of these extensive communication networks, linked to the potential of instruments that allow information to be stored, managed, and transmitted rapidly and cheaply, is creating a rapid transformation of modes of social and economic organisation. Ways of governing and administrating the public domain are not immune to these changes, nor is the administration of justice, which is also a public service.[2]

ICTs have indeed revolutionised the way we communicate, interact, transact, do business, and, ultimately, the way one practises law and administers justice. Important business information is increasingly created, processed, stored and communicated electronically. This is also applicable to government information and even information relating to social life. The result is a preponderance of information stored electronically, information which has the potential to serve as the basis upon which judicial disputes can be settled. From a legal point of view, therefore, the advancement of technology has created an entirely new source of evidence, namely electronic evidence. The rising importance of this new evidence brand has vastly outpaced the rate at which the legal industry has adapted to this new reality. It is, therefore, crucial to address the challenges. Given the fact that the natural habitat of electronic evidence is the digital world, it should be understood that part of the challenge is that the solution requires a safe and effective e-justice system to be in place, which, in turn, raises the issue of electronic procedure.

The majority of developed countries already have over two decades of experience behind them in designing and implementing e-government strategies in many public administration areas, such

1 Hereafter referred to as ICTs

2 Cerrillo & Fabra *E-justice: using Information Communication Technologies in the Court System* 2009 (hereafter referred to as Cerrillo & Fabra *E-justice*) xii

as taxes and health services. Nevertheless, the use of ICTs in the field of judicial administration is lagging behind.[3]

The pattern is not that different in South Africa. This country enacted the Electronic Communications and Transactions Act[4] 25 in 2002, which broadly aims at enabling and facilitating electronic communications and transactions[5] in the public interest,[6] and specifically to promote e-government services, among other things.[7] A national e-strategy plan (Information Society and Development [ISAD]) was adopted in terms of this Act to promote e-government services, but it did not specifically address the field of justice.

Law and justice are, nevertheless, not immune to changes in the prevailing communicative infrastructures as they are extremely information intensive. What happens after the introduction of information and communication technologies? How does, or how can, this new medium of ICT affect the judicial system? Since the very organisation of judicial systems is based on the exchange of information, it is submitted that the potential to be attained by the introduction of ICTs is even higher than it is in other fields.[8]

1.2 Problem Statement

Having noted that the world has undergone an electronic revolution affecting all sectors, including the justice system, it is opportune to highlight the legal issues raised by the use of technology in the justice system that this research project seeks to investigate. From the title of the thesis, it should be clear that the general framework of this research is e-justice in South Africa, and it is examined with reference to the challenges surrounding electronic evidence, on the one hand, and those affecting procedure, on the other hand. Through the examination of existing rules of evidence and procedure, this thesis seeks to ascertain whether these rules can resolve, or sufficiently deal with, technologically-related questions. The investigation is approached using two steps. The first step is an investigation into electronic evidence and issues

3 Cerrillo & Fabra *E-justice* xii
4 Hereafter referred to as the ECT Act
5 In terms of the ECT Act, "transaction" means a transaction of either commercial or non-commercial nature, and includes the provision of information and e-government services
6 S 2(1) of the ECT Act
7 S 2(1)(g) of the ECT Act
8 Cerillo & Fabra *E-justice* xii

relating to its admissibility and weight in court proceedings, while the second step deals with rules of procedure that are necessary for a safe and effective e-justice system in South Africa, in particular rules governing the filing and service of court documents or the discovery of documents.

This problem statement will now be explained in more detail. Regarding issues relating to the admissibility and weight of electronic evidence, it must be said as a starting point that electronic evidence is problematic. Considerable uncertainty surrounds such evidence. This research project looks at the nature and some special characteristics of electronic evidence which raise legitimate concerns about its accuracy and authenticity. The nature of electronic evidence is the first challenge one faces when examining this evidence. Is it a subset of a traditional category of evidence, such as real evidence or documentary evidence, or is it a *sui generis* category? As it will become evident from the discussions conducted throughout the thesis, electronic evidence is a mix of both traditional categories and a *sui generis* category. In other words, depending on the circumstances, rules governing documentary evidence or real evidence will apply to electronic evidence. These rules must, however, be applied with consideration given to the unique nature and special characteristics of electronic evidence. In addition, since electronic evidence may qualify as hearsay, relevant hearsay rules may also be applicable.

There is also uncertainty regarding electronic evidence because of the fact that such a type of evidence is seen as more vulnerable and, therefore, less reliable than traditional evidence such as documentary evidence. Legal professionals are concerned about such vulnerability and how easily such evidence could be manipulated, given its high degree of volatility. The authenticity of electronic evidence is often challenged in courts of law, and this contributes to the legal concerns about the usefulness, relevance and reliability of this type of evidence.[9] Electronic evidence also challenges many other notions and principles of documentary evidence. For instance, a document commonly refers to content on paper, easy to authenticate by way of a manuscript signature, whose integrity can be maintained, and any attempt to manipulate the document can be detected easily. There is also a lesser chance for the author, who personally signed the document, to repudiate the contents thereof. On the other hand, it is more difficult to establish the authenticity

[9] Mason (ed.) *Electronic Evidence: disclosure, discovery and admissibility* 2007 (hereafter referred to as Mason *Electronic Evidence: disclosure, discovery and admissibility*) v

of electronic evidence because of the environment from which it originates. The potential for anonymity and pseudonymous activity is prevalent in the digital environment, making it harder to authenticate the author of an electronic document. Electronic evidence integrity is a concern as well. It is indeed very easy to tamper with electronic evidence owing to the intangible and transient nature of the data without signs of obvious distortions, especially if the electronic evidence is converted into paper form. Electronic evidence can be changed by malicious software or viruses as well as during its transfer to a new medium. Software applications also create risks relative to the alteration and the manipulation of data. There is also the risk of technical obsolescence and the fact that electronic evidence can originate from a variety of sources, and from different file formats and application systems, across a number of jurisdictions. This volatility of electronic evidence also makes it easy to repudiate.

Given the shortcomings of traditional categories of the law of evidence to deal effectively with electronic evidence, there was a need to introduce a special regime for electronic evidence. This regime has contributed to the removing of the obstacles in the admissibility of electronic evidence; however, problems remain, given the complex and sophisticated nature of the rapidly-changing technology (such as newer versions of operating systems, including software applications and hardware) which generates electronic evidence. This necessitates a shift towards a focus on issues relevant to establishing the authenticity of, and suitable weight for, electronic evidence.[10]

Different solutions are constantly being explored in an attempt to ensure authenticity, integrity and the non-repudiation of electronic evidence. One of these is electronic signatures.[11] The electronic signature is a new form of signature. It adds to other existing forms of signatures, such as the famous manuscript signature, an "X" or thumbprint mark, a printed name, a stamped name, a typewritten name, a telegram, a telex or a facsimile containing a name. All these signatures have been held capable of fulfilling the functions of a signature, including the above-listed functions.[12] It goes without saying that an electronic signature can fulfil these functions

---

10 SALRC Issue Paper 27, and Project 126, *Review of the Law of Evidence: Electronic Evidence in Civil and Criminal Proceedings: Admissibility and related issues* 2010 (hereafter referred to as SALRC Issue Paper 27, *Review of the Law of Evidence* 2010) 7

11 For a deeper analysis of electronic signatures, see Ch 2 par 2.4.1 and Ch 4 par 4.3 of the thesis

12 Ch 4 par 4.2.3 of the thesis

too. It must be stressed, however, that electronic signature is a generic term that includes many forms of signatures created using electronic means, and not all of them offer the same degree of certainty with regard to the functions of authenticity, integrity and non-repudiation of signatures. For judicial matters, such as the electronic communication of court documents, it is imperative to use a form of electronic signature that offers the required level of trust. A digital signature can fulfil that requirement.[13] Public Key Infrastructure, or PKI technology, is able of creating digital signatures. PKI uses asymmetric cryptography, where each party has two keys, a public key, which can be publicised to the whole world without compromising its security, and a private key safely kept by the keyholder, which offers a more secure encryption. It is important, from a legal point of view, to analyse such technology to determine whether it can produce digital signatures that satisfy the legal requirements.[14]

It is important, however, to note that, to put in place digital signatures using PKI technology, the services of a third party are required. Cryptography providers or authentication service providers can fulfil that role.[15] This thesis investigates authentication products and services in support of advanced electronic signatures currently accredited in South Africa to determine how efficient they are in providing advanced electronic signatures which can ensure the authenticity and integrity of electronic evidence.[16]

Biometric technology is also able to produce reliable electronic signatures. It operates by verifying the identity of a human subject's unique physiological and or behavioural features, such as fingerprints, iris recognition, and hand and palm geometry.[17] It is, therefore, at least in theory, capable of producing electronic data uniquely linked to the signatory, capable of identifying the signatory, and created using means that the signatory can maintain under his[18] sole control.[19] It is, thus, worthwhile to analyse this technology and to ascertain to what extent it

---

13 Digital signature is discussed in Ch 2 par 2.4.1.2

14 Ch 2 par 2.4.1.2 and Ch 4 par 4.3.3.7.1

15 Cryptography and authentication are defined in Ch 2 par 2.4.1.2 below

16 Ch 4 par 4.3.2.3.1

17 Ch 2 par 2.4.1.2

18 For the purpose of this thesis reference to the masculine will include the feminine, and reference to the singular will include the plural

19 Brazell *Electronic signatures and Identities, Law and Regulation* 2008 (hereafter referred to as Brazell *Electronic signatures and Identities, Law and Regulation*) 72

can offer a solution as to the certainty of electronic documents.[20] In this research study, the analysis of electronic evidence will focus primarily on the South African legal system. It will be interesting to see how this question has been addressed by the South African legislature. Different pieces of legislation will be examined, namely: the Computer Evidence Act 57 of 1983, and the Act that repealed it, the ECT Act; the Civil Proceedings Evidence Act 25 of 1965;[21] the Criminal Procedure Act 51 of 1977;[22] and the Law of Evidence Amendment Act 45 of 1988. Reference will also be made to case law to perceive the approach of judges in dealing with electronic evidence.[23]

Apart from the South African jurisdiction, another legal system to enjoy significant attention throughout this research will be the English system. When looking at the English jurisdiction, attention will be given to different pieces of legislation, such as the Civil Evidence Act 1995, the Criminal Justice Act 1988, and the Criminal Justice Act 2003.

Whenever it will be in the interest of the research, however, apart from above-mentioned jurisdictions, reference will be made to relevant legal sources from other jurisdictions. This will be the case specifically in the analysis of electronic signatures where reference will be made to international instruments such as the United Nations Commission on International Trade Law[24] Model Laws on Electronic Commerce and Electronic Signatures respectively or the European Union Directive 1999/93/EC establishing the legal framework at European level for electronic signatures and certification services.[25] The Model Law on Electronic Commerce seeks to provide legal recognition to information in the form of a data message used in the context of commercial activities. Considering its limitation to commercial activities only, the question that may be raised is whether the evidence provisions of the Model Law could be relevant in the context of other civil or criminal proceedings. Since the evidence provisions of the ECT Act are based on

---

20 Ch 4 par 4.3.1.1.2

21 Hereafter referred to as the CPEA

22 Hereafter referred to as the CPA

23 Some of the cases discussed include *Narlis v South African Bank of Athens* 1976 (2) SA 573 (A); *S v Harper and Another* 1981 (1) SA 88 (D); *Ndlovu v Minister of Correctional Services and Another* 2006 (4) All SA 165 (W); *Trend Finance (Pty) Ltd v Commissioner for SARS* 2005 (4) All SA 657 (C); *Diners Club SA (Pty) Ltd v Singh and Another* 2004 (3) All SA 568 (D); *S v Ndiki & Others* 2007 (2) All SA 185 (Ck)

24 Hereafter referred to as the UNCITRAL

25 Hereafter referred to as the eSignature Directive or the EU Directive on Electronic Signatures

the Model Law, any conclusions made for the latter may be relevant for the former. Similar to the Model Law on Electronic Commerce, the application of the Model Law on Electronic signatures is limited to the case where electronic signatures are used in the context of commercial activities. Analysis of both Model Laws will allow a determination of whether they are suitable for use in a non-commercial context.[26]

The goal of the eSignature Directive is to make electronic signatures easier to use and to help them become legally recognised within the Member States. It lays down the criteria that form the basis for the legal recognition of electronic signatures.[27] It is critical for this thesis to discuss this Directive not only because England, as a member of the European Union, is bound by the Directive, but also because, as a general rule, directives are adopted after serious deliberations between experts from the European Union member countries. They, therefore, represent a good benchmark.

After discussing issues relating to the admissibility and weight of electronic evidence, the thesis will focus on the procedural aspect of the legal problem. It should be stressed that the vision is to have a safe and efficient e-justice system to deal effectively with electronic evidence and the business of the courts. This requires the introduction of ICTs in the administration of justice. ICTs should not only operate at the level of communication and exchange of data between different stakeholders involved in the administration of justice, such as attorneys and courts, at the pre-trial phase. For instance, they may allow attorneys to discover electronic evidence in electronic form. But ICTs will also operate in the running of a trial *per se* in order to facilitate the presentation of evidence or electronic evidence, giving rise to what we can refer to as electronic trials.

With this background in mind, the second leg of the problem to be investigated in this thesis is the legal challenges posed by the use of the ICTs in the administration of justice from a procedural law perspective. Can pleadings exchange be made electronically? Can a process of court service be made electronically? The exercise here will be to analyse the Rules of Court and other relevant sources to determine whether existing rules of procedure can resolve problems raised by the implementation of e-justice in South Africa and, if not, to suggest amendments

[26] Ch 4 par 4.3.1.1.1 & par 4.3.1.1.2
[27] Ch 4 par 4.3.1.2.2

based on international best practices. A good example to take into consideration in this regard is the Singapore experience. That legal system has proved that it is not "utopia" to have a paperless court. Indeed, to make that country competitive and to nurture growth and participation in the new global economy, the Singapore government has aggressively embraced Information Technology since 1989. The requisite legislative framework started to be put in place progressively from then on. The Evidence (Amendment) Bill was introduced in Parliament on 5 December 1995 and passed on 18 January 1996, and the Evidence (Amendment) Act came into force on 8 March 1996. A new section 62A of the Evidence Act allowed for video link testimony. A new section, 68A, was inserted to facilitate the use of multimedia technology in the Technology Court in the presentation of voluminous or complex evidence. A new section, 36A, was inserted to enable the Supreme Court Rules Committee to make rules to provide for the filing and receiving of evidence and documents in court by the use of information technology. Order 63A of the Rules of Court was, accordingly, introduced on 8 March 1997 to provide for "Electronic Filing and Service". It provides for the Registrar to establish an electronic filing system whereby specified documents may be filed, saved, delivered or conveyed by electronic submission through a network service provider. This enabled the legal framework to be constructed for electronic filing of court documents and the installation of the Technology Court.[28]

In South Africa, considerations of introducing technology into the administration of justice came to the fore for the first time in 1996. In a letter to the Minister of Justice, dated 14 October 1996, Justice HCJ Flemming proposed the introduction of legislation concerning the use of video conferences in court proceedings with particular reference to the giving of evidence by means of video-conferences in criminal matters. This was followed by a proposal to introduce electronic trials by Mr D Dalling, MP in a letter to the Minister of Justice dated 29 July 1997. As a result, the South African Law Reform Commission was requested to investigate the use of electronic equipment in court proceedings. The objective of the investigation was to determine whether the use of electronic equipment in court proceedings was a viable option to save costs and prevent delays in civil and criminal matters. The investigation did not receive attention until 2003 when the office of the National Director of Public Prosecutions requested the SALRC to expedite the

[28] Kim "Electronic evidence: Singapore's approach", July 2002 *Law Gazette* 1 (hereafter referred to as Kim "Electronic evidence: Singapore's approach") 3

investigation and to conduct a separate investigation into the possibility of postponements of cases *via* video conferencing. The Commission recommended the use of audio-visual links with reference to applications for leave to appeal and appeals in respect of accused persons in custody in prison. The recommendations eventually became law in the form of the Criminal Procedure Amendment Act 65 of 2008.[29]

In addition, technology pushed the Department of Justice to start a restructuring process to promote an e-justice programme aimed at introducing an Integrated Justice System (IJS) in South Africa. The objective was to re-engineer business processes, using the necessary technology, to ensure the effective integration of the component parts of the justice system. The Digital Nervous System of the IJS programme provides an ICT infrastructure throughout the Department of Justice. The Integrated Case Management System includes the Court Process Project (CPP) which was designed to provide automated civil and criminal case management systems in magistrates' courts.[30]

As will be shown later, in the discussion of e-justice from a technical point of view, technology has a positive impact on the functioning of the justice system in that it contributes to a more efficient judicial system by increasing productivity and to a more effective judicial system by reducing procedures duration, thus saving both time and money. It contributes also to improved transparency of how the judiciary works, as the technologies facilitate an improved control of cases and allow a better qualitative evaluation of outputs, and, ultimately, it contributes to increased confidence by citizens and businesses in the judicial system and greater legitimacy for the judicial power.[31]

There is, nevertheless, a need to take e-justice in South Africa to the next level. A functional e-justice system will make it possible for attorneys to communicate and exchange legal documents electronically, including electronic evidence, either with the Registrar of the court or other law firms. It will also facilitate the presentation of evidence in general or electronic evidence in particular in court.

---

29 SALRC Issue Paper 27, *Review of the Law of Evidence* 2010 1-2

30 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa*, a World Bank/International Records Management Trust Partnership Project, July 2002 (hereafter referred to as *Evidence-Based Governance in the Electronic Age Case Study*) 3

31 Ch 5 par 5.2.2.1.2

A very encouraging move came from the Durban High Court where a progressive judge made a landmark ruling allowing service of a legal notice on Facebook.[32] Before granting the application to use Facebook as a medium to serve a legal notice, she studied the workings of Facebook and was satisfied that it could be used as an effective tracing tool and could relay information to the individuals concerned.[33] This ruling was possible, said the judge, because of a recent amendment to the Uniform Rules of Court which provides for service by way of electronic mail, registered post, and fax.[34]

South Africa is on the right track, but it needs to do more to adapt to the electronic revolution more effectively. Undoubtedly, Singapore could be a good model to look to.

In summary, this thesis will analyse a two-fold problem, firstly, the legal issues around the admissibility and weight of electronic evidence in court, and, secondly, the legal challenges from a procedural law perspective in the establishment of an e-justice system to facilitate exchange of information and handle electronic evidence more effectively. The emphasis will be put on the law of civil procedure because in civil proceedings the amount of information exchanged is higher, and the benefits to gain from the introduction of technology are similarly higher. In addition, the thesis wants to stay away from the many constitutional challenges that may be raised in case of an electronic criminal procedure.

1.3 Points of departure

1.3.1 Basic theory

The question of electronic evidence will be examined from a general law of evidence point of departure. In other words, electronic evidence will be analysed with reference to traditional notions and principles of the law of evidence. These principles include the usefulness, relevance and reliability of electronic evidence. In addition, notions of authentication, integrity and non-repudiation of electronic evidence will be considered.

---

32 *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens* (unreported case no 6846/2006, 3-8-2012);this case is discussed under Ch 5 par 5.3.1.2.2

33 *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens* (unreported case no 6846/2006, 3-8-2012) at [9]

34 *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens* (unreported case no 6846/2006, 3-8-2012) at [7]

The question of legal challenges in the establishment of e-justice will be studied from a procedural point of departure, and, specifically in this instance, from the point of view of the law of civil procedure.

1.3.2 Research methodology

It is often said that legal research is too theoretical and of little use in the legal practice. Our submission is that legal research and legal practice are interdependent. The former helps the latter by analysing sources of law applicable to a specific legal problem, and it sheds light on which normative factors can be used and when they can be used in order to answer questions. In fact legal theories are tested in practice.[35] The problem of electronic evidence and procedure is undoubtedly of even greater interest to the legal practice than to the research area as, ultimately, the law is applied in practice. A study like this thesis should, therefore, be an important source of information for the legal practice when dealing with electronic evidence and procedure. Through the analysis of sources of law applicable to electronic evidence and procedure, however, the thesis will provide an insight into issues beneficial to both the academic world and the legal practice. This will be achieved by using different research methods, doctrinal or theoretical legal research, legal historical research, and comparative law.

Doctrinal legal research refers to research which asks what the law is in a particular area.[36] This method will assist this project in identifying and analysing primary sources pertaining to the question of electronic evidence and procedure, namely pieces of legislation, together with case law.[37] In addition, reference will be made to secondary sources, such as articles or other written commentaries on the case law and existing legislation.

Legal historical research will be also used to some extent. Ibbetson points out that there are many ways of doing such research.[38] One of these is by looking at the development of some legal

---

35 Du Plessis *A Self Help Guide: Research Methodology and Dissertation Writing* 2007 (hereafter referred to as Du Plessis *A Self Help Guide: Research Methodology and Dissertation Writing*) 30

36 Mc Conville & Chui *Research Methods for Law* 2010 (hereafter referred to as Mc Conville & Chui *Research Methods for Law)* 19

37 See pieces of legislation and case law mentioned in Ch 1 par 1.2 above

38 Ibbetson "Comparative legal history: a methodology" in Musson & Stebbings (ed) *Making Legal History, Approaches and Methodologies* 2012 130 (hereafter referred to as Ibbetson "Comparative legal history: a methodology") 131

institution over time.[39] This is the approach followed in this thesis, and it will be relevant in the analysis of changes in legal rules affecting electronic evidence. This method will be used in conjunction with the two other methods mentioned. It will take the form, for example, of providing a brief history of a rule or a law while discussing that rule or law or comparing it or its development in South Africa to other jurisdictions.[40]

Last, but not the least, this thesis will rely on the comparative law method. It is suggested that "comparative law" is an intellectual activity whose object is the law and whose process is comparison.[41] It is used to compare various legal systems of the world.[42] In this specific instance, the comparative law method is particularly important not only because problems, caused by the appearance of ICTs, are global problems requiring global solutions, but also because of the increasing influence of international and supra-national legal materials and the need to refer to materials from a variety of jurisdictions in order to engage in critical thinking. Reference will, thus, be made to international instruments such as the UNCITRAL Model Laws on Electronic Commerce and on Electronic Signatures, and the European Union Directives on Electronic Commerce and on Electronic Signatures.

In addition to the above instruments, the comparative law method will also be useful in comparing the South African legal system with selected foreign legal systems. The South African jurisdiction will, in essence, be compared to two jurisdictions, namely the English jurisdiction and the Singapore jurisdiction. The first-mentioned jurisdiction will be the main system to which the South African legal system will be compared throughout this research study, while the Singapore jurisdiction will serve as a system of comparison mostly in discussions related to e-justice from both a technical and procedural point of view.

The choice of the English system is justified by the influence that the English Common law has had on the development of the South African law of evidence and procedure. After conquering the Cape Colony, the English started to organise and modernise the judicial system of the new

---

39 Ibbetson "Comparative legal history: a methodology" 131

40 Du Plessis *A Self Help Guide: Research Methodology and Dissertation Writing* 31

41 Zweigert & Kotz *An Introduction to Comparative Law* (3rd ed) 1998 (Hereafter referred to as Zweigert & Kotz *An Introduction to Comparative Law*) 1; read also David & Brierly *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law* (2nd ed) 1978 (hereafter referred to as David & Brierly *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law*) 1-5

42 Zweigert & Kotz *An Introduction to Comparative Law* 1

colony and they introduced a law of evidence and procedure based on the English Common law.[43] In the light of this, it is natural or even imperative for a research project dealing with electronic evidence and procedure in South Africa to look at England, as the rules and techniques developed there to deal with these questions can enlighten the situation in South Africa.

Singapore is a true success story as far as the introduction of technology in the justice system is concerned. It managed to change the dismal[44] state of its judiciary drastically by the use of technology.[45] In its goal to develop a world-class judiciary, Singapore decided to convert court processes from a paper regime to an electronic one, and this has contributed to more efficient and effective courts.[46] A conversion from paper to electronic obviously raises legal issues from a procedural law point of view. Singapore has been very successful in dealing with these issues, and it, therefore, constitutes a good jurisdiction to look at.

1.4 Research structure

This research project is divided into six chapters. Chapter 1 is the introductory chapter. Chapter 2 provides an overview of basic concepts relating to e-justice, including electronic evidence and related issues. Chapter 3 analyses the admissibility and weight of electronic evidence in Court. Chapter 4 discusses the challenges posed by electronic evidence and the responses thereof, namely electronic signatures. Chapter 5 deals with e-justice from both technical and procedural law perspectives. Finally, Chapter 6 is the concluding chapter.

The rationale behind chapter 2 is to have a clear understanding of the terms to be used throughout the research. This thesis is clearly based on a multi-interdisciplinary approach with the use of a significant number of technical terms from different disciplines. It is, therefore, important to define these terms to enable the reader to understand them fully in the context of the research. Chapter 2 will then explore, among other things, the following concepts, evidence, electronic evidence, documentary evidence, real evidence, direct evidence, indirect evidence,

---

43 Zweigert & Kotz *An Introduction to Comparative Law* 232

44 Before the introduction of technology, the judiciary was characterised by huge case backlogs, breach of and disregard for the rules of court, and so on. See Sze "Chapter 3: Singapore" in Oskamp, Lodder and Apistola (ed) *IT Support of the Judiciary, Australia, Singapore, Venezuela, Norway, The Netherlands and Italy* 2004 (hereafter referred to as Sze "Chapter 3: Singapore") 49

45 Sze "Chapter 3: Singapore" 49

46 Sze "Chapter 3: Singapore" 50

hearsay evidence, electronic signature, digital signature, e-justice metadata, encryption, decryption, plaintext, hash function, Public/Private Key Infrastructure, Biometry, authentication, integrity, non-repudiation, and so on.

Chapter 3 is a very important chapter. It discusses the fundamental issues around the admissibility and weight of electronic evidence. Indeed this type of evidence has value only if it can be produced in court and given due legal weight. The chapter is divided into three sections. The first section discusses the general principles underlying the admissibility of electronic evidence as real evidence. The second section focuses on the interaction between the admissibility and weight of electronic evidence and the hearsay rule. Finally, the last section discusses the question of admissibility and weight of electronic evidence in relation to documentary evidence.

In chapter 4, challenges posed by electronic evidence are identified and examined. These challenges relate to, among other matters, the authenticity, integrity and non-repudiation of electronic evidence. This chapter also deals with responses to the identified challenges, namely electronic signatures. It seeks to examine the legal status of electronic signatures with reference to the Model Law on Electronic Signatures, the EU Directive on Electronic Signatures, the English law on Electronic Signatures, and the ECT Act. It also consists of an investigation into authentication and cryptography products or services such as biometry or PKI technology.

Chapter 5 deals, firstly, with e-justice from a technical point of view. It explores the concept, its relevance and the main applications of technology used in the electronic justice setting in England, Singapore and South Africa. In the second part, a discussion on rules of civil procedure relevant to the introduction and implementation of e-justice in the same jurisdictions is undertaken.

Chapter 6 is the concluding chapter of the thesis. Although conclusions are incorporated into each chapter, the most salient conclusions regarding issues discussed will be repeated in this chapter. The chapter will also provide suggestions and recommendations for a better technology and justice partnership. Finally, it lists areas for future research.

CHAPTER 2 BASIC CONCEPTS AND TERMINOLOGY

2.1 Introduction

This chapter is of a preliminary nature; it attempts to introduce basic concepts and terminology fundamental to an understanding of the subject which will be encountered throughout this research document. The aim is not to explore matters in detail, but rather to give an overview of the subject and a guide to the further analysis and discussion which is undertaken in later chapters. It must be stressed, however, that some issues are dealt with in a more comprehensive manner since they will not enjoy much attention later. It is indeed critical to undertake this exercise, especially considering the fact that this research project is of a highly technical nature using a significant number of technical terms from a variety of disciplines in a multi-interdisciplinary approach. The rationale behind this chapter is to give the reader a clear understanding of terms used throughout the research to enable him to take the most out of the research. Terms identified as needing explanation include, amongst others, evidence, electronic evidence, documentary evidence, oral evidence, real evidence, direct evidence, circumstantial evidence, hearsay evidence, electronic signatures, digital signature, e-justice, metadata, cryptography, ciphertext, plaintext, hash function, Public-Key Infrastructure, biometrics, bit, byte, and authentication, to name but a few.

For the sake of order and clarity, save for electronic evidence which will be classified in a category of its own, terms to be defined in this chapter will be divided essentially into two main categories: terms of legal nature on the one hand; and terms of technological nature on the other hand.

2.2 Terms of legal nature

2.2.1 Evidence

Evidence is information by which facts tend to be proved.[47] It provides grounds for belief that a particular fact or set of facts is true.[48] In general terms, it may be defined as any material which

[47] Keane & Mckeown *The Modern Law of Evidence* (9th ed) 2012 (hereafter referred to as Keane and Mckeown *The Modern Law of Evidence*) 2

[48] Dennis *The Law of Evidence* (4th ed) 2010 (hereafter referred to as Dennis *The Law of Evidence*) 3

has the potential to change the state of a fact-finder's belief with respect to any factual proposition which is to be decided and which is in dispute.[49] Hence, evidence essentially consists of oral statements made in court under oath, affirmation or warning (oral evidence), as well as documents (documentary evidence) and objects (real evidence) produced and received in court.[50] From a scientific perspective, evidence may be defined as any material which would aid the court in establishing the probability of past events into which it must inquire. In contrast, the legal viewpoint considers whether certain kinds of evidence should be excluded notwithstanding their potential in helping to reconstruct the facts.[51] This is the function of the law of evidence, which is a body of rules regulating the means by which facts may be proved in courts of law.[52] In other words, the law of evidence is a collection of rules governing what facts may be proved in court, what materials may be adduced to prove those facts, and the form in which those materials should be placed before the court.[53] It includes, furthermore, questions about what rules should be taken into account in assessing the weight or cogency of evidence and what standard of proof should be satisfied before a party bearing the burden of proof can be successful.[54] A brief introduction to the law of evidence in England and South Africa is provided below.

2.2.2 Law of Evidence

2.2.2.1 England

The English modern Law of Evidence is of a hybrid nature and reflects its common law history on the one hand, and its statutory nature on the other hand. Indeed, its development really begins with decisions of common law judges in the seventeenth and eighteenth centuries,[55] supplemented, in recent centuries, by a number of statutory reforms.[56] Common law has provided the English law of evidence with some of its most fundamental principles; one of these

---

49 Murphy *Murphy on Evidence* (11th ed) 2009 (hereafter referred to as Murphy *Murphy on Evidence*) 2

50 Schwikkard & Van der Merwe *Principles of Evidence* (3rd ed) 2009 19 (hereafter referred to as Schwikkard & Van der Merwe *Principles of Evidence* (2009)) 19

51 Murphy *Murphy on Evidence* 3

52 Keane & Mckeown *The Modern Law of Evidence* 2

53 Murphy *Murphy on Evidence* 1

54 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 2

55 Tapper *Cross & Tapper on Evidence* (12th ed) 2010 (hereafter referred to as Tapper *Cross & Tapper on Evidence*) 1

56 Statutes include the Evidence Acts of 1843 and 1851, the Criminal Evidence Acts of 1898, 1965, 1979 and 1999, the Civil Evidence Acts of 1968, 1972 and 1995, the Criminal Justice Acts of 1988 and 2003, the Human Rights Act 1998

is the existence of the exclusionary rules which preclude certain matters from being accepted as evidence of a fact in a court of law.[57] These rules, adopted largely because of the existence of the jury,[58] the oath,[59] and the common law adversary system of procedure,[60] are still applicable today, even *vis-à-vis* evidence that was not foreseen by the pioneer judges, such as electronic evidence.[61]

2.2.2.2 South Africa

The South African law of evidence is of English origin. South Africa has, indeed, imported from England most of its fundamental principles. One of the most striking characteristics of these is the existence of a significant number of rules which forbid the reception of logically relevant evidence, in other words, exclusionary rules, owing their existence to, amongst other things, trial by jury as pointed out above.[62] Although trial by jury was abolished from 1927 in civil cases[63] and 1969 in criminal cases[64] in South Africa, the evidentiary system designed for jury trials is still applicable.[65] South Africa has also inherited from England the adversarial method of trial, the principle of orality, the oath, the doctrine of precedent, and the so-called best evidence rule.[66] Given its relevance when one deals with a subject such as electronic evidence, the so-called best evidence rule needs to be explained at this stage since it will form the basis of any further analysis of the subject.

---

57 For example the common law rule against hearsay prohibits statements made by anyone other than the testifying witness as evidence of the facts stated. Although this rule has been statutorily amended, the general principle of excluding hearsay evidence remains applicable in terms of these statutory amendments unless certain conditions are satisfied

58 It was felt that jurors who were lay persons could overvalue the weight and importance of certain evidence or treat it as conclusive; hence the need to put restrictions

59 The oath is considered to provide the strongest hold on the consciences of men

60 In the adversarial system, the court cannot undertake a search for relevant evidence but must reach its decision on the basis of evidence presented by parties

61 Tapper *Cross & Tapper on Evidence* 2

62 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 5

63 S 3 of the Administration of Justice (Further Amendment) Act 11 of 1927

64 Abolition of Juries Act 34 of 1969

65 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 5

66 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 5

2.2.3 The best evidence rule

2.2.3.1 General rule

The best-evidence rule, as a general rule, excludes weaker evidence when stronger evidence is available. In other words, in terms of this rule, no evidence is ordinarily admissible to prove the contents of a document apart from the original document itself.[67] To prove ownership, therefore, the best evidence is a title deed, the register kept by the Registrar of Deeds, or such secondary evidence as has been made admissible by statute.

The rule applies only when the content of a document is directly in issue; it has no application where the issue is the existence of a relationship or status derived from the document.[68] Nor does it apply where a document's contents serve merely to prove a fact that is capable of being proved by means other than the document.[69] So, as a general rule, whenever the content of a document must be proved, the original document must be produced. This is in line with the decision reached in *S v Koralev and Another*[70] where images found on the accused's computer were held not to be original images since, it was said, they had either been downloaded from the Internet or transferred from a digital camera and, thus, were deemed inadmissible, especially considering the absence of some proof of their reliability and accuracy. The original images, therefore, it was held, would be those contained in the camera or in the original source from which they had been uploaded onto the Internet site.[71]

---

67 *R v Pelunsky* 1914 AD 360; *R v Amod & Co Ltd* 1947 (3) SA 32 (A) at 40. See, in general, Zeffert & Paizes *Essential Evidence* 2010 (hereafter referred to as Zeffert & Paizes *Essential Evidence*) 127; Wright & Winn *The Law of Electronic Commerce* (3rd ed) 1999 (hereafter referred to as Wright & Winn *The Law of Electronic Commerce)* 8-1

68 *R v Lombard* 1957 (2) SA 42 (T) at 46; *Gemeenskapsontwikkelingsraad v Williams and Others* (1) 1977 (2) SA 692 (W) at 698; The existence of a status or a relationship may be proved by oral or any other evidence as in the following cases: in *Alderson v Clay* 1816 1 Stark 405; 171 ER 511 the existence of a partnership was proved without the production of the partnership deed; in *R v Inhabitants of Holy Trinity, Kingston-on-Hull* 1827 7 B&C 611;108 ER 851 tenancy was proved without producing the lease agreement; in *R v Maruvey* 1918 NPD 29 oral evidence was adduced to prove a person' s immigration status

69 *Weltz and Another v Hall and Others* 1996 (4) SA 1073 (C)

70 2006 (2) SACR 298

71 In both the court *a quo* and the appeal court, it was, in argument, contended that the photographs and video images were not admissible in evidence because they did not meet the requirements for admissibility as set forth in *S v Ramgobin and Others* 1986 (4) SA 117 (N), where it was held that, for audio tape recordings and video tape recordings to be admissible in evidence in a criminal trial, it must be proved that the exhibits sought to be put in (a) are the original recordings and (b) that on the evidence as a whole there

As noted by Zeffert and Paizes, this case may appear difficult to reconcile with *Botha v S*,[72] where it was held that the fact that many of the documents adduced in evidence by the State were computer-generated and it could not be said that the documents were not the originals. This seems to suggest that, according to the court in that case, computer-generated documents are original documents.[73] In agreement with Zeffert and Paizes, we oppose this submission and support the view expressed in the previous case which is in line with the nature of electronic evidence and accords with the ECT Act.[74]

2.2.3.2 Exception: secondary evidence

In terms of the secondary evidence exceptions (to the best evidence rule), if the original document cannot be produced, the contents of the document can be proved by a true copy or by oral testimony. If a particular form of a copy is made admissible by statute, other secondary evidence will be accepted only after the party intending to produce it has accounted for the absence of both the original and the statutory copy.[75] Secondary evidence of a document will, furthermore, be admissible if the document is in the possession of a person residing outside the jurisdiction of, and not amenable to, the process of the court, but there must be evidence that sufficient effort was made to persuade him to produce it,[76] or if the document is destroyed[77] or there is evidence that it cannot be found after a thorough search.[78] Secondary evidence may be given when the production of the original writing would be impossible, unlawful, or very

exists no reasonable possibility of "some interference" with the recordings as stipulated in *S v Singh and Another* 1975 (1) SA 330 (N)

72 2010 2 All SA 116 (SCA) at par 27

73 Zeffert & Paizes *Essential Evidence* 128

74 It should, however, be noted that computer-generated documents were admitted as authentic copies rather than original documents since it is well established that authentic copies may be relied on when it is impossible or impracticable to produce the original. See Ch 1 par 1.2 for the nature of electronic evidence and S 14 of the ECT Act dealing with original as far as data message is concerned

75 *Mabena v Brakpan Municipality* 1956 1 SA 179 (T)

76 *Boon v Vaughan & Co Ltd* 1919 TPD 77

77 It must not be destroyed in contemplation of litigation but in the ordinary course of business as it was in *Barclays Western Bank Ltd v Creser* 1982 2 SA 104 (T) where a bank systematically destroyed its records, after storing them on microfilm, because of a lack of storage space

78 *S v Tshabalala* 1980 3 SA 99 (A); *Singh v Govender Brothers Construction* 1986 4 SA 613 (N) at 617D-E

inconvenient, for instance a notice affixed to a wall[79] or a certificate that could not lawfully be removed.[80]

2.2.4 Types of evidence

As previously pointed out, the nature of electronic evidence can be a controversial issue. It is, therefore, important to identify and explain the different types of evidence which might have an influence on electronic evidence as well as any evidence which could be of interest in a study focusing on the interaction between technology and law.

2.2.4.1 Oral evidence

As a general rule, in both criminal and civil cases, evidence must be given orally by the witnesses in the presence of the parties. The rationale behind this practice is to allow parties the opportunity to confront the witnesses who testify against them and challenge the evidence by questioning it in a situation where the demeanour of the witness can be observed to assess his credibility.[81] With the advent of technology, it is now possible for oral evidence to be given by means of closed circuit television or a similar electronic device.[82] This is why it is important to introduce this type of evidence since it will guide future discussions in the context of this research. Oral evidence must generally be given on oath or affirmation.[83] The South African trial system, based on orality, is characterised by the existence of the following components: examination in chief,[84] cross-examination,[85] re-examination,[86] and examination by the court.[87]

2.2.4.2 Real Evidence

Real evidence comprises all things examined by the court as a means of proof, which, upon proper identification, itself becomes evidence.[88] It consists of objects (such as a knife) received

---

79 *Watts and Darlow v R* 1919 NLR 108

80 *R v Zungu* 1953 3 SA 660 (N)

81 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 362

82 S 158(2) of the CPA

83 S 162 and 163 of the CPA; S 39 and 40 of the CPEA

84 It consists of the presentation of evidence favourable to the version of the party calling the witness

85 This is the name given to the questioning of the opponent's witness. It succeeds examination in chief

86 The purpose of re-examination is to clear up any point of misunderstanding which might have occurred during cross-examination

87 The court has the right to question a witness at any stage of the proceedings

88 *S v M* 2008 2 SACR 613 (SCA)

by the court, video recordings, photographs, electronically processed, produced, or recorded data, and specimens of handwriting.[89] If properly identified real evidence is relevant and there is no rule of evidence excluding its reception, it will be received as an exhibit, duly labelled and numbered, and available for inspection by the court.[90] Real evidence is seldom of much assistance unless it is supplemented by the testimony of witnesses.[91]

The following are some examples of real evidence that call for particular comment in the context of this research.

2.2.4.2.1 Photographs, films, tape, and video recordings[92]

Photographs can be used either to present places or things which are difficult to produce in court, such as damaged vehicles, or to enable witnesses to identify persons. Such photographs are real evidence. There must be evidence identifying the photographs as a true likeness of the place, object, or person which they purport to represent.[93] Section 232 of the CPA expressly allows for the production of photographs.

Sometimes a photograph can be treated as a document.[94] This situation is discussed below under paragraph 2.2.4.3 dealing with documentary evidence.

The principles relating to the use of films as real evidence are the same as those relating to photographs.[95] This was confirmed in the English case *The Statue of Liberty*,[96] an action concerning the collision between two ships, where a film of radar echoes recorded by a shore radar station was accepted as real evidence.

---

89 Zeffert & Paizes *Essential Evidence* 271

90 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 395

91 In a stabbing case, for example, the production of a knife is relevant only if there is evidence showing that it was used by the accused, and medical or other evidence that it could have caused the injuries in question. (Zeffert & Paizes *The South African Law of Evidence* (2nd ed) 2009 (hereafter referred to as Zeffert & Paizes *The SA Law of Evidence*) 849

92 An article worth mentioning in regard to documents, tape and video recordings and the law of evidence is De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" 2010 *SALJ* 558 (hereafter referred to as De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)"

93 Zeffert & Paizes *The SA Law of Evidence* 850

94 In terms of S 33 of the CPEA and S 222 of the CPA and, therefore, admissible in evidence without further identification if the photographer has acknowledged in writing that he is responsible for its accuracy

95 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 400

96 1968 1 WLR 739

Tape recordings may be admissible as real evidence.[97] The court should be satisfied that it is shown *prima facie* that the recording is original and sufficiently intelligible.[98] Sometimes a transcript of the recording will be admissible in evidence, subject to the court's being satisfied as to the accuracy of the transcription.[99]

Video records may be accepted as real evidence as the followings cases illustrate, *S v Mpumlo*,[100] *S v Ramgobin*,[101] and *S v Baleka*.[102]

2.2.4.2.2 Computer and machine-generated evidence

Computer and machine-generated evidence may, depending on the circumstances, be admitted as real evidence. For such evidence to be admitted as real evidence, it must have been generated without the intervention of the human mind.[103] If, however, the evidence was derived in part or in whole from a statement made by a person, then hearsay considerations would come into play.[104] In the above-mentioned case of *The Statue of Liberty*,[105] radar soundings of a ship's movement on the River Thames were held to be real evidence rather than hearsay evidence as the machine was operating without human intervention.[106] The admission of computer and machine-generated evidence as real evidence will be further examined in the analysis of *S v Ndiki and Others*.[107]

2.2.4.2.3 Documents

A document may be tendered in evidence for a variety of purposes, namely a party may rely upon the statements it contains as evidence of their truth, by way of exception to the hearsay rule or simply as original evidence, for example to show that they were made. In that instance, it

97 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 398
98 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 398
99 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 398
100 1986 3 SA 485 (E).The court held that a video film was not a document but real evidence which, so long as it satisfies the requirement of relevance, could be produced, subject to any dispute as to authenticity or interpretation
101 1986 4 SA 117 (N).The court held that there was no difference in principle between the admission of audio tapes and video recordings
102 1986 4 SA 192 (T).It was held that sound recordings and video recordings, and a combination of the two, are real evidence to which the rules relating to documentary evidence are not applicable
103 *The Statue of Liberty* 1968 1 WLR 739
104 Zeffert & Paizes *The SA Law of Evidence* 860
105 1968 1 WLR 739
106 *The Statue of Liberty* 1968 1 WLR 739 at 742
107 2007 2 All SA 185 (Ck)

constitutes documentary evidence and is subject to the rules considered in the next paragraph.[108] If, however, the document is tendered in evidence as a material object regardless of the words contained in it, to show, for example, its existence, the substance of which it is made (for example, parchment or paper) or the condition that it is in (crumpled or torn), it constitutes real evidence.[109]

2.2.4.3 Documentary Evidence

Apart from the testimony of witnesses and the introduction of real evidence, evidence may also be given by producing documents to the court. The term "document" is very wide and includes everything containing the written or pictorial proof of something.[110] In *R v Daye*,[111] a document was defined as "any written thing capable of being evidence" regardless of the material on which it was written. Various statutes define "document". In terms of the CPEA, "document" includes any book, map, plan, drawing, or photograph.[112] The CPA, on the other hand, defines a document as including "any device by means of which information is stored or recorded".[113] The ECT Act extends the definition of "document" to incorporate data message.[114]

As a general rule, for a document to be admissible in evidence it must satisfy three general rules, namely: (1) the original document must be produced, subject to exceptions; (2) the document must be authenticated; and (3) the document may have to be stamped in accordance with the Stamp Duties Act 77 of 1968.[115]

2.2.4.3.1 Original

The general rule stipulates that no evidence is ordinarily admissible to prove the contents of a document except the original document itself.[116] According to Zeffert and Paizes, a document is

---

108 De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" 562

109 Keane & Mckeown *The Modern Law of Evidence* 264; *R v Rice* 1963 1 QB 857, CCA (Ch 10)

110 *Seccombe and Others v Attorney-General and Others* 1919 TPD 270 at 277, cited by Mullins J in *S v Mpumlo and Others* 1986 3 SA 485 E at 489D-F

111 1908 2 KB 330 at 340

112 S 33

113 S 221

114 Data message is "data generated, sent, received or stored by electronic means and includes (a) voice, where voice is used in an automated transaction; and (b) a stored record", S 1

115 Zeffert & Paizes *The SA Law of Evidence* 828

116 *Standard Merchant Bank Ltd v Creaser* 1982 4 SA 671 (W) at 674B

an original if, according to substantive law and the issues raised in the trial, it is the document the contents of which have to be proved.[117]

The original rule also allows for the recognition of multiple originals in the case of carbon copies,[118] initialled copies, and even a roneoed copy.[119] This is interesting as, by analogy, it can apply to electronic documents as well.

An exception to the rule of original is the possibility of proving the contents of a document by way of secondary evidence. This is possible in the following circumstances: (1) the document is lost or destroyed; (2) the document is in the possession of the opposing party or third party; (3) it is impossible or inconvenient to produce the original; and (4) it is permitted by statute.[120]

2.2.4.3.2 Authenticity

A party who produces a document in evidence is ordinarily required to adduce evidence to satisfy the court of its authenticity, in other words to prove that the document was written or executed by the person who purports to have done so. This can be done in a variety of ways, of which the most common would be to call the writer to identify the document, or to present evidence of a person who saw him sign or write it or who can identify his handwriting. Authenticity can also consist of proving that a document was found in someone's possession.[121]

---

117 If the contents of a telegram alleged to have been sent by the accused are relied upon as evidence of his guilt, the form which he filled in at the post office is the original document, and the telegram actually delivered is secondary evidence only (*R v Regan* 1887 16 Cox CC 203). See, in general, Zeffert & Paizes *The SA Law of Evidence* 830

118 *Lynes v International Trade Developer Inc* 1922 NPD 301

119 *HerstigteNasionale Party van Suid-Afrika v Sekretaris van BinnenlandseSake en Immigrasie* 1979 4 SA 274 (T) ;a roneod copy is a copy made on a Roneograph which is a rotary duplicator that uses a stencil through which ink is pressed, http://www.wordwebonline.com/en/RONEOGRAPH (accessed on 12/05/2016)

120 *Singh v Govender Brothers Construction* 1986 3 SA 613 (N).See also *R v Amod & Co (Pty) Ltd* 1947 3 SA 32 (A) at 40, *S v Tshabalala* 1980 3 SA 99 (A) and *S v Adendorff* 2004 2 SACR 185 (SCA).See Ch 2 par 2.2.3.2 above

121 The ways of authenticating were described by Human J in *Howard & Decker Witkoppen Agencies and Fourways Estates (Pty) Ltd v De Sousa* 1971 3 SA 937 (T) at 940E-G as follows: "The law in relation to the proof of private documents is that the document must be identified by a witness who is either (i) the writer or the signatory thereof, or (ii) the attesting witness, or (iii) the person in whose lawful custody the document is, or (iv) the person who found it in possession of the opposite party, or (v) a handwriting expert, unless the document is one of which proves itself, that is to say unless it:

(1) is produced under discovery order, or
(2) may be judicially noticed by the court, or
(3) is one which may be handed in from the Bar, or
(4) is produced under a subpoena *duces tecum*, or

Authenticity of electronic documents can be done using different authentication techniques, such as the testimony of a witness with personal knowledge, by their distinctive characteristics and the like,[122] or by a process or system,[123] for example electronic signatures.[124]

With regard to electronic evidence in the form of social media evidence for example, it is submitted that there are two requirements that must be satisfied: demonstrate that the evidence originates from the social media site in question and attribute it to a specific person.[125] The first requirement can be accomplished by calling a person with personal knowledge of the social media site to testify that the evidence comes from the specific site.[126] The second requirement can be met, if there is no admission from the person who created the social media evidence, by means of circumstantial evidence.[127] In other words one will need either to look at the "access and control" of the social media information or at the information itself to determine if it contains "distinctive characteristics."[128]

2.2.4.3.3 The Stamp Duties Act 77 of 1968[129]

In terms of section 12 of the Stamp Duties Act 77 of 1968, save as is otherwise expressly provided in any law, no instrument required to be stamped under this Act shall be made available for any purpose whatever unless it is duly stamped. This requirement is not applicable to

(5) is an affidavit in interlocutory proceedings, or
(6) is admitted by the opposite party."

122 Rule 901(b)(4) of the Federal Rules of Evidence (text governing evidence in the USA), this rule provides that the distinctive characteristics of an item, including its "appearance, contents, substance, [or] internal patterns" may, in conjunction with circumstances, authenticate an item

123 Rule 901 (b)((9) of the Federal Rules of Evidence which states that authentication may be accomplished through evidence describing "the process or system used to produce a result and showing that the process or the system produces an accurate result."See in general Goode "The admissibility of electronic evidence" 2009-2010 *Rev. Litig.* 29(*1)* 1

124 The authenticity of electronic documents is discussed at length under Ch 4 par 4.3

125 Hoffmeister *Social Media in the Courtroom, A New Era for Criminal Justice?* 2014 (hereafter referred to as Hoffmeister *Social Media in the Courtroom)* 155

126 Hoffmeister *Social Media in the Courtroom* 155

127 Hoffmeister *Social Media in the Courtroom* 155

128 Hoffmeister *Social Media in the Courtroom* 156

129 Repealed by S 108 of the Revenue Laws Amendment Act 60 of 2008

documents submitted in criminal proceedings, and, in civil matters, the failure to have a document stamped will not constitute an absolute bar to admissibility.[130]

As far as electronic documents are concerned, it must be stressed that, if a document is required to be stamped in terms of the Stamp Duties Act, the ECT Act will not be applicable.[131] In other words, the provisions of the former Act will prevail, and the electronic document will need to be reduced to paper and the necessary stamp affixed.[132]

2.2.4.4 Hearsay Evidence

2.2.4.4.1 Common law

At common law, hearsay evidence was defined as any statement other than the one made by a person while giving oral evidence in the proceedings and presented as evidence of any fact or opinion stated.[133] To determine whether a statement was hearsay or not, the purpose of tendering the statement was to be considered. If the purpose was to establish the truth of what is contained in the statement, the evidence will be hearsay and inadmissible.[134] On the contrary, if the purpose was not to establish the truth of the statement but, rather, the fact that it was made, the statement will not be hearsay and will be admissible.[135]

Given the fact that the common law hearsay rule led to the exclusion of relevant and reliable evidence, a number of *ad hoc* exceptions was developed.[136] *Res gestae*[137] statements are examples of these exceptions. Various categories of *res gestae* were developed to facilitate the admission of hearsay evidence, of which "spontaneous statements" call for particular comment

---

130 See Schwikkard & Van der Merwe *Principles of Evidence* (2009) 408 and Zeffert & Paizes *The SA Law of Evidence* 842-843

131 S 4(3) read with schedule 1 of the ECT Act

132 Ch 3 par 3.4.2.1.1 C

133 Tapper *Cross & Tapper on Evidence* 588

134 Tapper *Cross & Tapper on Evidence* 588

135 *Subramaniam v Public Prosecutor* 1956 1 WLR 965 at 969

136 Although the exceptions are now obsolete (*Mnyama v Gxalaba* 1990 1 SA 650 (C)), PJ Schwikkard suggests that they may still be considered as "any other factor" that the court may take into consideration in exercising its discretion to admit hearsay evidence in the interests of justice; Schwikkard & Van der Merwe *Principles of Evidence* (2009) 286

137 The meaning of this phrase was stated by Choo as follows, "evidence of facts may be admissible as part of the *res gestae* if these facts are so closely connected in time, place, and circumstances with some transaction which is at issue that they can be said to form part of that transaction." Choo *Evidence* 2006 (hereafter referred to as Choo *Evidence*) 235

in the context of this research because electronic communication may contain more unguarded and spontaneous remarks than any other previous form of human communication. Unlike anything else available, it captures the present sense and contemporaneous reactions, opinions, and feelings of individuals as they live in the moment.[138] Consequently, it might be right to consider electronic communication as a form of *res gestae*.

In spite of their hearsay nature, spontaneous statements were admissible because they were considered to be the product of an instinctive response and, therefore, less likely to be an invention or deliberate distortion.[139] For a statement to be considered spontaneous, it had to be so closely linked to the event which gave rise to it that the presiding officer was able to conclude that the "event" dominated the mind of the declarant at the time of uttering the statement.[140]

2.2.4.4.2 The Law of Evidence Amendment Act 45 of 1988

The enactment of this piece of legislation superseded common-law rules applicable to hearsay. Hearsay, now statutorily regulated, is defined under the Law of Evidence Amendment Act 45 of 1988 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".[141] Such evidence remains in principle inadmissible. It may, however, be admissible in evidence at criminal or civil proceedings by consent,[142] provisionally where the court is informed that the person upon whose credibility the probative value of the evidence depends is going to testify during the proceedings,[143] or by discretion of the court in the interests of justice.[144]

---

138 Overly *Overly on Electronic Evidence in California* 1999 (hereafter referred to as Overly *Overly on Electronic Evidence in California*) 2-1

139 Choo *Evidence* 235

140 *S v Tuge* 1966 4 SA 565 (A).The court held that for a *res gestae* statement to be admitted into evidence: (a) "the original speaker must be shown to be unavailable as a witness";(b) "there must have been an occurrence which produced a stress of nervous excitement";(c) the statement must have been made whilst the stress was still "so operative on the speaker that his reflective powers may be assumed to have been in abeyance";(d)"the statement must not amount to a reconstruction of a past event". See also Schwikkard & Van der Merwe *Principles of Evidence* (2009) 286

141 S 3(4)

142 S 3(1)(a)

143 S 3(1)(b)

144 S 3(1)(c). The court must have regard to:
i The nature of the proceedings;
ii The nature of the evidence;

It should be stressed, however, that the Law of Evidence Amendment Act preserves the statutory exceptions to hearsay enacted before 1988,[145] while abolishing the so-called common-law exceptions.

2.2.4.5 Opinion evidence

Opinion evidence is evidence based on the opinion, that is, inference, conclusion, impression, or belief of a witness, whether expert or lay person.[146] Any opinion, whether expert or not, expressed on an issue which the court can decide without receiving such opinion is in principle inadmissible owing to its irrelevance.[147] By contrast, if the opinion can be of assistance to the court because the witness is in a better position than the court to form an opinion, the opinion will be admissible on the basis of its relevance.[148] There is little doubt that, given weak knowledge of technology matters by presiding officers, opinion evidence and, in particular, expert opinion evidence is (especially critical in issues relating to electronic evidence). Indeed, to ensure, for instance, that electronic evidence is authentic and has remained unaltered, the testimony of an expert in digital forensics is necessary. Digital forensics is the branch of forensic science dealing with the investigation of all devices capable of storing digital data. The most common application of digital forensics investigation is to support or refute a hypothesis before criminal or civil courts (as part of the electronic discovery process), during an internal corporate investigation in the private sector, or intrusion investigation (specialist probe into the nature and extent of unauthorised network intrusion).[149]

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.

145 Some important exceptions are Part VI of the Civil Proceedings Evidence Act 25 of 1965, the Criminal Procedure Act 51 of 1977 (sections 221, 222, 236, 246, and so on), the Computer Evidence Act 57 of 1983, the ECT Act

146 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 83

147 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 87; see also generally *S v H* 1981 2 SA 586 (SWA)

148 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 87

149 http://www.appyide.org/working-groups/digital-forensics/ (accessed on 29/10/15)

2.2.5 Miscellaneous concepts

2.2.5.1 Relevance

To be admitted in either criminal or civil proceedings, evidence must be relevant.[150] Relevance is essentially a matter of reasoning, common sense, and practicality. In *R v Matthews* [151] it was said that relevance is based on "a blend of logic and experience lying outside the law". In addition it was held in a more recent case that "the concept of relevance...is...essentially a matter of common sense, having its foundation in the facts, circumstances and principles of each particular case".[152] Relevance is not determined in a vacuum but on the facts of each particular case. In law, therefore, evidence is said to be irrelevant if, as a matter of common sense, it is totally irrelevant, or if, for the purpose of the trial, it is not sufficiently relevant to warrant it being received because the practical disadvantages outweigh its probative value.[153] Electronic evidence may face that challenge, that is, being excluded in spite of its relevance because its complexity may outweigh its probative value. It should, thus, be stressed that the fact that evidence is relevant does not necessarily mean that it will be admitted. Such evidence may not be received, for example, if there is a rule that excludes it.[154]

The requirement of relevance was considered in two American cases dealing with electronic evidence in the form of social media evidence, *State v Gaskins*,[155] and *State v Corwin*.[156] In the first case the defendant attempted unsuccessfully to introduce into evidence the Myspace profile of a minor with whom he was accused and convicted of having improper sexual contact. According to him the minor claimed on the said Myspace profile that she was 18 and had been sexually involved with an adult.[157] The defendant could not, however, provide evidence that he saw the Myspace profile before the unlawful sexual evidence, nor that the Myspace page was

150 S 210 of the CPA provides that "no evidence as to any fact, matter, thing shall be admissible which is irrelevant or immaterial and which cannot conduce to prove or disprove any point or fact in issue"; S 2 of the CPEA contains a substantially similar provision

151 1960 1 SA 752 (A)

152 *Van den Berg v Coopers & Lybrand Trust (Pty) Ltd and Others* 2001 2 SA 242 (SCA); See also Zeffertt & Paizes *Essential Evidence* 75

153 Zeffertt & Paizes *The SA Law of Evidence* 239

154 Such as privilege or unconstitutionally obtained evidence

155 No. 06CA0086-M (Ohio App. 9 Dist. Aug. 13, 2007)

156 295 SW 3d 573 (Mo. Ct. App. S.D. 2009)

157 *State v Gaskins* No. 06CA0086-M (Ohio App. 9 Dist. Aug. 13, 2007) at {33}

created before the assault.[158] In fact there was no dispute that the page was created after the incident and therefore the trial court held that the fact that the minor represented herself as eighteen years old after the incident was not relevant, what mattered was the defendant's belief regarding the minor's age at the time of the incident.[159] This was confirmed on appeal.[160]

In the second case, according to Hoffmeister,[161] the defendant sought to introduce into evidence a Facebook page to discredit the victim's version. The page contained posts related to sex, drinking, and passing out. The judge did not find these posts relevant to the issue in dispute, which was whether there was an attempt by the defendant to rape the victim on a specific night.[162] The decision was upheld on appeal.[163]

In South Africa, the recent case of *Harvey v Niland and Others*,[164] addressed the notion of relevance. Dealing with the admissibility of Facebook communications, the judge highlighted the common law principle that all relevant evidence not rendered inadmissible by an exclusionary rule is admissible in a civil court irrespective of the manner it was obtained.[165] In the present case the court was required to decide on the admissibility of an annexure consisting of printouts of Facebook communications obtained unlawfully. Plasket J referred to *Protea Technology Limited & Another v Wainer & Others*,[166] where it was argued that "the criminalisation of telephone-tapping (by section 2 of the Interception and Monitoring Prohibition Act 127 of 1992) had the result that a court had no choice but to exclude evidence obtained from the unlawful tapping of a person's telephone."[167] Heher J in the latter case disagreed and held that "the statute does not expressly or by necessary inference render the production of recordings made in

158 *State v Gaskins* No. 06CA0086-M (Ohio App. 9 Dist. Aug. 13, 2007) at {33}
159 *State v Gaskins* No. 06CA0086-M (Ohio App. 9 Dist. Aug. 13, 2007) at {34}
160 *State v Gaskins* No. 06CA0086-M (Ohio App. 9 Dist. Aug. 13, 2007) at {35}
161 Hoffmeister *Social Media in the Courtroom* 153
162 Hoffmeister *Social Media in the Courtroom* 154
163 Hoffmeister *Social Media in the Courtroom* 154
164 (5021/2015) [2015] ZAECGHC 149; 2016 (2) SA 436 (ECG); (2016) 37 ILJ 1112 (ECG) 2015
165 *Harvey v Niland and Others* (5021/2015) [2015] ZAECGHC 149; 2016 (2) SA 436 (ECG); (2016) 37 ILJ 1112 (ECG) 2015 at [38], to substantiate this the judge referred to *Protea Technology Limited & another v Wainer & others* [1997] 3 All SA 594 (W) at 604b-c
166 [1997] 3 All SA 594 (W)
167 *Protea Technology Limited & another v Wainer & others* [1997] 3 All SA 594 (W) at 602 d-e

contravention of its terms inadmissible in evidence before a court trying a civil dispute".[168] After considering case law and all relevant factors Plasket J was satisfied that the annexure was admissible.[169]

2.2.5.2 Admissibility and weight of evidence

These two notions should not be confused. If what is adduced can, in law, properly be put before the court, it is admissible.[170] Once it has been or could be admitted, its cogency or persuasiveness, alone or in conjunction with other evidence, can be considered.[171]

Evidence is either admissible or inadmissible; it cannot be more or less admissible. After being ruled admissible, it can carry more or less weight depending on the particular circumstances of the case. As a general rule, admissibility of evidence is determined on the basis of its relevance which, in turn, is determined by considering the potential weight of evidence in a preliminary investigation to determine whether such evidence would be of assistance in proving the facts at issue.[172]

New developments in law have removed the obstacles in admissibility of electronic evidence.[173] Problems, nevertheless, remain with the weight of such evidence given the complex and sophisticated nature of the rapidly-changing technology which generates electronic evidence.

2.2.5.3 Direct and circumstantial evidence

Direct evidence is evidence which is usually in the form of oral testimony of a witness who perceived the facts at issue with his own unaided senses.[174] Hence the human perception of a screen print-out is admissible.[175]

---

168 *Protea Technology Limited & another v Wainer & others* [1997] 3 All SA 594 (W) at 606 e-f

169 *Harvey v Niland and Others* (5021/2015) [2015] ZAECGHC 149; 2016 (2) SA 436 (ECG); (2016) 37 ILJ 1112 (ECG) 2015 at [53]

170 Admissibility

171 Weight

172 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 20

173 S 15(1) of the ECT Act

174 Huxley *Evidence the Fundamentals* (2nd ed) 2010 (hereafter referred to as Huxley *Evidence the Fundamentals*) 5

175 The image on a screen can constitute sufficient evidence of data copied on to the RAM of a computer used to play counterfeit games to establish an offence of breach of copyright *R v Gilham* [2009] EWCA Crim 2293,

In contrast to direct evidence, circumstantial evidence is evidence from which the existence or non-existence of facts at issue may be inferred. So, proof that the defendant owns a gun is indirect or circumstantial evidence of his involvement in a crime if it is shown that his gun was used to kill P.[176] Most of the digital evidence produced in court is indirect evidence for which the most significant inference to be made consists of the assertion that the evidence is accurate, and can, therefore, be trusted.[177]

2.3 Electronic Evidence

2.3.1 Definition

Electronic evidence, sometimes described as "digital evidence" or "computer evidence", may be defined using two approaches. The first is a narrow approach tailored to the current state of technology, which is a very risky approach considering the rapid technological change which can make a narrow definition become obsolete within years if not months.[178] The second approach, which is suitably future proof and preferred for this research, focuses on the most abstract aspects of technologies and will, therefore, cut across traditional divisions and categories in the law of evidence.[179] The definition below follows this approach. According to Stephen Mason and Burkhard Schafer, electronic evidence means:

> data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less probable than it would be without the evidence.[180]

To grasp this definition fully, it is important to clarify the meaning of certain terms. Two terms particularly call for clarification, namely "digital" and "analogue".

"Digital" is defined in the *Oxford English Dictionary* as made of signals, information or data represented by a series of discrete values (commonly the numbers 0 and 1), typically for

---

173 CL&J 749, *Times* (12 January 2010), cited by Stephen Mason in *Electronic Evidence* (2nd ed) 2010 (hereafter referred to as Mason *Electronic Evidence* (2010)) 302

176 Huxley *Evidence the Fundamentals* 5

177 Mason *Electronic Evidence* (2010) 302

178 Mason *Electronic Evidence* (2010) 22

179 Mason *Electronic Evidence* (2010) 22

180 Mason *Electronic Evidence* (2010) 25

electronic storage or processing. Such data is commonly represented by discrete values of physical quantity such as voltage or magnetic polarization, typically in binary form.[181]

In contrast to "digital", "analogue", when referring to a device, means a device that makes use of analogue signals or data, or, in other words, a device that operates by the manipulation of continuously variable physical quantities which are analogues of the quantities being computed.[182] Data is analogue if it is created by an analogue device.

In simple terms, both these technologies are used to transmit information, audio or video, which is transformed into electric signals. The difference is that in analogue technology information is translated into electric pulses of varying amplitude, while, in digital technology, the translation of information is into binary format (zero and one) where each bit is representative of two distinct amplitudes.[183] In addition, data are subject in analogue technology to deterioration by noise during transmission and write-read cycle, while in digital technology the transmission and write-read cycle of data are noise-immune without deterioration.[184] Examples of analogue data include outputs of analogue devices such as analogue recordings, audio or video information recorded as an analogue signal (audio cassettes, video tapes), analogue cameras (photographic films), or vinyl records. Examples of digital data include data created, transmitted, or stored through the following media, digital radio, digital television, digital photography, GPS, digital laptops, digital computers, digital tablets, smartphones, MP 3 players, digital cameras, or the Internet.[185]

The definition of electronic evidence suggested above is to be welcomed in that it is technology neutral and covers the whole subject matter of this research, which is electronic evidence in its widest sense. It will, therefore, be retained for the purposes of this thesis. Firstly, it includes all

---

181 *Oxford English Dictionary available at* http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/52611?redirectedFrom=digital#eid (accessed on 06/03/2013)

182 *Oxford English Dictionary available at* http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/7029?redirectedFrom=analogue#eid(accessed on 07/03/2013)

183 Anonymous "Analog vs Digital" available at http://www.diffen.com/difference/Analog_vs_Digital (accessed on 07/03/2013)

184 Anonymous "Analog vs Digital" available at http://www.diffen.com/difference/Analog_vs_Digital (accessed on 07/03/2013)

185 Anonymous "Analog vs Digital" available at http://www.diffen.com/difference/Analog_vs_Digital (accessed on 07/03/2013)

forms of evidence created, manipulated, or stored in a computer in its widest meaning. "Computer" should be understood here as an electronic device[186] (or system of devices) which is used to store, manipulate, and communicate information, perform complex calculations, or control or regulate other devices or machines, and is capable of receiving information (data) and of processing it in accordance with variable procedural instructions (programs or software).[187] Thus, "computer" in this sense should not be restricted to what is commonly called computer.[188] Secondly, the suggested definition includes the various forms of devices by which data can be stored or transmitted, including analogue devices that produce an output. It includes, for example, "computer" as defined above, telephone systems, wireless telecommunication systems and networks, such as the Internet, and computer systems that are embedded into a device, such as mobile telephones, smart cards, and navigation systems. The third element restricts the data to information relevant to the process by which a dispute, irrespective of the nature of the disagreement, is decided by the adjudicator.[189]

This definition also includes what we can refer to as data message evidence in the meaning of the ECT Act. "Data message" is defined in this Act as meaning:

> 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.[190]

And "data" in terms of the ECT Act means:

> electronic representation of information in any form.[191]

As a result, data message evidence can be defined as evidence consisting of electronically represented information, irrespective of its form, which is generated, sent, received, or stored by electronic means and which includes voice, where voice is used in an automated transaction, and

---

186 Operating according to the principles or methods of electronics (study of phenomena associated with the flow of electrons and practical application of such phenomena), such as a transistor, microchip, or electron tube.

187 *Oxford English Dictionary available at* http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/37975?redirectedFrom=computer#eid121196826(accessed on 07/03/2013)

188 A personal computer or a laptop

189 Mason *Electronic Evidence* (2010) 25

190 S 1

191 S 1

a stored record. Without any doubt it falls within the scope of our adopted definition of electronic evidence.

2.3.2 Characteristics of electronic evidence in digital format

Documentary evidence is a particularly important form of evidence in South Africa as it is in many other common law legal systems, such as those of England or Singapore. Consequently, electronic documents, an important form of electronic evidence, play a significant role in the law of evidence and can constitute a good example to illustrate some of the most important characteristics of electronic evidence.[192]

The fact that many of the most important software applications that enable the creation of electronic documents or files intentionally mimic the "look and feel" of traditional, paper-based stationary, allowing these electronic documents to be stored in folders or thrown away in a trash bin when no longer needed, should not create the misleading impression that electronic documents are exactly the same as paper documents and that they exist somewhere on the computer as a single, complete whole and maintain their structural integrity even when the file is closed or the computer is switched off, as a paper document continues to exist when it is put out of sight and into a folder.[193] It should be acknowledged that electronic documents have particular characteristics which affect both the test for authenticity and the way evidence is secured and handled.[194] These characteristics are outlined below. They relate to dependence on machinery and software, mediation of technology, technical obsolescence, volume and replication, storage media, deletion and destruction of electronic evidence and metadata.

2.3.2.1 Dependence on machinery and software

Paper documents can be easily accessed even long after their creation provided one has good eyesight and knowledge of the language in which the document is written. This is not the case with electronic data which depend on hardware and software to be rendered into human readable format. This is why an electronic document is better understood as a "process by which otherwise unintelligible pieces of data that are distributed over the storage medium are

192 Mason *Electronic Evidence* (2010) 26
193 Mason *Electronic Evidence* (2010) 26
194 Mason *Electronic Evidence* (2010) 26

assembled, processed and rendered legible for a human user".[195] In that sense, the document is nowhere; it does not exist independently from the process that recreates it every time a user opens it on screen.

Hardware and software produce electronic evidence, for example metadata or logs which are relevant to an electronic document. It should be noted that many software programs that were common in the 1990s are no longer commercially available, and, even if they were available, it might be impossible to install them onto an up-to-date version of the operating system. Reading old data might, thus, sometimes be a headache because it might be necessary to have a specific machine with specific software installed, causing additional costs to a party, as in the case of *PHE, Incorporated dba Adam & Eve v Department of Justice*,[196] where PHE was ordered to review information contained in a database despite the fact that no program existed to enable them to obtain the information requested by the Department of Justice.[197]

2.3.2.2 Mediation of technology

For data in electronic format to be human-readable, the mediation of a set of technologies is required. As a consequence, the display of the same source object may vary according to the technology used. The appearance of a Website, for example, can vary depending on when it is viewed and what browser is used. Hence, there can be no concept of a single, definitive representation of a particular source digital object. From a legal point of view, this can have dramatic consequences. A good example is the case of a contract in electronic format drafted carelessly and referring to paragraphs of the contract without enumerating them, since in the original version the paragraphs are plainly visible through line breaks in the text. Once sent to the buyer, however, and opened with a different software program, paragraphs are no longer apparent. The use of technology can also alter electronic evidence, for example by altering its metadata. This will occur by the mere fact of starting a computer and opening the document. The observation of electronic evidence by different persons using only marginally different machinery which will recreate different versions of the electronic evidence in question creates difficulty in determining which version should be regarded as the more authentic. This is why it

195 Mason *Electronic Evidence* (2010) 28
196 139 F.R.D. 249 (D.D.C. 1991)
197 Mason *Electronic Evidence* (2010) 28

is important to have protocols and standards to minimise the risks associated with the handling of electronic evidence. Appropriate standards, benchmarks, and procedures for the type of hardware and software used must exist. This is easily available for commonly-used platforms such as Windows®, but not so for the proprietary software of a third generation mobile phone or an unusual type of open source software, for example.[198]

2.3.2.3 Technical obsolescence

Technical obsolescence is a major problem facing electronic documents. Indeed, with rapid technological change in operating systems, application software, and hardware, electronic documents may reach a point where they cannot be read, understood, or used. This is particularly of concern in relation to disclosure or discovery. It may also happen that a software company no longer produces software backward or downward compatible, or, in other words, new versions of the software which are able to operate with other products that were designed for an older product.[199]

2.3.2.4 Volume and replication

The integration in the latter quarter of the twentieth century of telecommunications and computers giving rise to computer networks has been the trigger for the increase in the creation and exchange of data. Computers, previously confined to a specific geographical area, started to be linked by way of local area networks and computer networks, and, later, local area networks were linked through wide area networks, the best known of which is the Internet. From that point, users were able to create and transmit large volumes of data. A simple example is the case of a single word-processing document which can be sent to an indefinite number of people across the globe. By sending this file to a given number of people, the number of copies is likely to increase if each addressee copies the file to another drive on its computer, and the organisation backs up the email database each day, then backs up the main database each week, and afterwards burns the copies on CD-ROMs or stores them on other external devices. This is known as networked communications. In essence, emails, instant messaging, and other forms of communication are a duplicate and distributed technology. Consequently, the amount of data to

198 Mason *Electronic Evidence* (2010) 28-29

199 Mason *Electronic Evidence* (2010) 28-29

be searched to identify relevant documents for litigation or the prosecution of a criminal offence becomes enormous.[200] In the Enron investigation case, for example, a dataset corpus of 500MB of messages was posted to the Web, and dealing effectively with such an amount of data is not easy. Methods of analysis exist, such as data-mining software or link analysis software, with their own problems of accuracy, reliability, and prejudicial effects. There is, furthermore, another controversial issue with regard to the number of copies of a document in existence which can affect the parties to litigation in the determination of the version of the document upon which to rely. An email, for example, will exist in any case on at least two computers or servers, the sender one and the recipient one. The metadata in the sent email will differ from the metadata in the received email, even if nothing else in the email is altered. In case there is a dispute on the content of the email, it will be important to determine the content of which email should be trusted over the content of the other. Digital forensics will, therefore, play a critical role in that regard.[201]

2.3.2.5 Storage media

The media upon which electronic data is stored is fragile and unstable, and it can deteriorate quickly and without external signs of deterioration if not stored correctly. It also runs the risk of accidental or deliberate damage and accidental or deliberate deletion. The form of storage media also changes. It started with a variety of floppy disk drives; the 8-inch gave way to the 51/4-inch, which was superseded by the 3.5-inch, and then came the Zip® drive produced by Iomega® which was less popular than the 3.5-inch floppy disk. Most forms of floppy disk have now been superseded by flash-drive systems and rewritable CDs, CD-ROM and DVDs.

In addition, computers and systems now operate largely in a networked environment, in a world parallel to the physical world allowing a number of products, such as MP3 files, computers, laptops, mobile telephones, personal digital assistants or PDAs, Blackberry®, and iPAQ® to be linked by means of applications, including facsimile transmissions, voice over Internet protocol (VoIP), email, computer to computer, and instant messaging, that run over networks (the Internet, intranet, wireless networking, cellular networks, dial up). The nature of this structure

200 Mason *Electronic Evidence* (2010) 31
201 Mason *Electronic Evidence* (2010) 31

makes anything done on a device and connected to a network easily capable of being distributed and duplicated, so that the same item of electronic data can reside almost anywhere. This obviously has legal implications in that it will affect how a criminal investigation is conducted and how much effort will be required from a party to civil proceedings to find relevant information for discovery or disclosure.[202]

This is a vast challenge, particularly for large organisations, to locate relevant documents in electronic format, especially email correspondence, stored on back-up tapes or elsewhere. This was the case in two American cases. In *Zubulake v UBS Warburg LLC*,[203] as part of the preliminary hearings, UBS was ordered to produce all relevant emails that existed on optical disks, its servers, and certain back-up tapes. UBS was under a legal duty to store emails in accordance with the Securities and Exchange Commission Regulations. In this instance, two storage methods were used, back-up tapes for the purpose of disaster recovery and optical disks, so that relevant emails could be found in three possible places, files in use by employees, emails archived on optical disks, and emails sent to and from a registered trader (excluding internal emails) that were stored on optical storage devices. 94 back-up tapes were identified as being relevant for the purposes of disclosure. The costs for restoring and searching the tapes amounted to US$ 11 524.63, plus the expenses relating to the time it took lawyers to review the emails bringing the total cost to US$ 19 003.43.

In the second case, *Coleman (Parent) Holdings, Inc v Morgan Stanley & Co Inc*,[204] a number of preliminary hearings took place to deal with the extent of the discovery of documents, in particular email communications. Coleman accused Morgan Stanley of failing to provide relevant emails when requested to do so. Coleman was successful in the first trial but on appeal the order was reversed. The court accepted the argument by Morgan Stanley of the problems encountered in its attempt to identify and produce the material requested; some back-up tapes were in locations that were not searched or in locations where they should not customarily be stored, the tapes were not clearly labelled as to their contents, and many of them were in a format different from other email back-up tapes.

---

202 Mason *Electronic Evidence* (2010) 41-42

203 217 F R D 309 (S D N Y 2003) and 216 F R D 280 (S D N Y)

204 Civil Action No. 06 CV 0882 (RCL) (DDC)

These examples show how difficult it is to identity relevant email communications. Given the distributed environment nature there is a strong likelihood that one will face practical problems in determining materials required to be disclosed or discovered. It is, therefore, important to prevent the destruction of evidence and establish the place where the evidence is likely to be before starting to search sources to identify relevant documents. One should, therefore, locate back-up tapes on the premises, in off-site remote storage, on individual computers, servers, in archives, or a disaster recovery system. Storage media that need to be identified and located include tapes, disks, drives, USB sticks, iPods®, laptops, PCs, PDAs, mobile telephones, pagers, and audio systems (including voicemail), to name but a few.[205]

2.3.2.6 Deletion and destruction of electronic evidence

In contrast to a physical object or a paper document which will be destroyed effectively by placing it into a paper shredder, by setting it on fire, or by using other destructive means to dispose of information, it is relatively difficult to do away with an electronic document. Despite a user's intention when clicking on the "delete" icon on a computer, the electronic document tends to remain on the computer hard drive and is capable of being retrieved, sometimes even if it is overwritten. It is important to understand the process of how electronic documents are stored on a computer or other digital devices to grasp the deleting process more effectively. When saved on a computer, documents, files, and programs are written to the hard disk drive in a number of places. The data is written randomly, rather than sequentially or chronologically, or in any other logical order. The computer system determines the best way and best place to store files on a hard drive to optimise the data retrieval process, which is generally instructed by the computer's central processing unit (CPU).[206] Then, the computer creates a sort of table of contents or index to locate data stored on the drive; this is commonly known as the File Allocation Table (FAT). When data is deleted, therefore, the file name is simply deleted from the FAT, and the space occupied by that file is marked as being available for overwriting. This means that the "deleted" data or portions of it will be recoverable by digital forensics experts unless and until new data is written to each and every sector that was previously occupied by that

[205] Mason *Electronic Evidence* (2010) 44; For a discussion on electronic discovery see Ch 5 par 5.3.2

[206] Lange & Nimsiger *Electronic Evidence and Discovery: What Every Lawyer Should Know* 2004 (hereafter referred to as Lange & Nimsiger *Electronic Evidence and Discovery: What Every Lawyer Should Know*) 5

file.[207] On occasions, parties have deleted, or intended to delete, files. In *United States v Triumph Capital Group, Inc*[208] the accused was alleged to have purchased a software program to purge his computer of incriminating evidence. Forensic tests were undertaken and revealed that relevant data had been deleted, and the files were recovered. In *L C Services v Brown*,[209] the operating system on Andrew Brown's computer had been changed or re-installed at the time that the claimants were pursuing disclosure of documents by the defendants, but the remains of email communications were recovered by a digital evidence specialist. In *Arista Records, LLC v Tschirhart*,[210] the defendant was successful in deleting files. In that instance, he used wiping software to expunge evidence of his having downloaded music files using iMesh® and BearShare® computer-to-computer software in defiance of a notice issued by a court to preserve such evidence.

2.3.2.7 Metadata

The term "metadata" refers to data providing information about one or more aspects of the data. In case of an electronic document, it is typically embedded information about the document not readily accessible after conversion of the native electronic document into an electronic image or paper document. It includes *inter alia*:

- the means of creation;
- the purpose;
- the time and date of creation, modification and sending of an email;
- the creator or author; and
- the location on a computer network of where the data was created.[211]

A digital image may, for example, include metadata that describe how large the picture is, the image resolution, and the time of creation. A text document's metadata may contain information about how long the document is, the author, the time the document was written, and a short summary of the document.

---

207 Lange & Nimsiger *Electronic Evidence and Discovery: What Every Lawyer Should Know* 6

208 211 F.R.D. 31 (D. Conn. 2002)

209 [2003] EWHC 3024 (QB) at [53] and [54], [2003] All ER (D) 239 (Dec)

210 2006 WL 2728927

211 Par 5(7) of English Practice Direction 31B

Metadata about a photograph will identify the owner, copyright and contact information, what camera created the file, along with exposure information, and descriptive information such as keywords about the photo. Metadata are written either by the camera, or the photographer, or the software after being downloaded to a computer.

Web pages include metadata in the form of meta-tags which describe the content of Web pages. Most search engines use these data when adding pages to their search index.

Metadata may be created automatically by a computer system or manually by a user. Elementary metadata captured by computers can include information about when a file was created, who created it, when it was updated, the file size, and the file extension. It should, however, be pointed out that some of the information contained in the metadata will not necessarily be accurate, for example the identity of the author of a document information since a person may create a document not from a new file but from a template or an old file deleting the majority of the old text, or a person might log on to a computer or system using the name of another person, or a person may use software installed and registered in another name on his own computer. The purported time of creation can also be false; this will be the case if the time on the computer was not accurate, for example on a laptop flown across time zones without being adjusted accordingly.[212]

Since most of the time metadata are created automatically by the computer without the knowledge of the user, they are, therefore, more difficult to alter, manipulate, or delete, and for this reason they constitute very useful information in the analysis of an electronic document.

The importance of metadata varies with applications. As a general rule, the more interactive the application is the more important metadata are in understanding the application's output. "At one end of the spectrum is a word processing application where the metadata is usually not critical to understanding the substance of the document. The information can be conveyed without the need for the metadata. At the other end of the spectrum is a database application where a database is a completely undifferentiated mass of tables of data. The metadata is the key to showing the relationships between the data; without such metadata, the tables of data would have little meaning. A spreadsheet application lies somewhere in the middle. While metadata is not as

[212] Mason *Electronic Evidence* (2010) 33

crucial to understand a spreadsheet as it is to a database application, a spreadsheet metadata may be necessary to understand the spreadsheet because the cells containing formulas, which arguably are metadata themselves, often display a value rather than the formula itself. To understand the formula, the user must be able to ascertain the formula within the cell."[213]

Metadata can be divided into three main categories:[214]

a. Descriptive metadata describes the content of a document. It will include information such as the title, key words, abstract, and the name of the alleged author.
b. Structural metadata deals with the structure of the document, in other words how a number of objects are brought together. It will include, for example: the "file identification" which identifies an individual chapter forming part of a book or report; the "file encoding" which allows the identification of codes used in relation to the file, including the data encoding standard used (for example ASCII), the method used to compress the file and the method of encryption, if used; the "file rendering" which allows one to determine how the file was created by providing information relating to the software application used, operating system and hardware dependencies; the "content structure" making it possible to define the structure of the content of the record, including a definition of the data set, the data dictionary, files relating to authority codes and the like; and the "source" which identifies the circumstances surrounding the capture of the data.
c. Administrative metadata provides information for the purpose of resource management. It can be divided into two subsets: rights management metadata; and preservation or record-keeping metadata.

Metadata can be accessed in different ways, one is to right click and select "properties" in the application that created the document, as in MS Word® for example, or by using software specifically designed for that purpose. In the same vein, metadata can be removed with specialist software.[215] This was the case in *Williams v Sprint/United Management Company*[216] where the

213 *Williams v Sprint/United Management Company* 230 F.R.D. 640 (D. Kan. 2005); 2005 WL 2401626 (D. Kan. 2005)
214 Mason *Electronic Evidence* (2010) 34-35
215 Mason *Electronic Evidence* (2010) 34-35
216 230 F.R.D. 640 (D. Kan. 2005); 2005 WL 2401626 (D. Kan. 2005)

defendant, before passing on documents in electronic format to the plaintiffs, modified the Excel® files by deleting, amongst others, metadata including the files' names, dates of modification, authors, history of revisions, printout dates, and other information. The defendant was ordered to produce the spreadsheets with the necessary metadata.[217]

2.4 Terms of technological nature

2.4.1 Electronic signature

2.4.1.1 Definitions

"Electronic signature" is a generic term which refers to different ways in which a communication can be signed electronically. It includes amongst other things the typing of one's name at the bottom of an email or an Internet order form; the display of one's email at the top of the message; a scanned signature; a digital signature; a written signature transformed into a format that can be electronically stored on a magnetic strip; and a biometric signature.[218]

The Electronic Transactions Act 1998 of Singapore defined "electronic signature" as any letters, characters, numbers, or other symbols in digital form attached to or logically associated with an electronic record and adopted with the intention of authenticating or approving the electronic record.[219] And "electronic record" was defined as meaning a record[220]generated, communicated, received, or stored by electronic, magnetic, optical, or other means in an information system or for transmission from one information system to another.[221]

It must be stressed that the Electronic Transactions Act 1998 was repealed by the Electronic Transactions Act 2010[222] which does not contain a definition of "electronic signature" but rather

---

217 For a discussion of that case see also the Note of Cucu, "The requirement for metadata production under *Williams v Sprint/United Management Co:* an unnecessary burden for litigants engaged in electronic discovery" 2007 *Cornell Law Review* 93 221

218 Simmons & Simmons *E-Commerce Law, Doing Business Online* 2001 (hereafter referred to as Simmons & Simmons *E-Commerce Law*) 27

219 S 2

220 Information inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form (S 2)

221 S 2

222 S 39(1)

of "electronic" which is defined as "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities."[223]

The English Electronic Communications Act 2000 defines "electronic signature" as anything in electronic form incorporated in, or otherwise logically associated with, any electronic communication or electronic data and purported to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.[224]

The European Directive on electronic signatures defines "electronic signature" as data in electronic form which are attached to, or logically associated with, other electronic data and which serve as a method of authentication.[225]

In terms of the UNCITRAL Model Law on Electronic Signatures, an electronic signature means data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.[226]

Last, but not the least, in South Africa the ECT Act defines "electronic signature" as any data attached to, incorporated in, or logically associated with other data which is intended by the user to serve as a signature.[227]

All these definitions are very similar in nature. They are discussed in more detail later.[228]

In addition, apart from the generic electronic signature, there exists another form of electronic signature considered to be more secure and reliable. This is commonly known as digital signature. It is defined below.

223 S 2(1)
224 S 7(2)
225 Art 2(1)
226 Art 2(a)
227 S 1
228 Ch 4 par 4.3

2.4.1.2 Digital signature

A digital signature is an electronic equivalent of a manual signature and fulfils the same functions.[229] It is a mathematical scheme for demonstrating the authenticity of a digital message or document. It gives a recipient reason to believe that an electronic message was created by a known sender who cannot deny sending it (authentication and non-repudiation) and that the message was not altered in transit (integrity).[230] Digital signatures are commonly used for software distribution, financial transactions, and they can be useful in the transfer of electronic evidence or exchange of legal documents occurring during the electronic justice process in order to detect forgery or tampering.

The Electronic Transactions Act 2010 of Singapore defines "digital signature" as an "electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person, having the initial untransformed electronic record and the signer's public key, can accurately determine:

(a) whether the transformation was created using the private key that corresponds to the signer's public key; and
(b) whether the initial record has been altered since the transformation was made."[231]

It further defines "asymmetric cryptosystem" as a system capable of generating a secure key pair, consisting of a private key for creating a digital signature and a public key to verify the digital signature.[232] Hash function" is defined as an "algorithm[233] mapping or translating one sequence of bits[234] into another, generally smaller, set (the hash result) such that:

229 Oei "Digital Signatures" in Smedinghof (ed) *Online Law, the SPA's Legal Guide to Doing Business on the Internet* 1996 (hereafter referred to as Oei "Digital Signatures")

230 Oei "Digital Signatures" 54-55

231 Par 1(1) of Third Schedule

232 Par 1(1) of Third Schedule

233 This is a detailed formula or set of rules for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. Harris & Crowley (ed.) *The Sedona Glossary: For E-Discovery and Digital Information Management (*3rd ed) 2010 (hereafter referred to as Harris & Crowley *The Sedona Glossary: For E-Discovery and Digital Information Management*) 3

234 A bit is a binary digit, the smaller unit of a computer data.A bit consists of either 0 or 1.There are eight bits in a byte which is the basic measurement of most computer data. Although characters are stored in bytes, a few bytes are of little use for storing a large amount of data.Storage is, therefore, measured in larger increments of bytes (Kilobyte, Megabyte, Gigabyte, Terabyte, Petabyte, Exabyte, Zettabyte, Yottabyte,

(a) a record yields the same hash result every time the algorithm is executed using the same record as input;
(b) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm; and
(c) it is computationally infeasible that 2 records can be found that produce the same hash result using the algorithm."[235]

In terms of the English Electronic Communications Act 2000, an electronic signature incorporated in, or associated with, a particular electronic communication or particular electronic data is certified (digital signature) if a person (whether before or after making the communication) makes a statement confirming that,

(a) the signature,
(b) a means of producing, communicating, or verifying the signature, or
(c) a procedure applied to the signature,

is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.[236]

The term "digital signature" is not specifically mentioned in the UNCITRAL Model Law on Electronic Signatures. A closer look, however, reveals that insight can be gained from the definition of a reliable signature for the purpose of satisfying the requirement in law of a signature of a person. For that purpose an electronic signature will be deemed reliable if:

(a) the signature creation data are, within the context in which they are used, linked to the signatory and no other person;
(b) the signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(c) any alteration to the electronic signature, made after the time of signing is detectable; and,

---

Brontobyte and Geopbyte). Harris & Crowley *The Sedona Glossary: For E-Discovery and Digital Information Management* 3 7

235 Par 1(1) of Third Schedule

236 S 7(3)

(d) where the purpose of the legal requirement for a signature is to provide assurance of integrity, any alteration made after the time of signing is detectable.[237]

The equivalent for a digital signature used by the Directive on Electronic Signatures is an "advanced electronic signature" which is defined as an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;
(b) it is capable of identifying the signatory;
(c) it is created using means that the signatory can maintain under his sole control; and
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[238]

Similarly to the European Union, South Africa has adopted the term "advanced electronic signature" which is defined as an electronic signature which results from a process which has been accredited by the Accreditation Authority as provided for in section 37 of the ECT Act.[239]

The Accreditation Authority may accredit authentication products and services in support of an advanced electronic signature if he or she 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 the user;
(c) is created using means that can be maintained under the sole control of that user;
(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; and
(e) is based on the face-to-face identification of the user.[240]

In terms of the ECT Act authentication products and services refer to products or services designed to identify the holder of an electronic signature to other persons.[241] Among those products and services, one can cite cryptography products and cryptography services.

237 Art 6(3)
238 Art 2(2)
239 S 1 of the ECT Act
240 S 38(1)

"Cryptography[242] product" is defined as any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring:

(a) that such data can be accessed only by relevant persons;
(b) the authenticity of the data;
(c) the integrity of the data; or
(d) that the source of the data can be correctly ascertained.[243]

"Cryptography service", on the other hand, is defined as any service which is provided to the sender, or a recipient of a data message, or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring:

(a) that such data or data message can be accessed or can be put into an intelligible form only by certain persons;
(b) that the authenticity or integrity of such data or data message is capable of being ascertained;
(c) the integrity of the data or data message; or
(d) that the source of the data or data message can be correctly ascertained.[244]

Examples of cryptographic techniques include the Public-Key Infrastructure. A Public-Key Infrastructure is a system for the creation, storage, and distribution of digital certificates (also known as public key certificates or identity certificates) which are electronic documents that use digital signatures to bind a public key with an identity. The digital certificate can be used to verify that a particular public key belongs to an individual or a certain entity.[245]

Authentication products can also rely on biometrics. Biometric authentication refers to the identification of humans by their characteristics or traits. It is used in a computer system as a

---

241 S1

242 Cryptography is the science of encryption, which is the process of converting ordinary information (plaintext) into unintelligible gibberish (ciphertext). Decryption is the reverse operation; it transforms unintelligible ciphertext into plaintext. A cipher is a pair of algorithms that create the encryption and the reversing decryption - Schellekens *Electronic Signatures, Authentication Technology from a Legal Perspective* 2004 (hereafter referred to as Schellekens *Electronic Signatures, Authentication Technology from a Legal Perspective*) 3

243 S 1 ECT Act

244 S 1 ECT Act

245 Oei "Digital Signatures" 52

form of identification and access control. These characteristics include, amongst other things, a human subject's unique physiological and or behavioural features, such as fingerprints, iris recognition, or hand and palm geometry which are reduced to digital format and make it possible to authenticate an individual.[246]

2.4.2 E-justice

E-justice has a broad definition, including, in general, the use of information and communications technologies in the field of justice. Its primary objective is to help justice to be administered more effectively for the benefit of citizens through the use of electronic means. These technologies facilitate access to justice, help to rationalise and simplify judicial proceedings, and reduce procedural deadlines and operating costs in litigation.

E-justice implies the use of a wide variety of technological instruments such as computers, televisions, telephones, faxes, enabling a range of applications ranging from case management systems to video conferences or Internet and Web-based applications such as e-justice portals and other social network applications, to name but a few.

Although this thesis will attempt to cover as many technologies and applications pertaining to e-justice as possible, a strong emphasis will be put on those relevant in the communication and exchange of data between stakeholders involved in the administration of justice, namely attorneys, courts, and citizens, as well as technologies facilitating the handling and presentation of electronic evidence.

2.5 Conclusion

The main purpose of this chapter has been to provide an introduction to basic concepts and terminology fundamental to an understanding of the subject which will be encountered throughout this research. Terms have been defined following an approach differentiating between, at the one end of the spectrum, terms of legal nature, and, at the other end of the spectrum, terms of technological nature and, in the middle, hybrid terms, in other words terms which were difficult to categorise. It must be noted, however, that the demarcation is not always

[246] See also Mason *Electronic Signatures in Law* (3rd ed) 2012 (hereafter referred to as Mason *Electronic Signatures in Law* (2012)) 269-272

clearly evident. It is, nonetheless, useful in organising the chapter in a clear, ordered, and logical manner. The chapter did not, furthermore, deal with terminology exhaustively, meaning that certain terms will be explored and explained if necessary when they are encountered. Having said that, the most salient terms have been dealt with, and, therefore, one can to move to the next chapter dealing with the admissibility and weight of electronic evidence.

CHAPTER 3 ADMISSIBILITY AND WEIGHT OF ELECTRONIC EVIDENCE

3.1 Introduction

This chapter discusses the fundamental issues around the admissibility and weight of electronic evidence. The importance of this type of evidence cannot be underestimated in the electronic age in which we are living, where every institution of government, business, and industry, and even the family, interact and communicate electronically. This creates a vast amount of information generated and stored electronically. In the light of this background, it is important to investigate how the question of the admissibility and the weight of electronic evidence is addressed in the selected jurisdictions. Indeed this type of evidence has value only if it can be admissible in court and given due legal weight. This chapter is divided into three main sections, preceded by an introduction and is summed up by a conclusion. The first section deals with the admissibility and weight of electronic evidence as real evidence with an emphasis on both the English and the South African jurisdiction. The second section focuses on the interaction between the admissibility and weight of electronic evidence and the hearsay rule. Finally, the last section discusses the question of admissibility and weight of electronic evidence in relation to documentary evidence.

3.2 Admissibility and weight of electronic evidence as real evidence

As noted in the previous chapter, the concept of "admissibility of evidence" refers to information that can properly be put before the court,[247] while "weight of evidence" refers to the persuasiveness evidence can have once admitted to satisfy the court as to the *facta probanda*.[248] In most common law jurisdictions, the basis for admitting evidence is its relevance. An overview of the state of the law regarding the admissibility and weight of electronic evidence as real evidence is undertaken comparatively in England and South Africa in what follows.

247 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 20

248 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 20; *facta probanda* are facts in issue in a case, in other words, facts that a party is required to prove to win the case (Schwikkard & Van der Merwe *Principles of Evidence* (2009) 17)

3.2.1 England

The admissibility of electronic evidence as real evidence is analysed in the following lines by differentiating between electronic evidence in analogue format and electronic evidence in digital format.

3.2.1.1 Electronic evidence in analogue format

In respect of this category, Stephen Mason[249] reports that the first time the admissibility of that type of evidence was raised in England was in *R v Maqsud Ali, R v Hussain*.[250] This case concerned itself with the admissibility of an analogue tape recording. Counsel for the appellants argued that a tape recording was inadmissible in law. In the court judgment, Marshall J declared the following: that the time had come for the court to express its views on a matter expected to gain in importance as time passes. In expressing its views, the court first highlighted the status of photographs which have been admissible in evidence for years as long as they are relevant and they originate from negatives that are untouched. Then, the court pointed out that evidence of things, which could not be picked up by the naked eye, have also been admitted, such things include those visible only through telescopes or binoculars. Finally noting that now devices exist that allow picking up, transmitting and recording conversations, the court saw no difference in principle between a tape recording and a photograph. It stressed, however, that this does not mean that tape recordings are admissible irrespective of the circumstances. In spite of this last statement the court strongly believed that it would be wrong to deny the law of evidence advantages brought about by new techniques and devices as long as the accuracy of the recording can be ascertained and the voices recorded properly identified; and the evidence is relevant, that is admissible. The court was thus satisfied that a tape recording is admissible in evidence.[251]

The court, as shown in this passage, warned against the risk of rejecting valuable evidence merely on the grounds that it was the output of new techniques or new devices. It places tape recordings on a par with photographs which have been admissible for years. It also sets the

249 Mason *Electronic Evidence* (2010) 302

250 [1966] 1 QB 688, [1965] 2 All ER 464, [1965] 3 WLR 229, CA

251 *R v Maqsud Ali, R v Hussain* [1966] 1 QB 688, [1965] 2 All ER 464, [1965] 3 WLR 229, CA at 701[B]-[E]

conditions for the admissibility of tape recordings, that is, the record must be relevant, there must be proof of the accuracy of the recording, and the voices recorded must be clearly identifiable.

The admissibility of electronic evidence as real evidence was also considered in *The Statue of Liberty*.[252] In this case, a collision occurred in the Thames estuary between two ships. The estuary was continuously monitored by radar, and a film of radar echoes was made wholly automatically. It was argued that the film was hearsay and inadmissible in evidence. The court correctly rejected this submission and accepted the film as real evidence.[253] The court held that "if tape recordings are admissible, it seems equally a photograph of radar reception is admissible – as, indeed, any other type of photograph."[254] It continued by saying that "it would be an absurd distinction that a photograph should be admissible if the camera were operated manually by a photographer, but not if it were operated by a trip or clock mechanism."[255] In the same vein, when evidence of weather conditions is at the issue, the court held that "the law would affront common sense if it were to say that those could be proved by a person who looked at the barometer from time to time, but not by producing a barograph record."[256] This is also applicable to other types of dial recordings it was noted. To support its view, the court also pointed out that cards from clocking-in and out machines are frequently admitted in accident cases.[257] Commenting on this case, Tapper supported the view of the court by stating that, contrary to the situation where a human being would have been monitoring the estuary and recording his observation into a tape recorder who must be available to testify for the recording to be admissible in evidence, there is not such a need when the machine is operating in a purely mechanical function. Evidence produced in that instance should qualify as real evidence and, therefore, can be used circumstantially to prove what it appears to assert. He went on to say that where machines have replaced human beings, it makes no sense to insist upon rules devised to cater for human beings, but, rather, as expressed in this case, to accept that the law is bound to take cognisance of the fact that mechanical means replace human effort.[258]

252 1968 1 WLR 739
253 *The Statue of Liberty* 1968 1 WLR 739 at 739 C
254 *The Statue of Liberty* 1968 1 WLR 739 at 740 E
255 *The Statue of Liberty* 1968 1 WLR 739 at 740 F
256 *The Statue of Liberty* 1968 1 WLR 739 at 740 F
257 *The Statue of Liberty* 1968 1 WLR 739 at 740 G
258 Tapper *Computer Law* (4th ed) 1989 (hereafter referred to as Tapper *Computer Law*) 374

The precedent of *The Statue of Liberty*[259] case could have also been relevant in *R v Pettigrew*[260] had it been considered. In that case, a printout from the Bank of England's computer was adduced by the prosecution to prove that some banknotes found in the possession of the accused were part of a particular consignment despatched by the Bank. The printout listed the numbers of the first note and the last note in the consignment, and the numbers of notes within the numerical sequence not included in the consignment. In consequence, if numbers of the relevant notes falling between the first number and the last number did not coincide with the numbers listed as not included, it would mean that these numbers were part of the consignment. The system worked as follows, an operator placed a sequence of printed notes into the machine and entered the number of the first note and the nominal amount to be included in the bundle. The machine would then check the printing of the notes and reject any defective notes until it reached the nominal amount required for the bundle. After that the machine would print out two automatically compiled records, a list of numbers of rejected notes, and the number of the last note in the bundle. Counsel for the prosecution unwisely argued that the printout was admissible under the provisions of the Criminal Evidence Act 1965 as a business record. This Act, however, required, in terms of section 1(1)(a), that for such record to be admissible as evidence of the truth of any matter dealt with in it, any requisite information should be supplied by those who have, or may reasonably be supposed to have, personal knowledge of the those matters. The Court of Appeal held that the operator did not have personal knowledge of the numbers of the rejected notes since they were compiled automatically by the computer. As noted by Colin Tapper, this conclusion is an accurate and perfect application of the hearsay rule. It is, however, regrettable that the use of the printout as real evidence as in *The Statue of Liberty* case was not considered. Had it been considered, the issue would have moved to ascertain whether or not the machine was working correctly at the appropriate time. This would have required testimony from the manufacturers of the machine, the programmers, and those who tested it.[261]

Unlike *R v Pettigrew*,[262] *The Statue of Liberty*'s approach was followed in *R v Wood*[263] and in *Castle v Cross*.[264] In the former case, it was necessary to ascertain the precise chemical

259 1968 1 WLR 739
260 1980 71 Cr. App. R. 39, C.A
261 Tapper *Computer Law* 374-375.See also Mason *Electronic Evidence* (2010) 303-304
262 1980 71 Cr. App. R. 39, C.A
263 1983 76 Cr. App. Rep. 110, C.A

composition of some ingots of metal in order to establish whether they were part of a stolen consignment. In relation to two of the metals, one metal was analysed by means of an X-ray spectrometer and the other by a neutron transmission monitor. The output of these machines required extensive and laborious calculation to reveal the amount of metals present in the ingots. This was done by a computer and the computer output was adduced in evidence and admitted as real evidence. The court explained that the computer was being used only as a calculator, and did not purport to reproduce any human assertion which had been entered into it. It further held that there was no more room for objecting to the output of computer as hearsay than there was for objecting to that of the spectrometer or transmission monitor upon which the computation was based. In this instance, the programmer gave evidence as to the programming of the machine, and the operator gave evidence as to its operation. Interestingly, the counsel for the defence admitted that his objection was purely technical, and that the computer analysis was correct. As submitted by Colin Trapper, it would be scandalous if the use of a computer should lead to the exclusion of such perfectly reliable evidence.[265]

In *Castle v Cross*,[266] a printout of a breath-testing machine, the Intoximeter 3000, was tendered in evidence. Rejected by the magistrate's court on the basis that it was hearsay, it was later accepted as real evidence by the Divisional Court which held that the printout was the product of a mechanical device which falls into the category of real evidence.

Video tapes and security camera evidence are other examples of electronic evidence falling under the umbrella of real evidence. As noted by Stephen Mason, evidence of images from security cameras can be very helpful in the identification of the perpetrators of crimes. The enhancement of these images coupled with the use of sophisticated techniques, such as facial mapping, can help to identify parties to an offence.[267] According to Stephen Mason, such evidence has been admitted in English courts, mainly in criminal cases.[268]

---

264 1985 1 All E.R. 87, Q.B.D

265 Tapper *Computer Law* 376

266 1985 1 All E.R. 87, Q.B.D

267 Mason *Electronic Evidence* (2010) 345

268 The following is a non-exhaustive list of relevant cases given by Stephen Mason: *R v McShane* 1977 66 Cr App Rep 97; *R v Fowden and White* 1982 Crim LR 588, CA; *R v Grimer* 1982 Crim LR 674, 126 Sol Jo 641, CA; *R v Williams* 1984 1 WLR 971; *R v Stockwell* 1993 97 Cr App Rep 260, CA; *R v Clarke* 1995 2 Cr App Rep 425;

Commenting on the technique of facial mapping, Stephen Mason advises that careful attention to the manner in which the technique has been used by an expert witness be given before admitting the evidence. He recommends, therefore, taking into account the following conclusions by Gregory[269] in relation to the use of enhanced digital imagery:

(a) The original image needs to be properly authenticated;
(b) The original image must remain intact to enable the original to be compared with the enhanced version;
(c) The original image should be preserved in such a way that its integrity cannot be impugned;
(d) The process of enhancement should be fully documented;
(e) The process of enhancement should be carried out in such a way that the process can be repeated by the other party; and
(f) The enhanced images should be preserved in such a way that prevents it from being manipulated and thereby preserves its integrity.

These conclusions are in line with the view expressed by the court in *R v Clarke*,[270] where it was held that the evidence should be scrutinised, because such evidence could be flawed, in the same way that fingerprint evidence can be flawed. This submission is particularly relevant, especially in situations where both the technology and techniques used by the experts and the evidence of police differ. This was the case in relation to voice recognition in *R v Flynn and St John*.[271] The prosecution sought, in this case, to identify alleged conspirators of robbery through voice recognition techniques. A listening and transmitting device was secretly fitted in the car used by the conspirators. The prosecution relied on the evidence of four police officers, who claimed to have recognised the voices of the appellants on the covert recording, and on the written statement of an expert witness, an independent forensic consultant. At trial, counsel for the appellants objected to the introduction of the voice recognition evidence and the transcripts produced by the police. Both types of evidence were, nevertheless, ruled admissible. This ruling was challenged. The appeal court noted the controversial nature of the admission of voice recognition evidence and made some general comments. It distinguished between, at the one end of the spectrum,

---

R v Peach 1995 2 Cr App Resp 333, 159 JP 412; *R v Feltis (Jeremy)* 1996 EWCA Crim 776; *R v Hookway* 1999 Crim LR 750; *R v Briddick* 2001 EWCA Crim 973;R *v Loveridge* 2001 EWCA Crim 973

269 Gregory *Modern Visual Evidence* 8.04 [4] quoted by Mason *Electronic Evidence* (2010) 345-346

270 1995 2 Cr App Rep 425

271 2008 EWCA Crim 970

expert evidence including auditory analysis and secondary acoustic or spectrographic analysis, and, at the other end of the spectrum, what is described by the experts in this case as lay listener evidence. The latter requires that the witness possesses some special knowledge of the suspect that enables him or her to recognise the suspect's voice. The court further held, based on the expert evidence produced in this case, that identification of a suspect by voice recognition is more difficult than it is by visual identification and that identification by voice recognition is likely to be more reliable when carried out by experts using acoustic and spectrographic techniques as well as sophisticated auditory techniques, rather than by lay listener identification. The court also pointed out the fact that the officers had limited opportunity to acquire familiarity with the appellants' voices and also the poor quality of the covert recording; it, therefore, upheld the appeal.[272]

Apart from the above examples where electronic evidence in analogue format is accepted as real evidence, there are also examples of electronic evidence in digital format accepted as real evidence. This situation is discussed below.

3.2.1.2 Electronic evidence in digital format

Electronic evidence in digital format can also be accepted as real evidence. This was the case in *R v Governor of Brixton Prison, ex p Levin*.[273] This was an appeal against extradition where Vladmir Levin was alleged to have used a computer terminal in St Petersburg to gain unauthorised access to a Citibank terminal in Parsipanny, New Jersey to make 40 fraudulent transfers of funds to the value of US$ 10.7m from the accounts of clients to accounts controlled by him or his associates. Printouts of screen displays of the historical records of computer payments transactions were adduced in evidence and were admitted as real evidence. The court held that the printouts were produced to prove that such transfers took place and that their evidential status was not different from that of a photocopy of a forged cheque.[274] Stephen Mason concurred with the court's view and went on to say that it is now clear that printouts are a form of real evidence although the truth of their content is subject to further testimony. He,

---

272 Mason *Electronic Evidence* (2010) 346-348

273 1997 AC 741

274 *R v Governor of Brixton Prison, ex p Levin* 1997 AC 741 at 746

therefore, recommended that proper testimonial foundations of digital evidence be presented to court to demonstrate the truth of the statement contained in the printout of the digital evidence.[275]

In *R v M (R),*[276] a printout by the complainant representing what she had read on the computer screen when she opened an email was accepted as real evidence. Kay LJ held that the printout might have been hearsay if she had not given oral evidence. But, since she did, she was entitled to produce a document to confirm in clear terms what she had seen. This is not different from a photograph depicting a scene described to the court by a witness. It is, however, not clear, notes Rosemary Pattenden, why this confirmation was permitted.[277]

In light of the situation in England where electronic evidence both in analogue and digital format is accepted as real evidence, it is right to have a look at the South African jurisdiction to determine the treatment reserved for both types of electronic evidence. The review follows below.

3.2.2 South Africa

The discussion on the application of rules governing real evidence to electronic evidence in South Africa follows the same pattern as above. In other words, the first part deals with the application of these rules to electronic evidence in analogue format whereas the second part deals with their application to electronic evidence in digital format.

3.2.2.1 Electronic evidence in analogue format

Electronic evidence in analogue format or in the form of the output of an analogue device such as photographs, films, video films, or sound recordings may be admissible as real evidence in South Africa. The discussion below shows the divergent views relative to the legal position currently observed on this question.

---

275 Mason *Electronic Evidence* (2010) 308

276 2003 EWCA Crim 3067

277 Pattenden "the rule against hearsay" in Malek (ed) *Phipson on Evidence* (16th ed) 2005 (hereafter referred to as Pattenden "the rule against hearsay") 790

In *R v Behrman*,[278] the admissibility of tape recordings was considered. This was an appeal from a conviction in a magistrate's court. The appellant was convicted for contravening section 2 of Act 4 of 1908, and the prosecution relied on *inter alia*: (1) a recording of a conversation between the accused and Captain R.J. Pretorius relating to the attempt by the former to corrupt the latter; and (2) the transcripts of this recording. The transcripts were made by two Head Constables by listening to the recording, and copies were produced, but it was admitted that the task was very difficult and that, at times, voices were not audible at all. Parts were indistinct too, and certain words wrongfully identified. The court *a quo* found the playing of the tape unintelligible and requested the aid of two experts and "dubbings" or electro-transcribed copies were made in the form of discs. The discs were said to be identical to the original recording. Despite all the irregularities, the magistrate admitted the transcripts on "the common sense point of view" indicating that it was the best evidence available and that the court was not there to usurp the functions of witnesses but to decide on those witnesses. He, therefore, aligned to the position of the prosecution and overruled the defence's objection.

As noted by the learned presiding judge, Bresler, J, in appeal, this reasoning is not very compelling. The magistrate failed to address this issue substantially. In this author's view, he should have adopted the approach followed in the above-discussed English case of *R v Flynn and St John*.[279] Indeed the poor quality of the tape recordings or dubbings, and the inaccurate transcripts, make this evidence unreliable and, therefore, not authentic. Since, to be admissible, real evidence must be authentic this evidence should have not been admitted. As noted by Zeffert and Paizes, however, not every flaw in a recording is fatal to authenticity, only a flaw giving rise to the reasonable possibility of a distorted version of the reality.[280] Further commenting on the admissibility of evidence of the present nature, Bresler, J recommended that correspondence be maintained between the original and the "dubs" and between the various transcripts of the latter. Undeniably this was not the case in this instance where the defence was able to compile numerous omissions and inconsistencies in respect of the transcripts. He proceeded to say that where efforts to elicit the contents of the original tape might leave some room for uncertainty, as in this case, there should be evidence to identify all the voices. In conclusion, the presiding judge

278 1957 1 SA 433 (T)
279 2008 EWCA Crim 970
280 Zeffertt & Paizes *The SA Law of Evidence* 859

held the transcripts to be inadmissible. He, nevertheless, confirmed the conviction and sentence because of the overwhelming nature of the evidence of guilt.

Hiemstra A.J., while concurring with the conclusion of the presiding judge as to the conviction and the sentence, expressed a different view as far as the transcripts were concerned. His opinion was that the transcripts were correctly admitted. According to him, the dictaphone is a device useful for establishing the truth which can in no way violate the established rules of evidence if the procedure he suggests below is followed:

1. There must be proof that the recording tape could not have been tampered with and in fact contains the relevant conversation and no other.
2. The court need not listen and transcripts may be handed in provided that the tape is made available to the defence to enable it to challenge the accuracy of the transcript.
3. The number of transcripts is only relevant insofar as their reliability is challenged.
4. The voices need not be identified as long as they are kept strictly apart on the transcript and there is proof that no other voices could have been recorded than those of the people present at the conversation regarding which independent evidence is given. It should be permissible for the court to infer from the context who spoke the separate sentences.
5. No expertness is required for making the transcripts, beyond honesty, intelligence, and a good sense of hearing.[281]

Hiemstra AJ believed, therefore, that, if the procedure set out above is followed, the possibility of an injustice is negligible, and he was satisfied too that this procedure had been complied with in this case.

S v Singh and Another[282] is another appeal case from conviction in a magistrate's court where the appellants were charged and convicted for contravening section 29(1) of the Black Administration Act 38 of 1927. Annexed to the charge was a schedule headed, "Transcript of the tape-recorded statements allegedly made at Kajee Hall on 21.3.1973." The schedule contained a transcript of speeches or addresses alleged to have been made by the appellants. In the trial court, it was submitted, on behalf of the appellants, that the quality of the tape-recordings was so poor that they should be discarded *in toto*. The appeal court considered it necessary to listen to the

281 *R v Behrman* 1957 1 SA 433 (T) at 439

282 1975 1 SA 330 (N)

tape recordings and did so in open Court. It was of the opinion that there was no justification for this submission since the quality of the recordings was good enough to hear what the speakers were saying, and it held that the annexure to the charge accorded with the content of the recording. Dealing with the admissibility of the tape recordings, the magistrate, on the authority of Hoffman,[283] and cases cited there, held that the real evidence is the tape itself, and that the court and the parties could check its accuracy on the spot. He also mentioned the Scottish case of *Hopes v H.M. Advocate:*[284]

> Where the typist prepared a transcript of a barely intelligible tape-recording; by hearing the recording played many times the witness had acquired the ability to identify it with greater accuracy than a person listening to it for the first time. Her opinion was accordingly held to be admissible although one would not have regarded her as an expert.

It seems, therefore, that the transcript, although secondary evidence, as long as it is evidence of the original recording will be admitted if it is not possible or convenient to play the tapes in court. In addition there must be sufficient evidence to identify the speakers.

At the hearing of the appeal, submission was made on behalf of the appellants that a reasonable possibility existed that the tapes had been tampered with. Responding to this submission, the presiding judge highlighted the important nature of the matter by reminding, as pointed out by *Hoffman, supra*, some difficulties the use of tape recordings had given rise to, for example, the fact that tapes can be easily edited or altered. He then referred to *R v Stevenson and Others*,[285] where the issue of a possible fabrication was raised and test rules were laid down:

1. Before the Court would admit them in evidence [tape recordings] it had to be established that they were the original recordings; if sufficient doubt was raised by the defence to indicate that it was likely that they were not the originals, and so not the primary and best evidence, the Court had no alternative but to reject them.
2. Accordingly if there is evidence that some interference with the tape recordings might have taken place they are not admissible in evidence.

283 *SA Law of Evidence* 2nd ed 288
284 1960 SC (J) 106
285 1971 1 All ER 678

The first point appears to be too stringent since it ignores exceptions to the best evidence general rule allowing, under certain circumstances, admission of a copy of the original.

On point 2 above, Leon J. preferred the following formulation. "[I]f on the evidence as a whole there exists a reasonable possibility of such interference, the tape recordings would not be admissible in evidence".

After perusing evidence led on behalf of the State, Leon J. was satisfied that there was not a reasonable possibility that either of the tapes had been tampered with.

Another case worth mentioning is *S v W.*[286] The appellant was convicted in this instance for an indecent exhibition in contravention of section 19(b) of the Sexual Offences Act 23 of 1957 during a dance performance. The State relied upon video films and photographs taken during the performance. In appeal, submission was made on behalf of the appellant that the trial court had erred in receiving this evidence as it allegedly distorted the presentation since on occasions one photographer had used flash lights, and another a zoom lens. The appeal court disagreed with this submission and held that, even if the objection was valid, it was relevant only for the weight to attach to the evidence and not for its admissibility. It distinguished this instance from cases where a photographic image is created through lighting and focusing techniques, which is false and misleading, and where high potential prejudice to the accused justifies exclusion of evidence. In this case, the photographs and film were found by the trial court to be true representations of the objects and persons which they purported to represent, and, therefore, qualified as real evidence. The appeal court was satisfied on the basis of the evidence that the flash light and zoom lens were used as a means of clarification and emphasis and not of distortion. In addition, the court raised the risk of measuring up a photograph or a film against some theoretical and unattainable standards of perfection. And, therefore, the appeal court correctly endorsed the trial court's finding as to the admissibility of the evidence.

The evidence in argument in the murder and public violence case of *S v Mpumlo and Others*[287] was a video film portraying certain events relating to disturbances in a certain township in the Eastern Cape. A copy of the video film was tendered in evidence. The argument turned around

[286] 1975 3 SA 841 (T)
[287] 1986 3 SA 485

the nature of the video film; was it real evidence or documentary evidence? The State's view was that it was real evidence and, therefore, could not be subject to restrictions applicable to the proof of documents tendered in evidence. On behalf of the accused, Mr Poswa argued, first, for a total inadmissibility of the video film and, alternatively, accepted that the video film could qualify as a document, in the same way as a photograph qualifies, and, therefore, it should be subject to proof of authenticity and to the best evidence rule.

For the purpose of this section, the discussion is limited to the consideration of the video film as real evidence as its admissibility under documentary evidence will be considered at a later stage. The court, without any doubt, found in this case that the video film, like a tape recording, was real evidence, distinct from documentary evidence, and admissible in evidence provided it is relevant and that dispute as to its authenticity or interpretation is addressed.

S v Baleka and Others[288] goes further than *S v Mpumlo and Others*.[289] Objection was raised by the defence in that case to the admission of certain tape recordings as evidence in a criminal trial. The audio magnetic tape recordings fell into two categories. Seven tapes of unknown origin purported to reflect the proceedings at the conference and national launch of the UDF on 20 August 1983. Faults and peculiarities were identified in these tape recordings and reflected in the transcripts; they did not, however, render the speeches and rest of the proceedings unintelligible. The second category was tape recordings made clandestinely by the police using either a source sent into the meeting with a microphone and radio transmitter or a secret microphone installed beforehand. So-called technical problems were identified with regard to the second category. According to the expert witness who testified on behalf of the State, this was a normal situation for recordings in the field with normal equipment and often old tapes.

Two approaches were in opposition. The defence argued that the approach in *S v Singh and Another*,[290] as confirmed in *S v Ramgobin and Others*,[291] should be followed, whereas the State rested its case on the judgment given by Van Dijkhorst J, on 3 June 1983 on the admissibility of

---

288 1986 4 SA 1005 (T);De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" 567

289 1986 3 SA 485

290 1975 1 SA 330 (N)

291 1986 4 SA 117 (N) at 32

twelve video recordings. *S v Singh and Another*,[292] as already mentioned, established a two-pronged test for the admissibility of tape recordings; that is, the recording must be the original, and it must not have been interfered with in any way. The Judge President in the *Ramgobin*[293] case supported that test and held further that, for the tapes to be admissible, the State must prove beyond reasonable doubt:

(1) that the recordings before Court related to the meetings and conversations alleged in the indictment;
(2) by way of testimony of a witness who saw and heard the events allegedly recorded, that the recording accurately reflects those events; and
(3) that the tapes are the original recordings and have not been interfered with in any way, whether by mistake or otherwise, since the original recordings were made.[294]

The judge president adopted this strong view because he believed that tape recordings can be altered (and materially altered) in such a way that even experts cannot detect the alteration and that, therefore, they are dangerous from an evidential point of view unless precautions in the form of the above are taken.

Van Dijkhorst J., considering *S v Ramgobin and Others*,[295] objected and retorted by stating that *viva voce* evidence may be inherently dangerous, and yet it would be absurd to refuse to hear such evidence because the witness might turn out to be a liar. While recognising that a witness can easily be subjected to cross-examination, he, nevertheless, remarked that the accused does not stand helplessly tied to the stake of a tape recording since the evidence of the tape recording can be gainsaid by calling the speakers themselves or members of the audience to cast doubt on its authenticity and veracity. Zeffertt and Paizes opposed this view because, in their mind, it does not take into account the nature and the magnitude of the dangers. According to them, the accused, in spite of the possibility that he has to lead evidence in rebuttal, does still have his hands tied to the stake by being deprived of the most effective safeguard against abuse, the opportunity to cross-examine the witnesses of a party claiming the correctness of the recording

292 1975 1 SA 330 (N)
293 1986 4 SA 117 (N)
294 *S v Baleka and Others* 1986 4 SA 1005 (T) at 1023
295 1986 4 SA 117 (N)

before it is received.[296] In addition they advise a court, when dealing with dangerous evidence such as video tapes, to build a shielding and protective wall around those who may potentially suffer prejudice and not weaken their defences because of academic and impractical considerations, although they might be sound in abstract theory.[297]

Van Dijkhorst J was, nonetheless, of the view that the approach advocated in the *Ramgobin*[298] case could lead to the unacceptable situation that a court refuses to consider relevant evidence because it might be fabricated, where the correctness of that evidence is not even placed in issue in cross-examination but only its admissibility. This is exactly what could have happened in the present case if the above approach had been followed. And this, in spite of the fact, as pointed out by Van Dijkhorst J, that it was never put to any witness that the tapes were not a true reflection of the proceedings of the meeting that the tapes had been tampered with, or that they did not relate to the meetings mentioned. He concluded, therefore, that it would have led to a miscarriage of justice if he had had to exclude this evidence from consideration when all the evidence is weighed at the end of the case.

In respect of the requirement that the State must prove admissibility of tapes recordings beyond reasonable doubt, Van Dijkhorst J felt uncomfortable. He submitted that the documentary best evidence rule should not be extended to tape recordings, but conceded that, if he was wrong in that submission and that the best evidence rule had still to apply, then no more than a *prima facie* evidence of originality must be required at the admissibility stage. He agreed that the recordings must be shown to relate to the matters in issue, in other words, be relevant. But he disagreed that relevance needs to be proved beyond reasonable doubt. One needs simply to show *prima facie*, he remarked, that the material tendered has some probative value, for example, in that case, forging a link between the tape and the meeting to which it is said to relate. He further disagreed with the view that, before the tape recording is admissible, a witness must testify that he or she saw or heard the events allegedly recorded and that the recording accurately reflected those events. This approach, in his view, would relegate the evidence of tape and video recordings to a mere corroborative role and only to a limited extent. He did not, however, relieve the State of its duty to convince the Court of the reliability and accuracy of the tape recordings, but he failed to

296 Zeffertt & Paizes *The SA Law of Evidence* 855
297 Zeffertt & Paizes *The SA Law of Evidence* 855
298 1986 4 SA 117 (N)

understand why this has to be done before the final argument at the end of the case, and why proof of reliability and accuracy should be furnished only by *viva voce* evidence of a witness who saw and heard the events recorded, while circumstantial evidence might, in a given case, lead to the same conclusion. He did not see any objection either to the use of a copy. He noted, nevertheless, that the Court must be satisfied, before accepting a copy, that it accurately reflects what was recorded. He did not, moreover, support the view that tape recordings must not have been tampered with in any way, whether by mistake or otherwise. He rejected this submission on the basis that it is too widely stated as it removes from the Court the opportunity to determine whether the interference materially affected the recording as a whole. A sound approach would, therefore, be , according to him, to deal with each interference, stoppage, interruption, and fading of sound on its merits, determine whether it is material and whether it amounts to tampering, and then consider whether the State has proved that the whole tape or a particular portion of it on which it relies is reliable and accurate. Hefer JA in *S v Nieuwouldt*,[299] supported this view and submitted that, even if proof of authenticity were to be a prerequisite to the admissibility of a tape recording, the recording could not be rejected merely because it contains erasures, substitutions, or insertions. Exclusion of a recording on the sole basis of some accidental erasure would, therefore, be absurd Hefer JA pointed out. He warned, however, against the danger of accepting a recording against which there is a reasonable possibility that it reflects a distorted version of the reality. It is, therefore, important for the State to exclude the reasonable possibility of a false recording. In concluding, Van Dijkhorst J expressed his concern about the risk of requiring an unattainable standard of perfection before admitting tape recordings as it was held in respect of photographs or films in *S v W.*[300]

Another case worth mentioning in the discussion of electronic evidence as real evidence is *S v Fuhri*.[301] The appellant was convicted in this case for a contravention of section 85(4) of the Road Traffic Act 29 of 1989 in that he exceeded the speed limit. The only point in issue in the second appeal was whether a photograph of a speed camera was admissible in evidence to prove such speed limit excess without the testimony of a witness who could verify that it was a true image of what appeared in front of the camera lens at that specific moment. The court held that,

299 1990 4 SA 217 (A)
300 1975 3 SA 841 (T)
301 1994 2 SACR 829 (A)

where the relevant science or art had advanced to such a level of general acceptance, it was not necessary for human verification; the court could take judicial notice thereof.[302] It relied *inter alia* on the authority of *People v Doggett,*[303] which constitutes a good example of a photograph accepted for being probative in itself. The analogy of X-ray photographs is worth raising here, as it was held in that case that such type of evidence is admissible in evidence although there is no one who can testify from direct observation inside the body that they accurately represent what they purport to show. A contrary view would illogically limit the use of a device whose memory is undoubtedly more accurate and reliable than that of a human witness. It will, furthermore, exclude from evidence pictures taken with a telescopic lens or taken by a camera set to go off when a building's door is opened at night, to name but a few.

The court relied also on *R v Maqsud Ali, R v Hussain*[304] which held that it is wrong to deny the law of evidence of advantages to be gained by new techniques and devices.

Unlike *S v Fuhri,*[305] *S v Terblanche*[306] reached a different conclusion. The appellant was charged and convicted in the second case for contravention of alcohol limitation in a sample of blood in terms of Ord. 21 of 1966 (T). The instrument used to determine the alcohol content of his blood was a gas chromatograph which largely operated automatically. The appellant challenged the correctness of the instrument used. The court held that the correctness and effectiveness of the instruments had not been proved and indicated that evidence was necessary to explain the workings of the gas chromatograph. The conviction was, therefore, set aside.

Waste Products Utilisation v Wilkes (Biccari Interested Party)[307] was a case dealing with unlawful competition and breach of contract. In contention was the admissibility of certain tape recordings of telephone conversations between the first defendant, Wilkes, and a third party, on

302 *S v Fuhri* 1994 2 SACR 829 (A) at 830 b

303 83 Cal App 2d 405, 188 P2d 792.The evidence of a crime in this case was a photograph showing the defendants committing an act of sexual perversion. The photograph was adduced without the testimony of an eyewitness that it accurately depicted what it purported to show. Other evidence was, however, produced as to when, in point of time, the picture was taken, the place where it was taken, and to prove that the defendants were the persons displayed in the picture. In addition, evidence was given by a photographic expert that the picture was not a composite nor a fake but a true representation of a "pure" negative.

304 [1966] 1 QB 688, [1965] 2 All ER 464, [1965] 3 WLR 229, CA

305 1994 2 SACR 829 (A)

306 1981 1 SA 791 (T)

307 2003 2 SA 590

the one hand, and Wilkes and Bicardi, his attorney of record, on the other hand. The tape recordings and the transcripts of the telephone conversations, the authenticity of which was not put in issue, were held admissible as evidence despite their having been made in contravention of legislation and being unlawfully obtained.

Similar to electronic evidence in analogue format, electronic evidence in digital format can also be accepted as real evidence. Below is an outline of the legal position on the matter in South Africa.

3.2.2.2 Electronic evidence in digital format

A certain number of cases have dealt with such category in South Africa. In *Ex Parte Rosh*,[308] the Applicant brought an *ex parte* application for an order presuming the death of her husband ("Rosh"). The application was refused, and the Applicant appealed. The Court on appeal was requested to consider amongst other issues the admissibility of certain evidence in the form of computer printouts. These documents consisted of telephone company's computer printouts which were automatically generated for all calls made by its subscribers. The generation process was as follows: the computer was activated every time someone picked up the handset of the telephone; when a call was made, the computer automatically registered the time, date, length of call and number to which the call was made; eventually the computer-generated information was printed out; and the printout was made available to the relevant telephone subscribers. Relying upon, amongst others, the authority of *The Statue of Liberty*[309] and *S v Fuhri*[310] cases the Court admitted the computer printouts as real evidence as they came about automatically and not as a result of any input of information by a human being. It was satisfied that there was no room for dishonesty or human error. Indeed, a look at the evidence as a whole in this case demonstrates how reliable such electronic evidence was. It was, for instance, corroborated by carbon copies of telephone accounts recorded by telephone operators in the performance of their duties. Information contained in the printout and similar printouts had, moreover, been accepted by both the telephone company and its subscribers as being correct over a number of years. At the time this application took place the world was approaching the 21st century and it was experiencing

308 1998 1 All SA 319
309 1968 1 WLR 739
310 1994 2 SACR 829 (A)

the invention of many gadgets capable of recording material facts without human agency. This situation led courts in both South Africa and England to recognise that the evidence produced by such gadgets is *prima facie* accurate. This is in accord with reality and common experience.

Taking place in the new century, *S v Koralev*[311] dealt with the commission of indecent acts involving minors and the creation or possession of child pornography.[312] The point in issue was the admissibility of photographs and video images found on the first appellant's computer. It was contended that these photographs and video images were not admissible in evidence against the appellants because they did not satisfy the requirements of admissibility as set forth in *S v Ramgobin and Others*.[313] Considering this case with reference to the supporting case of *S v Singh and Another*[314] and the opposing cases of *S v Baleka and Others*[315] and *S v Fuhri,*[316] Gyanda J held that counsel for the appellants was right when declaring that:[317]

(a) Before the images in question could be admissible…there had to be some proof of their accuracy in the form of corroboration that the events depicted therein actually occurred.
(b) Corroboration in the sense required must be found in some independent source of evidence, which makes the evidence constituted by the images in the photographs and video recordings more acceptable in that it supports an aspect or aspects thereof.
(c) … the visual material can take centre stage, but requires a support cast which, in the evidence before the court *a quo*, is clearly missing.
(d) Captain De Beer's [the State's expert witness] evidence does not supply any corroboration in respect of the reliability and accuracy of the images allegedly found on the hard drive of the first appellant's computer.

With regard to point (d), Captain De Beer's evidence referred only to the absence of tampering during the transfer of images from the hard drive of the computer into the format it was placed before the court. From his evidence, however, it was clear that at least one image was in fact tampered with. Indeed the head in image No 1 bearing label 008JPEG did not sit well on the body of the person photographed. This was noticed by the court *a quo*. This prompted Gyanda J

311 2006 2 SACR 298
312 Contraventions of the Films and Publications Act 65 of 1996 and the Sexual Offences Act 23 of 1957
313 1986 4 SA 117 (N)
314 1975 1 SA 330 (N)
315 1986 4 SA 1005 (T)
316 1994 2 SACR 829 (A)
317 *S v Koralev* 2006 2 SACR 298 at 306-307

to say that since, in this day and age, it is easy with modern technology to tamper with images such as those relied on for the conviction in this case extreme caution must be applied to evidence in relation to such images. The acceptance of, and reliance on, such evidence must be subject to due and proper compliance with the above requirements.

S v Ndiki and others[318] is another case where the court considered whether electronic evidence in digital format or the output of it could constitute real evidence. The court was called upon to determine amongst other issues the nature of computer printouts adduced in evidence. Of the two categories of documents that were considered by the court, only one is relevant at this stage,[319] it concerns Exhibits D5 to D9. These documents were created without human intervention or assistance from data stored in the computer of which one or more functionaries had, nevertheless, personal knowledge. Van Zyl J, correctly held that such evidence constituted, in his view, real evidence because the computer, through its operating system, processed existing information, did calculations, and "created" additional information without human intervention, such as sequential numbers, the "creation" of cheques, and the recording of the identity of the person who operated the computer at any given time. He further rightly noted that the admissibility of such evidence is dependent upon the accuracy and the reliability of the computer, its operating systems and its processes, as opposed to the credibility of a natural person.

Electronic evidence in digital format has, furthermore, been dealt with in a more recent case, *S v Motata*.[320] In this case, the electronic evidence consisted of a disc containing audio recordings and photos captured by an I-mate Jam cellular phone and the transcripts of the audio recordings thereof. A trial-within-a-trial was ordered to determine the authenticity and the originality of the recordings. At the end of the trial-within-a-trial the recordings were ruled admissible. This interlocutory ruling was, however, still subject to reversal at the end of the trial if the defence could raise some issues surrounding the recordings. This did not happen as pointed out by the court in the following terms, "if the defence had challenged the authenticity of the recordings and the accuracy of the transcript, it was not done in a manner that was patently clear for all to see". The court thus accepted the recordings made from the laptop, although not original and best

318 2007 2 All SA 185 (Ck)

319 The other will be considered in the analysis of electronic evidence as documentary evidence

320 Unreported Case No: 63/968/07 Magistrate Court for the Regional Division of Gauteng, Johannesburg

evidence, as being recordings of the events they purported to represent free of manipulation and alteration. It held further that the recordings made sense and the sentences followed one another logically. It found, moreover, that the test in respect of authenticity and originality, in other words quality and potential to reflect the events as they relate to the incident, had been passed.

This series of cases on electronic evidence in digital format accepted as real evidence in South Africa concludes this section on the admissibility and weight of electronic evidence as real evidence analysed comparatively in England and South Africa. The review of cases in both jurisdictions shows that traditional rules on real evidence are able to accommodate electronic evidence generated automatically without the intervention of a human being. Instances exist, however, where electronic devices merely reproduce information which has been stored in them. Such electronic evidence triggers the operation of rules of hearsay evidence which are discussed below.

3.3 Admissibility and weight of electronic evidence and the hearsay rule

Hearsay, as defined in the previous chapter, aims at excluding assertions made by persons other than the testifying witnesses as evidence of the truth of any fact stated.[321] This section follows the same path as the previous one, that is, it discusses the correlation between hearsay evidence and electronic evidence in both analogue and digital format comparatively in England and South Africa.

3.3.1 England

3.3.3.1. Introduction

In common law, the admissibility of electronic evidence, such as photographs, computer printouts, video and audio recordings, depends, firstly, on whether the electronic evidence is derived from information fed into the machine by a person. If the electronic evidence was created without the intervention of a human mind, it is real evidence.[322] This was examined in

321 See Ch 2 par 2.2.4.4

322 Pattenden "The rule against hearsay" 789; See also the cases discussed previously such as the *Statue of Liberty* 1968 1 WLR 739 Case

the above section. If the electronic evidence is derived from information provided by human agency and is tendered to prove the truth of the information, it is hearsay.[323]

In England, the hearsay rule has been the subject of a lengthy reform process, including three major reforms for civil proceedings and four for criminal proceedings. The first general statutory overhaul of the rule was the Evidence Act 1938, an Act of restricted scope limited to civil proceedings and confined to documentary hearsay only. Then, the Civil Evidence Act 1968, which made a wide range of hearsay material admissible under certain procedural conditions, was enacted. The civil reform eventually culminated with the Civil Evidence Act 1995 whereby hearsay was, in effect, admissible in civil proceedings.[324] In criminal proceedings, initially there was the Criminal Evidence Act 1965, a reforming statute, and then major changes were brought about firstly by the Police and Criminal Evidence Act 1984, and, secondly, by the Criminal Justice Act 1988 whereby documentary evidence was admissible in criminal trials if the maker of the statement was unavailable or the document a business record. Finally, the Criminal Justice Act 2003 was passed and adopted a categorical approach by introducing categories of admissibility and a limited residual discretion to admit reliable hearsay that did not fit into any of the fixed exceptions.[325]

The following section gives an overview of the interaction between electronic evidence and the hearsay rule. It first reviews case law, especially cases developed in the previous section, that is, electronic evidence in analogue format and in digital format, and, then, it examines some of the above-mentioned statutes.

3.3.3.2 Electronic evidence case law and hearsay rule

In most of the cases mentioned in the previous section, where electronic evidence was accepted as real evidence, such admission depended upon successfully distinguishing such use from a hearsay use. In *The Statue of Liberty* case,[326] admission into evidence of a radar record was resisted on the basis that it was hearsay. As pointed out above, however, this record originated from a purely mechanical function of a machine and, therefore, constituted real evidence and not

323 Pattenden "The rule against hearsay" 790
324 Pattenden "The rule against hearsay" 811-812
325 Pattenden "The rule against hearsay" 811-812
326 1968 1 WLR 739

hearsay.[327] In contrast, as pointed out by Tapper, if a human being was watching the estuary and dictating his or her observations into a tape recorder, the tape recording would amount to hearsay if adduced to prove facts stated herein and would be inadmissible in evidence if no exception to the hearsay rule could be invoked.[328] In the present case, the court correctly rejected the contention that the radar film was hearsay.

R v Pettigrew[329] is a good example of the application of the hearsay rule in the context of electronic evidence. In this case the electronic evidence in contention was held to be hearsay because of the intervention of a human mind in its creation. Reliance for its admission on the statutory exception of a business record in terms of the Criminal Evidence Act 1965 was unsuccessful. This Act, in section 1(1)(a), required, for a business record to be admissible as the truth of any matter dealt with in the record, the person who supplied the information must have had personal knowledge of the matter. In this case, however, the operator did not have personal knowledge of the numbers of the notes that were rejected, because they were compiled automatically by the computer and should have qualified as real evidence.

In contrast, in *R v Wood*,[330] the court dismissed the contention that the computer output of calculations of output from an X-ray spectrometer and a neutron transmission monitor was hearsay by explaining that the computer was used only as a calculator and did not purport to reproduce any human assertion which had been entered into it. For the court, there was no more room to object to the output of the computer as hearsay than there was to object to that of the spectrometer or transmission monitor upon which the computation was based. It was, however, held that, if a computer printout is relied upon to prove what it states and what it states depends wholly or partly upon information supplied by a person, the printout is regarded in common law as hearsay.

Castle v Cross[331] is an interesting case in that a printout of a breath-testing machine, the Intoximeter 3000, was first rejected in evidence by the magistrate's court on the basis that it was

327 See Ch 3 par 3.2.1
328 Tapper *Computer Law* 374
329 1980 71 Cr. App. R. 39, C.A
330 1983 76 Cr. App. Rep. 110, C.A
331 1985 1 All E.R. 87, Q.B.D

hearsay, before being later accepted as real evidence by the Divisional Court which held that the printout was the product of a mechanical device which falls into the category of real evidence.

In respect of electronic evidence in digital format, Mason contends that such evidence is arguably hearsay.[332] To illustrate his view, he gives the example of a source code which conveys information and says it is equivalent to a declaration, as argued by Steven W. Teppler.[333] Mason reports Teppler's example of the United States Patent Office Number 5,619,571, which includes some uncompiled source code containing the following line of code with a comment:

> // Allocate a buffer to build the IFD (If this fails, we are F'd)

For Mason, this comment is an acknowledgment of the possibility of a shortcoming in the software code that has been written, not that the software code is, or will be, at fault.[334]

At this stage, it is imperative to dissect the source code in order to understand fully its exact nature. A source code is a code written in a high-level or assembly language which is converted into object code by a compiler, assembler, or interpreter.[335] In other words, it is any collection of computer instructions (possibly with comments) written using some human-readable computer language, usually as text. The source code is often transformed by a compiler program into low-level machine code understood by the computer. The machine code might then be stored for execution at a later time. Or an interpreter can be used to analyse and perform the outcomes of the source code program directly on the fly. Mason[336] refers to the article of Svein Willasen[337] who explains source code in the following terms:

---

332 Mason *Electronic Evidence* (2010) 335

333 Mason *Electronic Evidence* (2010) 335.Steven W. Teppler affirms that "despite the mostly orthogonal arguments in opposition, the undisputed nature of digital data itself compels the conclusion that all digital data is hearsay" Teppler, "Digital data as hearsay" 2009 *Digital Evidence and Electronic Signature Law Review* 6 (hereafter referred to as Teppler "Digital data as hearsay") 9

334 Mason *Electronic Evidence* (2010) 336

335 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/185182?redirectedFrom=source+code#eid21845861 (accessed on 13/08/13)

336 Mason *Electronic Evidence* (2010) 336

337 Willassen, "Line based hash analysis of source code infringement" 2009 *Digital Evidence and Electronic Signature Law Review* 6 (hereafter referred to as Willassen "Line based hash analysis of source code infringement") 210.

> Software is written as source code. The source code is written by the programmer, by entering instructions in an editor. The sequence of instructions defines the function of the program, such as taking input from the user, performing calculations, showing output on the screen and so on. This source code is then usually compiled into an executable program (an executable program causes a computer to perform tasks in accordance with the instructions), which is distributed to the users of the program. The source cannot be derived completely from the executable program.

An interesting case worth mentioning in the analysis of a source code is *Ibcos Computers Ltd v Barclays Mercantile Highland Finance Ltd*.[338] In this case Jacob J gives a helpful commentary on source code in the following terms:

> The program the human writes is called the "source code". After it is written it is processed by a program called a compiler into binary code. That is what the computer uses. All the words and algebraic symbols become binary numbers...It is possible to insert messages in a source code. A reader who has access to it can then understand, or understand more readily, what it is going on. Such notes, which form no part of the program so far as the computer is concerned, are called "comments". They are a kind of side-note for humans. In the DIBOL or DBL programs with which I am concerned, a line or part of a line of program which is preceded by a semi-colon is taken by the compiler as a comment. That line is not translated by the compiler into machine code. The program would work without the comment.

The above case illustrates the difference that exists between the code written by programmers that provide instructions to the computer and the comments made by the programmer while writing the code. As noted by Mason, inaccurate information or incorrect instructions will render the computer unresponsive, while misspelt comments will not affect the operation of the computer.[339]

Now that one has gained insight on the creation and operation of a source code and the digital information it involves, the discussion on the nature of digital information vis-à-vis hearsay becomes even more interesting. Teppler provides a good ground for discussion.

For the purposes of distinguishing what digital data is hearsay, Teppler notes that judicial authority in the US appears to divide digital data into three categories: the first category includes

338 1994 FSR 275

339 Mason *Electronic Evidence* (2010) 337

the creation of computer-generated information input into a computer solely by a person; the second category comprises computer-generated information into a computer in part by a person, and in part by a computer application; the third category refers to computer-generated information created without direct human input or assistance.[340] He illustrates the first category by giving the example of a memorandum created by a person using a word processing application. The content of the memorandum is generally considered hearsay (if offered to prove the truth of the matter asserted). Since this memorandum, however, as any computer-generated data, has metadata, an interesting question asked by Teppler is whether the metadata is also hearsay? Teppler cites decided authority to respond negatively considering that the generation of metadata is made without input or assistance from a person.[341] Such evidence, if put in the South African context, will be subject to rules of hearsay as regarding the memorandum content and to rules of real evidence as to metadata associated with the memorandum. In other words, the content of the memorandum will be subject to analysis as to whether it was hearsay and, therefore, to be excluded, or an exception and, therefore, admitted; the metadata associated to the content, however, would need only to be authenticated to be admitted. This is exactly what Teppler objects to. According to him, all computer-generated information should be considered as hearsay and be subject to a "reliability" requirement as an exception to the exclusionary rule. In that way artificially created distinctions could be avoided.[342] The second category, that is, digital data generated in part by a person and in part by computer application, can be exemplified by a person creating a form to be filled out by other people using various forms of software. In fact, as pointed by Teppler, digital data in category one and category two are the same and should be treated in an identical manner.[343] The third category relates to digital data generated without the intervention of a human being and can be illustrated by the situation where a computer creates a record of a transaction with another computer, such as computer-generated information created by a remote computer during the process by which the remote computer received computer-generated information transmitted to it from another computer or the metadata associated with the content (for example the file header or the IP address). Such

340 Teppler "Digital data as hearsay" 15
341 Teppler "Digital data as hearsay" 16
342 Teppler "Digital data as hearsay" 17
343 Teppler "Digital data as hearsay" 16-17

evidence was held, in *U.S. v Hamilton*,[344] not to be hearsay as there was no person making a declaration. Teppler counter argued against this logic by affirming that the data received could be considered as hearsay in that "the receiver computer was carrying out the stated intent or declaration of the system or network administrator, or a programmer, to carry out some request that the receiving computer was told by the sending computer, which in turn was requested by a statement or declaration of the person or sender".[345] Teppler concludes by submitting that all computer-generated information is hearsay of some sort and that these categories are merely distinctions without difference.[346]

The viewpoint of Teppler to consider all computer-generated information as hearsay may cause confusion in practice. Even if it is accepted that there is hearsay of some sort in any computer-generated information, in some instances the link is just too remote to really significantly affect such information. The mere fact that computer-generated information is the product of a software programme relying on a source code which was developed by human being is not sufficient in this author's view to justify this information to be considered as hearsay. Otherwise the output of all devices and machines created by a human being should be considered as hearsay by the simple fact of human involvement in the creation of the machine or device. Such viewpoint is dangerous as it will create an unnecessary burden for litigants. In addition it might lead to the exclusion of perfectly reliable information if no exception to the exclusion can be invoked while the probative value of the information does not even depend on the credibility of a person. Lastly it will challenge principles of the law of evidence governing real evidence. The emphasis should therefore be put more on the direct involvement of the human being in the production of the computer-generated information to determine hearsay nature or not. In other words the approach of *The Statue of Liberty*[347] case should be retained.

344 412 F3d 1138, 2005 WL 1519112 (10th Cir. 2005)
345 Teppler"Digital data as hearsay" 18
346 Teppler"Digital data as hearsay" 18
347 1968 1 WLR 739

3.3.3.3 Statutory exceptions to the hearsay rule

Four statutes providing exceptions to the hearsay rule in England are discussed below. They include the Bankers' Books Evidence Act 1879, the Law of Evidence Act 1968, the Civil Evidence Act 1995 and the Criminal Justice Act 2003.

3.3.3.3.1 Bankers' Books Evidence Act 1879

This Act is among the first statutes to limit the hearsay rule in common law in England. In terms of this Act, a copy of any entry in a banker's book shall in all proceedings be received as *prima facie* evidence of such entry, and of the matters, transactions, and accounts therein recorded, subject to a number of requirements.[348] The purpose of the Act was to avoid the disruption of bank activities because of the necessity to produce the bank's original records in court.[349]

Despite the fact that this Act was enacted in an a different time, with different bank practices in mind, and referred, in its original form, exclusively to "books", this did not prevent the court in *Barker v Wilson*[350] from applying a robust construction so as to accept more modern methods, a microfilm in this instance. It was contended by the appellant in this case that the definition of "bankers' books"[351] in section 9 of the 1879 Act did not include microfilm. The justices were of the opinion, however, that the section 9 list of books was not exhaustive and that there was no reason to exclude microfilm from the definition, which is acceptable in all modern accountancy and auditing techniques. So for Caulfield J, if microfilm is used by a bank to record the payment of cheques by photographing the name of the payee and other matters, there is no doubt that it falls under the definition of "book". Bridge LJ concurred by declaring the following:

> The Bankers' Books Evidence Act 1879 was enacted with the practice of bankers in 1879 in mind. It must be construed in 1980 in relation to the practice of bankers as we now understand it. So construing the definition of 'bankers' books' and the phrase 'an entry in a banker's book', it seems to me that clearly both phrases are apt to include any form of permanent record kept by the

348 S 3

349 Tapper *Computer Law* 406

350 1980 2 All ER 81

351 "Bankers' books" is defined by this section as including ledgers, day books, cash books, account books, and all other books used in the ordinary business of the bank

> bank of transactions relating to the bank's business, made by any of the methods which modern technology makes available, including, in particular, microfilm.[352]

The definition was subsequently amended and section 9(2) now reads as follows:

> Expressions in this Act relating to 'bankers' books' include ledgers, day books, cash books, account books and other records used in the ordinary business of the bank whether those records are in written form or are kept on microfilm, magnetic tape or any other form of mechanical or electronic data retrieval mechanism.

Tapper commended the judicial flexibility shown in *Barker v Wilson*[353] and recommended a similar approach in dealing with any pedantic quibbles that may be raised about the applicability of the amended definition to newer techniques.[354]

As recommended by Tapper, in *Job v Halifax PLC*,[355] His Honour Judge Inglis accepted printouts from log files as evidence of the matters recorded therein, that is, transactions made by the claimant. The log files consisted of information that had been sent by the ATM about a transaction to the bank's record system.

3.3.3.3.2 The Law of Evidence Act 1968

In 1964, the Law Reform Committee was tasked with a mission to look at rules which were no longer appropriate in modern conditions. It looked at the hearsay rule and the Evidence Act of 1938, which it found defective because it excluded many business records, particularly those falling under modern systems of record-keeping. It, therefore, recommended explicitly including as an exception to the hearsay rule mechanically-recorded statements, provided that there was a duty to record them.[356] The recommendations were included in the Civil Evidence Act of 1968. This Act was unique in the sense that it incorporated a section dealing with the admissibility of evidence derived from computers. In terms of this Act, hearsay[357] was admissible in civil

---

352 *Barker v Wilson* 1980 2 All ER 81 at 83

353 1980 2 All ER 81

354 Tapper *Computer Law* 408

355 2009, (unreported) Case number 7BQ00307. The full transcript of the judgment is available, with a commentary by Alistair Kelman, in 2009 *Digital Evidence and Electronic Signature Law Review* 6 235-245

356 Tapper *Computer Law* 384

357 Hearsay was defined as a statement in any civil proceedings other than one made by a person while giving evidence in those proceedings. The statement could be oral, written, or other

proceedings only by virtue of this Act and other statutory provisions,[358] or by agreement of the parties.[359] Three new principal routes to admissibility were, thus, introduced by this Act, namely first-hand hearsay,[360] records made by one acting under a duty,[361] and statements produced by computers.[362]

Section 5 of the Civil Evidence Act 1968 calls for more attention since it dealt with computer evidence. In terms of this section, a statement contained in a document produced by a computer was, subject to the rules of court, admissible as evidence of any fact stated therein, provided certain conditions were met.[363] The conditions were: that the document containing the statement had to be produced by the computer during a period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period;[364] that information, similar to that contained in the statement, was regularly supplied to the computer in the ordinary course of those activities;[365] that, throughout the material part of that period, the computer was operating properly or, if not, this fact did not affect the production of the document or the accuracy of its content;[366] and, finally, that the information contained in the statement reproduced, or was derived from, information supplied to the computer in the ordinary course of those activities.[367]

"Computer" was defined in this Act[368] as any device for storing and processing information.[369] The definition was wide enough to suggest that it could even apply to state-of-the-art, of that time, devices like electric typewriters and hand-held calculators since it did not ask that storage or processing be automatic.[370] Tapper recommended rather, as a better approach, altogether dropping any attempt at a definition and accepting that "computer" had become an ordinary

358 "Statutory provision" was defined in this section as meaning any provision contained in, or in an instrument made under, this or any other Act, including any Act passed after this Act
359 S 1
360 S 2(1)
361 S 4(1)
362 S 5(1)
363 S 5(1)
364 S 5(2)(a)
365 S 5(2)(b)
366 S 5(2)(c)
367 S 5(2)(d)
368 For the purposes of Part I of the Act
369 S 5(6)
370 Tapper *Computer Law* 396

English word which a judge is perfectly capable of comprehending.[371] The advantage would have been, according to him, not to confine the definition to the technology of a particular time. He conceded implicitly, however, that the definition was still important to prevent the standard output of a word-processing package running on a small home computer, for example, to come within the complex of definitions and so be subject to the conditions imposed by section 5.[372] "Statement" was defined as including any representation of fact, whether made in words or otherwise.[373] And it was necessary for the statement to be contained in a document for the electronic evidence concerned to benefit from the regime of this section. In other words, oral evidence of the operation of a computer derived, for example, from reading the result of a calculation from a visual display device or looking over the shoulder of a secretary working at a word-processor, was not admissible as evidence under section 5.[374] Finally "document", in terms of this Act, included *inter alia* any photograph, any disc, tape, sound track, or other device in which sounds or other data (except visual images) which are embodied so as to be capable of being reproduced therefrom, or any film,[375] negative, tape, or other device in which one or more visual images are embodied so as to be capable of being reproduced therefrom.[376] It is interesting to note that this 1968 Act definition was sufficiently comprehensive to cover most commonly used forms of computer storage of the time and even of now.

Surprisingly, section 5 did not provide for the requirement of personal knowledge of the truth of the information by the originator of the information processed by the computer. This was quite problematic since it ignored, for instance, the fact that erroneous data could be entered into the machine. This approach, as noted by Trapper, was not only opposed to sections 2 and 4 of the same Act, on the one hand, but also to all other hearsay exceptions for evidence derived from computers throughout the common law world, on the other hand. In both cases, an emphasis was put on personal knowledge from the originator of the information.[377]

371 Tapper *Computer Law* 396
372 Tapper *Computer Law* 396
373 S 10(1)
374 Tapper *Computer Law* 396
375 Film included microfilm
376 S10(1)
377 Tapper *Computer Law* 396

3.3.3.3.3 The Civil Evidence Act 1995

The Civil Evidence Act 1995, which repeals Part 1 of the Civil Evidence Act1968,[378] is the first Act to abolish the hearsay rule. It provides that evidence shall not be excluded in civil proceedings on the ground that it is hearsay.[379] "Hearsay" means, under this Act, a statement made otherwise than by a person while giving oral evidence in the proceedings which is tendered as evidence of the matters stated.[380] References to hearsay include hearsay of whatever degree."[381] The party proposing to adduce hearsay evidence is, however, required to give notice of that fact and, on request, give particulars of the evidence.[382] The notice and particulars' requirement may, nevertheless, be waived by way of a provision made by the rules of court specifying classes of proceedings or evidence in relation to which this requirement does not apply,[383] or by agreement of the parties.[384] In addition, compliance with the duty to give notice may be waived by the person to whom notice is required to be given.[385] As a matter of fact, the failure to comply with the requirement to give notice or particulars of evidence does not affect the admissibility of the evidence,[386] but only the weight to be given to the evidence in accordance with section 4.[387] Stephen Whale notes that this is in contrast to other provisions of the Civil Procedure Rules which give the court discretion to refuse to admit evidence submitted in breach of the rules.[388] This is in line with the view expressed by the Law Commission that, if discretion to exclude evidence was to be exercised where proper notice was not served, the effect would be to reintroduce the hearsay rule.[389] In *Sunley v Gowland White Ltd,*[390] the Court of Appeal held that a report was admissible in spite of the absence of a hearsay notice. It relied not only on section 2(4) of the Civil Evidence Act 1995, but also on paragraph 27.2 of Practice

---

378 Schedule 2
379 S 1(1)
380 S 1(2)(a)
381 S 1(2)(b)
382 S 2(1)
383 S 2(2)(a)
384 S 2(3)
385 S 2(3)
386 S 2(4) first sentence
387 S 2(4)(b)
388 Whale "Hearsay in Civil Proceedings" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 (hereafter referred to as Whale "Hearsay in Civil Proceedings") 817
389 Whale "Hearsay in Civil Proceedings" 817
390 2003 EWCA Civ 240

Direction 32,[391] which provides that all documents contained in bundles agreed for use at a hearing shall be admissible as evidence of their contents unless the court orders otherwise or a party gives written notice of objection to the admissibility of particular documents.

This Act reaffirms the common law exceptions to the hearsay rule initially preserved by the Civil Evidence Act 1968:[392] namely, published works dealing with matters of a public nature (for example, histories, scientific works, dictionaries, and maps);[393] public documents (for example, public registers, and returns made under public authority with respect to matters of public interest);[394] and records (for example, the records of certain courts, treaties, Crown grants, pardons and commissions).[395] It is interesting to note that this category of documents, some of which would be now found in digital form, is admissible as evidence of facts stated therein.[396] In addition, a document originating from the records of a business or public authority may be received in evidence without further proof.[397] The document will be deemed to form part of such records if a certificate to that effect, signed by an officer of the business or the authority to which the records belong, is produced to the court.[398] "Document" is construed here as meaning anything in which information of any description is recorded, and "copy", in reference to a document, means anything onto which information recorded in the document has been copied by whatever means and whether directly or indirectly.[399] This wide definition of "document" and "copy" facilitates the admission in evidence of data stored in digital format. The same applies to "records" which, in this context, is broadly understood as records in whatever form,[400] including electronic records supposedly. "Business" encompasses any activity for profit or not, regularly carried on by any body (whether corporate or not) or by an individual.[401] "Public authority" includes any public or statutory undertaking, any government department, and any person

391 Which supplements the Civil Procedure Rule 32
392 S 9(1) read with S9(2)(b) to (d) of the Civil Evidence Act 1968
393 S 7(2)(a) of the Civil Evidence Act 1995
394 S 7(2)(b)
395 S 7(2)(c)
396 S 7(2)
397 S 9(1)
398 S 9(2)
399 S 13
400 S 9(4)
401 S 9(4)

holding office under Her Majesty.[402] Depending on the specific circumstances of a case, however, the court may exercise its discretion in refusing to apply the above provisions[403] to a particular document or record, or to a description of documents or records.[404]

3.3.3.3.4 The Criminal Justice Act 2003

In terms of section 114 of the Criminal Justice Act 2003, in criminal proceedings a statement not made in oral evidence in the proceedings is admissible as evidence of any matter stated on the following conditions: it is made admissible by a provision of chapter 2 of Part 11 of this Act or any other statutory provision;[405] by any rule of law preserved by section 118;[406] by consensual agreement of all parties to the proceedings;[407] or by the court in the interests of justice.[408]

A provision of chapter 2 worth mentioning here is section 117 which deals with the admissibility of business and other documents and provides that, in criminal proceedings, a statement contained in a document is admissible as evidence of any matter stated if oral evidence given in the proceedings would be admissible as evidence of that matter[409] and other requirements are satisfied.[410] These requirements are specially considered in the section dealing with documentary evidence.[411] In *Brown v Secretary of State for Social Security*,[412] section 24 of the Criminal Justice Act 1988 (a similar provision to section 117, now repealed) was considered. The statements from computer records adduced by the Secretary of State were held not admissible under section 24(4) of the Criminal Justice Act 1988. The respondent failed to give evidence that is was impossible for the makers of the statements to have recollection of the matters referred to in their statements.[413]

402 S 9(4)
403 S 9(1)-(3)
404 S 9(5)
405 S 114(1)(a)
406 S 114(1)(b)
407 S 114(1)(c)
408 S 114(1)(d)
409 S 117(1)(a)
410 S 117(1)(b) and (c)
411 S 3.2.3
412 1995 C.O.D. 260
413 Mason *Electronic Evidence* (2010) 341

Section 118 of the Criminal Justice Act 2003 is another important provision. This section preserves the common law exceptions to the hearsay rule comprised of published works dealing with matters of a public nature, public documents, and records.[414]

The statutes discussed above illustrate the evolution of the hearsay rule in England from the 19th century to date. With the development of technology and its corollary electronic evidence, it becomes imperative to find ways of adapting old rules to new realities. The Bankers'Books Evidence Act 1879 made the first attempt to limit the hearsay rule as to allow the admission of electronic evidence.[415] The Civil Evidence Act 1968 followed suit and made admissible statements produced by computers under certain conditions.[416] The Civil Evidence Act 1995 went even further by abolishing the hearsay rule making thus all hearsay admissible provided the notice and particulars' requirement is adhered to.[417] Lastly, the Criminal Justice Act 2003 makes also hearsay admissible.[418] In conclusion, the law as it stands today in England allows the admission of electronic evidence irrespective of its hearsay nature. With this in mind, it becomes interesting to consider the situation in South Africa.

3.3.2 South Africa

As already mentioned, the hearsay rule applicable in South Africa is of English origin. The English common-law hearsay was incorporated into the South African law of evidence with its exceptions. The position was thus the same, namely that hearsay was inadmissible unless it fell under the recognised exceptions. The situation has since evolved by way of legislative intervention. The first general legislation to amend common-law hearsay in South Africa was, according to Tapper, the Civil Proceedings Evidence Act 1965 which followed the English Evidence Act 1938.[419] Other important pieces of legislation regulating hearsay evidence particularly relevant in the analysis of electronic evidence include: the Criminal Procedure Act 51 of 1977;[420] the Electronic Communications and Transactions Act 25 of 2002;[421] the Computer

414 See S 27(2) of the Civil Evidence Act 1995
415 Ch 3 par 3.3.3.3.1
416 Ch 3 par 3.3.3.3.2
417 Ch 3 par 3.3.3.3.3
418 Ch 3 par 3.3.3.3.4
419 See S 34; Tapper *Computer Law* 399
420 S 221
421 S 15(4)

Evidence Act 1983;[422] and, central to this issue, the all-important Law of Evidence Amendment Act 45 of 1988. The rule of hearsay is analysed in the context of electronic evidence with regard to the above statutes in what follows. Common law hearsay, although statutory abolished, however, deserves brief consideration before dealing with the relevant statutes and addressing some cases.

3.3.2.1 Common law

The purpose of excluding hearsay at common law was its unreliability, as it relied on the testimony of non-testifying witnesses who could not be tested by cross-examination. This was particularly concerning in a jury trial where jury members did not have the required skill and expertise to assess the weight of such evidence properly.[423] The rule, however, sometimes excluded reliable evidence in spite of the existence of exceptions. The main concern of the common-law rule was its rigidity, which led to the exclusion of hearsay which did not fall under recognised exceptions, no matter how reliable it was. Sometimes the result was grave injustice.[424] It is, therefore, to be welcomed that the Law of Evidence Amendment Act 45 of 1988 has relaxed this rigidity by abolishing the common-law hearsay.

Under common law, therefore, electronic evidence such as a data message, used to establish the fact that information in it was sent, received, or stored, is not excluded. If, however, the data message is used to show the truth of its contents, it is hearsay and inadmissible unless it falls under one of the exceptions to the hearsay rule.[425] This was, however, the position prevailing prior to 1988. From that date onwards electronic hearsay, as is the case with any other hearsay, is governed by the Law of Evidence Amendment Act 45 of 1988 which is discussed below.

422 Repealed

423 Hoffmann & Zeffert *The South African Law of Evidence* (4th ed) 1988 (hereafter referred to as Hoffmann & Zeffert *The South African Law of Evidence*) 125

424 Hoffmann & Zeffert *The South African Law of Evidence* 126

425 Hofman "Electronic evidence in criminal cases" 2006 *SACJ* 3 257 (hereafter referred to as Hofman "Electronic Evidence in criminal cases") 264

3.3.2.2 The Law of Evidence Amendment Act 45 of 1988

3.3.2.2.1 Definition

This landmark Act 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.[426] What distinguishes this definition from the common-law hearsay is that, in this case, a statement does not need to be tendered with the purpose of asserting the truth of its content to be hearsay. All it needs is for its probative value to depend on someone other than the testifying witness. This leads one to the question, what the "probative value" of evidence is? To answer this question, it is worth referring to the example given by Schwikkard. In his scenario, X parks outside a supermarket, and, when he comes out after shopping, he notices that his car had been bumped into from the back. Then a total stranger, who claimed to have witnessed the accident and recorded the registration number of the other car, approaches him and hands him a piece of paper with a number plate corresponding to a car owned by Y. X sues Y and the piece of paper is tendered in evidence. The probative value of this piece of evidence is to establish that Y's car was the car that collided with X's car.[427] The next issue is to determine upon whose credibility does the probative value depend? Before responding to this question, it is crucial to define what is meant by "depends on"? Zeffertt and Paizes suggest, as an option, to read "depends on" as meaning "depends substantially or primarily upon", but they advocate for a more functional approach which will consider evidence to be hearsay if its probative value depended *sufficiently*[428] upon the credibility of someone other than the witness.[429] In the above scenario, therefore, the probative value of the piece of paper will depend upon the credibility of Y.

3.3.2.2.2 Section 3 of the Law of Evidence Amendment Act 45 of 1988

This section takes an exclusionary approach towards hearsay and provides as follows:

3. (1) Subject to the provisions of any other law, hearsay evidence shall not be admitted as evidence at criminal or civil proceedings, unless –

426 S 3(4)
427 Schwikkard & Van der Merwe *Principles of Evidence* 275
428 Emphasis in the original text
429 Zeffertt & Paizes *The SA Law of Evidence* 390

(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.

The discussion that follows reviews the three scenarios under which hearsay evidence can be admitted, that is, by agreement of parties (A), provisionally (B) and in the interests of justice (C).

A. Admission of hearsay by agreement (section 3(1)(a))

Under this provision, hearsay evidence may be admitted by consent. The consent can be explicit or implied. Indeed, the failure to object to the admission of hearsay evidence can be regarded as

consent. This view was expressed in *S v Waldeck*,[430] where it was held that the defence, by its conduct, agreed or acquiesced in the State's procuring hearsay evidence. Zeffertt and Paizes, nevertheless, advise on the preference to insist on express consent and not rely on a failure to object to the admission of hearsay evidence as implied or tacit consent. This is even more crucial in a criminal trial when the accused is unrepresented.[431]

B. Provisional admission of hearsay (section 3(1)(b) read with section 3(3))

Hearsay evidence may be admitted provisionally if the court is informed at the time of adducing the hearsay evidence that the person upon whose credibility the probative value of such evidence depends will testify in such proceedings. If at the end of the day, he does not testify, the hearsay evidence will be excluded unless it is accepted by consent as above or admitted in the interests of justice. In the event that he testifies but disavows the hearsay evidence, a literal reading of paragraph (b) of subsection 3(1) seems to suggest that such hearsay should not, nevertheless, be excluded. The Supreme Court of Appeal in *S v Ndhlovu and Others*,[432] rejected this interpretation and held that such situations were not different from those where the declarant does not testify at all, since the utility of cross-examination is similarly negated. It was further held that the admissibility of such hearsay evidence not confirmed under oath should, therefore, be considered under the interests of justice requirement. Zeffertt and Paizes disagree with the position of the Supreme Court of Appeal. In their view, the court overstated the extent to which the utility of cross-examination is negated when the declarant disavows the original statement or fails to recall making it. They suggest that, in such cases, questioning the declarant in a manner that highlights inconsistencies or additional information may assist the court in making a reasonable assessment of the reliability of the original statement.[433]

C. Admission of hearsay in the interests of justice (section 3(1)(c))

Hearsay evidence may be admitted if the court is of the opinion that it is in the interests of justice to do so. To reach such a conclusion the court must take into account the six factors listed in

430 2006 2 SACR 120 (NC)
431 Zeffertt & Paizes *The SA Law of Evidence* 394
432 2002 2 SACR 325 (SCA)
433 Zeffertt & Paizes *The SA Law of Evidence* 396

paragraph (c) of subsection 3(1).[434] It is also free to consider any other factor which should, in the opinion of the court, be taken into account.[435] These seven factors are discussed below from point (i) to (vii).

(i) The nature of the proceedings

It is important to distinguish here essentially between civil proceedings and criminal proceedings. In civil proceedings, admission of hearsay evidence in the interests of justice will be easier to justify because of the lower standard of proof applicable, namely a balance of probabilities. In criminal proceedings, however, the constitutional right to a fair trial,[436] which includes the presumption of innocence and the right to challenge evidence, makes the admission of hearsay difficult when the evidence is tendered against the accused. As a matter of fact there is a greater reluctance to admit hearsay evidence in criminal cases where such evidence plays a decisive part in convicting an accused.[437]

(ii) The nature of the evidence

According to Schwikkard, in spite of the lack of clear guidance from the case law, it can be inferred from *Hewan v Kourie NO*[438] that the primary concern of courts when dealing with the nature of evidence is the reliability of such evidence. He added that this criterion is also important when dealing with probative value.[439] The unreliability of hearsay evidence is due, as noted by Zeffertt and Paizes, to the fact that the person upon whose credibility the probative value of such evidence depends is not subjected to the curial devices designed to identify, assess, and eliminate aspects of the evidence that render it potentially unreliable.[440] They suggest, therefore, that the court in such situations uses a three-pronged approach, consisting, firstly, in understanding what the potential dangers are, secondly, in considering the extent to which those dangers actually arise in the case before it, and, thirdly, in identifying factors that tend to reduce

434 (i) to (vi)
435 (vii)
436 S 35 of the Constitution, Act 108 of 1996
437 See *Metedad v National Employer's General Insurance Co Ltd* 1992 1 494 (W).Read also Zeffertt & Paizes *The SA Law of Evidence* 399-401
438 1993 3 SA 233 (T)
439 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 279
440 Zeffertt & Paizes *The SA Law of Evidence* 401

or even eliminate those dangers.[441] The dangers that need to be considered by the court are, firstly, insincerity on the part of the absent declarant or actor, secondly, erroneous memory, thirdly, defective perception, and, finally, inadequate narrative capacity.[442] These dangers are discussed in the following lines.

1. Insincerity

To judge the sincerity on the part of the absent declarant or actor, different factors need to be considered, such as "whether the evidence was assertive or non-assertive; whether it was against the interests of the absent actor or declarant, whether there was any motive to lie; the relationship between the absent actor or declarant and the party against whom the evidence is tendered; the timing of the act or statement, and whether it was voluntarily or spontaneously made; whether it was subject to the oath, cross-examination or any devices calculated to induce one to speak the truth; the status of the person and his or her reputation for honesty; the multiplicity of declarants and the ensuing unlikelihood of conspiracy, the circumstances in which the statement was made."[443]

It is submitted that there is no reason why these factors cannot be applied to ascertain the sincerity on the part of the declarant of hearsay electronic evidence. Let one consider a hypothetical case where a Whatsapp's voice note is tendered in evidence. In the voice note the declarant X describes a motor vehicle collision between Y's parked car and W's moving car and describes precisely W's car make, model, colour, and registration number and sends the voice note to Y. Y in a claim for damages against W adduces the voice note in evidence to prove that W was to blame, while X was unavailable to testify. The above will indeed be useful.

Zeffertt and Paizes give various examples of cases where the courts have identified the potential danger of insincerity and, after finding grounds for negating it, have accepted the evidence.[444] A case worth mentioning is *S v Shaik and Others.*[445] In this case, the conviction of the appellants for contravening section 1(1)(a)(i) of the Corruption Act 94 of 1992 was based largely on the

441 Zeffertt & Paizes *The SA Law of Evidence* 401

442 Zeffertt & Paizes *The SA Law of Evidence* 401*;* Zeffertt & Paizes further affirm that these hearsay dangers were recognised by the Constitutional Court in *S v Molimi* 2008 2 SACR 76 (CC) at par 34, note 65

443 Zeffertt & Paizes *The SA Law of Evidence* 402

444 Zeffertt & Paizes *The SA Law of Evidence* 402

445 2007 1 SA 240

contents of an encrypted fax. The appellants objected to its reception but the trial Court admitted it on the basis of what it considered to be a common-law exception to the rule against hearsay. The Court of Appeal decided that it was not necessary to inquire whether or not such exception was recognised in common law since hearsay evidence is now regulated by section 3 of the Law of Evidence Amendment Act 45 of 1988. With regard to the nature of evidence, the evidence consisted of T's (an executive of a French arms company that played a pivotal role in "the arms deal") advice to his superiors as to what happened at a meeting between him, the first appellant (a businessperson) and Z, a prominent politician. It was recorded shortly after the meeting and, on face of it, incriminated all three of them. The advice was conveyed by encrypted fax to Paris. The Appeal Court believed in the sincerity of the author of the fax since it was very incriminating for himself and the court further held that it was highly unlikely that T would have exposed himself to such dangers had it not been necessary to do so. The Court concluded by saying that the fax had a high probative value despite T's general unreliability.

2. Memory

Factors that need to be considered in ascertaining the reliability of memory include: the length of time between the act or statement and the event; how important the matter is to the maker of the statement or actor; whether the maker or actor has a direct interest or not; whether the evidence is first- or second-hand hearsay; the degree of detail the evidence contains; and the extent of the reliance on the memory of the absent declarant or actor.[446]

In respect of the first factor, the fact that it is more and more common to carry a device, such as a Smartphone, allowing the creation of electronic data almost instantly means that the length of time between the act or statement and the event will be minimal, therefore, reducing the risk of defective memory in the case of electronic evidence. Depending on the type of electronic evidence, however, this factor and the others still need to be investigated to ascertain the reliability of memory as far as such evidence is concerned. Zeffertt and Paizes refer to an unreported case where these factors were found to have enhanced the reliability of the hearsay evidence in issue. It was *S v Montgomery*,[447] in which the evidence adduced included information made a relatively short time before the court hearing; was not duly complicated; was

[446] Zeffertt & Paizes *The SA Law of Evidence* 403

[447] (Unreported WLD, case no A814/05, (25 May 2005))

highly dramatic and unusual and not likely to be forgotten; and the witness was himself involved in some of the events he described.[448]

3. Perception

When dealing with the accuracy of perception, it is important to consider the following factors: whether the maker had a proper opportunity to perceive the facts which his act or statement is offered to show; whether he had personal knowledge of the facts; whether the hearsay evidence is of a first-hand or second-hand nature; whether doubt exists as to the ability of the maker to have perceived the facts in issue properly (for example, poor eyesight or hearing).[449] In *S v Mpofu*,[450] the Appeal court held that the court *a quo* erred in receiving evidence of a piece of paper on which a passer-by had written the registration number of the car which had allegedly struck the deceased. The passer-by did not testify, and the court held that there was no objective way of testing her opportunity for observation and so the reliability of what she recorded. In *Mamushe v S*,[451] the Supreme Court of Appeal held that hearsay evidence of identification can be admitted only if the possibility of mistake can be safely excluded in some other way, for example with reference to objectively established facts.

4. Narrative capacity

Factors affecting the narrative capacity include: the manner of the transmission of information by the absent actor or declarant to the witness; whether anything can suggest that the maker's act or statement could have been driven by a belief or fact other than the one it intends to establish; the simplicity or complexity of the act or statement; whether the hearsay evidence is of a first-hand or second-hand nature; and the court's opinion on the ability of the witness to convey accurately the act or statement of the maker considering the peculiar susceptibilities of hearsay to erroneous transmission.[452] It is submitted that writing is clearer than oral communication. In *Mnyama v Gxalaba and Another*,[453] it was held that the danger of misreporting oral statements is ordinarily high because of a witness's poor recounting skills or nuances that can change the meaning of the

448 Zeffertt & Paizes *The SA Law of Evidence* 403
449 Zeffertt & Paizes *The SA Law of Evidence* 404
450 1993 3 SACR 109 (N)
451 2007 4 All SA 972 (SCA)
452 Zeffertt & Paizes *The SA Law of Evidence* 403-404
453 1990 1 SA 650 (C)

statements. These dangers are, however, mitigated in respect of electronic hearsay transmitted electronically. Indeed advances in technology allow for the easy communication of information either in oral or written form. The possibility of reading, listening, or viewing the information as much as necessary, therefore, reduces the risk of misreporting. This can be illustrated by a BBM voice note.

After considering these four dangers relating to insincerity, memory, perception and narrative capacity in the assessment of the nature of the evidence, one can look next at the third factor relevant in the admission of hearsay evidence under the interests of justice requirement, namely the purpose for which the evidence is tendered.

(iii) The purpose for which the evidence is tendered

"The purpose for which the evidence is tendered" has been interpreted as meaning that evidence tendered for a compelling reason is more likely to be received than evidence tendered for a doubtful or illegitimate purpose.[454] The fact that evidence is tendered to establish a fundamental issue as opposed to a subordinate issue, however, was held in certain cases as weighing against its admission.[455] This view was contested in *S v Mpofu*,[456] where it was stressed that truthfulness and reliability were the factors to consider for the admission of evidence.

(iv) The probative value of the evidence

"Probative value" means value for purposes of proof. In other words, "what the hearsay evidence will prove if admitted?" and, "will it do so reliably?"[457] The probative value of the evidence is, in fact, one variable of legal relevance, the other variable being prejudicial effect. Evidence is said to be relevant only if the first outweighs the second.[458]

---

454 *Metedad v National Employer's General Insurance Co Ltd* 1992 1 SA 494 (W); in *S v Ndhlovu and Others* 2002 2 SACR 325 (SCA) par 44 factors taken by the court to admit hearsay evidence included the fact that its purpose was "direct, not oblique, and its attainment depended not on speculative inference – as may be the case in statements of future intention – but squarely on the reliability of the hearsay"

455 *Hlongwane and Others v Rector, St Francis College and Others* 1989 3 SA 318(D); *Hewan v Kourie NO and Another* 1993 3 SA 233 (T)

456 1993 2 SACR 109 (N)

457 *S v Ndhlovu and Others* 2002 2 SACR 325 (SCA) par 45

458 Zeffertt & Paizes *The SA Law of Evidence* 407. Legal relevance is a necessary condition of admissibility.

(v) The reason why the evidence is not given by the person upon whose credibility the probative value of such evidence depends

Reasons why the evidence is not given by the person upon whose credibility the probative value of such evidence depends may include *inter alia* the death of the declarant; the witness's absence from the country; an inability to trace a witness; the extremely frail health of a witness; fear of retribution, including loss of life; and prohibition in law to disclose information.[459]

(vi) Any prejudice to a party which the admission of such evidence might entail

Prejudice to a party can be caused by the fact that the person upon whose credibility the probative value of evidence depends is not subject to the techniques designed to detect and expose error, such as testifying in open court with the careful scrutiny of judge, triers of fact, adversary, counsel and spectators and the absence of oath or cross-examination, to name but a few.[460] The prejudice may, however, be mitigated in certain circumstances, for example when the statement was made under oath, or the adversary had an opportunity to question the maker of the statement.[461]

Zeffertt and Paizes address the constitutional implications that potential prejudice in the admission of hearsay evidence may give rise to in criminal cases. They refer to section 35(3) of the Constitution which provides for the right to a fair trial for any accused person, which right includes the right to challenge evidence.[462] They argue that section (3)(1)(c), to the extent that it allows for the admissibility of hearsay evidence, constitutes a limitation of the right to challenge evidence, and they are further confident that this limitation is reasonable and justifiable.[463]

(vii) Any other factor which should, in the opinion of the court, be taken into account

It is suggested that common-law exceptions to the hearsay rule can serve as a factor which the court may take into account to admit hearsay evidence. As an illustration, one can cite dying

459 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 280-281
460 Zeffertt & Paizes *The SA Law of Evidence* 410
461 Zeffertt & Paizes *The SA Law of Evidence* 410
462 S 35(3)(i)
463 Zeffertt & Paizes *The SA Law of Evidence* 411

declarations and spontaneous statements,[464] or contemporaneity.[465] Another factor that can be considered is consistency with proven facts.[466]

In conclusion, it is evident from the above discussion on the Law of Evidence Amendment Act 45 of 1988 that this Act offers more flexibility in the treatment of hearsay compared to the common-law hearsay that it abolishes. Electronic hearsay can also benefit from the relaxed regime. This Act, however, is not the only one providing exceptions to the hearsay rule affecting electronic evidence. Four other major statutes providing exceptions to the hearsay rule are discussed below. They include the CPEA, the CPA, the Computer Evidence Act 57 of 1983 and the ECT Act.

3.3.2.3 Other statutory exceptions to hearsay

3.3.2.3.1 The Civil Proceedings Evidence Act 25 of 1965

The CPEA creates an exception to the hearsay rule in respect of documentary evidence in general and in respect of bankers' books in particular. With regard to the former, it provides under section 34 (1) that, " in any civil proceedings where direct oral evidence of a fact would be admissible, any statement made by a person in a document and tending to establish that fact shall on production of the original document be admissible as evidence of that fact." This exception is, however, subject to certain requirements. The first one is that the person who made the statement should have had personal knowledge of the matters dealt with in the statement,[467] or, where the document in question is or forms part of a record purporting to be a continuous record, it is further required that the person who made the statement must have done so 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.[468] In addition to either of the above requirements, the person who made the statement must be called as a witness unless this is impossible for some good reason, such as he has died; his bodily or mental condition makes him

464 *S v Mbanjwa* 2000 2 SACR 100 (D)
465 *Skilya Property Investments (Pty) v Lloyds of London Underwriting* 2002 3 SA 765 (T)
466 Schwikkard & Van der Merwe *Principles of Evidence* (2009) 282
467 S 34(1)(a)(i)
468 S 34(1)(a)(ii)

unfit to attend as a witness; he is outside the Republic, and it is not reasonably practicable to secure his attendance; or all reasonable efforts to find him were unsuccessful.[469]

Notwithstanding these criteria, the presiding officer has overriding discretion to admit in evidence a statement which does not comply with the above requirements if, having regard to all circumstances of the case, he is satisfied that undue delay or expense would otherwise be caused.[470]

"Statement" is defined as any representation of fact, whether made in words or otherwise.[471] It is submitted, however, that a "representation of fact" may include a statement of opinion if the maker's opinion would have been admissible in oral evidence.[472] In contrast, a written statement by a witness to a motor accident stating that in his opinion one of the drivers was negligent would not have been admissible because the direct oral evidence of such an opinion would have been inadmissible in the first place.[473]

"Document" is defined as including any book, map, plan, drawing, or photograph.[474] Van der Merwe affirms that it is an open question whether this definition of "document" is wide enough to include computers and other recent manifestations of ICT technology.[475] Indeed, if one considers that the Civil Proceedings Evidence Act is inspired by the English Evidence Act of 1938 which was repealed because it excluded many business records, particularly those falling under modern systems of record-keeping, it seems logical to submit that the interpretation of the South African Act should follow suit. Uncertainty, however, remains on that point. In *Narlis v South African Bank of Athens*,[476] although the computer evidence in issue was not admitted under section 34 of the Civil Proceedings Evidence Act 25 of 1965, there was no clear indication that it did not fall under the definition of "document". This is why Holmes, J A recommended

469 S 34(1)(b)
470 S 34(2)
471 S 33
472 Zeffertt & Paizes *The SA Law of Evidence* 2 420. The two authors refer to the case of *Dass (an infant) v Masih* 1968 2 All ER 226 cited in *Blyth v Van den Heever* 1980 1 SA 191 (A) as authority
473 *Dass (an infant) v Masih* 1968 2 All ER 226 cited by Zeffertt & Paizes *The South African Law of Evidence* 421
474 S 33
475 Van der Merwe *et Al Information and Communications Technology Law* 2008 (hereafter referred to as Van der Merwe *Information and Communications Technology Law* (2008)) 105
476 1976 2 SA 573 (A)

the approach of the English Civil Evidence Act of 1968 which found it necessary to include a specific provision dealing with the admissibility of computerised statements.[477]

These questions will be studied in detail in the section dealing with the admissibility of electronic evidence as documentary evidence below.[478]

The second exception to the hearsay rule under the Civil Proceedings Evidence Act relates to the bankers' books, and it is found in section 28 which makes bankers' books admissible in certain cases. Under this section, "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." The written affidavit, or any other evidence, must certify that such books are, or have been, the ordinary books of such a bank, that the 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 a bank.[479] It is suggested that this exception is applicable to bank records in the form of data messages.[480] It is, however, not applicable when the bank is a party to such proceedings.[481]

3.3.2.3.2 The Criminal Procedure Act 51 of 1977

Provisions liberating hearsay evidence from the exclusionary rule in the CPA include sections 221, 222 and 236. Section 221 deals specifically with the admissibility of certain trade or business records, while section 222 imports in criminal proceedings certain provisions of the Civil Proceedings Evidence Act, including section 34 which was addressed in the point above. Finally, section 236 is similar to section 28 of the Civil Proceedings Evidence Act and provides for the admissibility of entries in the accounting records of a bank and of any document in the possession of any bank relating to the said entries or to any business transaction of the bank. The definition of "document" under the CPA is much wider, and specifically includes a recording or a transcribed computer printout produced by any mechanic or electronic device and device by

477 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 578

478 See Ch 3 par 3.4.3

479 S 28

480 *Nedbank Ltd v Mashiya and Another* 2006 4 SA 422 (T) at [26] cited by Hofman "Chapter 17: South Africa" in Mason (ed) *Electronic Evidence* (2010) (hereafter referred to as Hofman "Chapter 17: South Africa") 687

481 S 32

means of which information is recorded or stored.[482] This definition and the above provisions will later be analysed in more detail.[483]

3.3.2.3.3 The Computer Evidence Act 57 of 1983

The Computer Evidence Act created an exception to the hearsay rule by providing for the following, "in any civil proceedings an authenticated computer print-out[484] shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible."[485] A printout was authenticated by means of an authenticating affidavit which needed to satisfy a certain number of requirements.[486] In-depth analysis of this Act is undertaken at a later stage.[487]

3.3.2.3.4 The Electronic Communications and Transactions Act 25 of 2002

A general exception to the hearsay rule is created by section 15(4) of the ECT Act, in terms of which "a data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract."

Hofman suggests, in respect of data messages, that the section 15(4) exception to the hearsay rule may well replace exceptions created by sections 28 and 34 of the Civil Proceedings Evidence Act as well as by sections 221 and 236 of the CPA.[488] In addition, he points out six main difficulties with the wording of section 15(4).[489] The first difficulty relates to the scope of the exception for communications made "in the ordinary course of business", which is much wider than the previous business record exceptions. In consequence this exception could also

---

482 S 236(6)
483 Ch 3 par 3.4.3
484 This is the spelling of the Act and apart from the quotation, the spelling printout will be used
485 S 3(1)
486 S 2(1)
487 See Ch 3 par 3.4.3
488 Hofman "Chapter 17: South Africa" 688
489 Hofman "Chapter 17: South Africa" 688

apply to any email or a recorded voice message in the course of business. Secondly, in contrast to the above-mentioned exceptions (save exceptions for banking records), it provides not only for the admissibility of data messages but also makes them rebuttable proof of the facts they contain. In other words, a presumption of truth is created in terms of which data messages will be deemed accurate unless the contrary is proven. Hoffman is clearly concerned about this situation which might lead to circumstances where records of unreliable businesses would be presumed accurate. The third difficulty identified by Hoffman relates to the requirement of a certificate "by an officer in the service of such person" for the data message to be admissible. He feels that this requirement is less stringent than the affidavit required for banking exceptions, providing, therefore, fewer guarantees of responsibility. Fourthly, he notes that, if the person intending to produce this form of evidence has no control over the computer system containing such evidence, it may be difficult to obtain the certificate required to make the evidence admissible. Fifthly, because of the wide range of evidence admissible in terms of section 15(4), he notes that the court could find itself overloaded by volumes of evidence to consider. And, lastly, section 15(4) may raise constitutional challenges in criminal proceedings because of the presumption of truth it creates, which might shift the onus of proof to an accused.[490]

Section 15(4) was interpreted in *Trend Finance (Pty) Ltd and another v Commissioner for SARS and another*.[491] In this case the applicants sought the review and the setting aside of the determination by the respondents, being the Commissioner for the South African Revenue Service and the Cape Town Controller of Customs, that there had been underpayment of customs duty and value-added tax in respect of certain consignments imported by the applicants. In contention was, amongst other things, the admissibility of certain hearsay in terms of section 15(4) of the ECT Act. The hearsay consisted of annexures to a letter from a non-testifying witness, Mr Lee (Mr Lee's letter), comprising computer printouts amongst other copies. Van Reenen J noted, firstly, that a data message is something existing in electronic form as a result of having been generated, sent, received, or stored by electronic means.[492] Thus, when section 15(4) provides for the admissibility of a data message, it implies the necessity for the evidence to be in electronic form, for example on a computer disc.[493] He added that, in the same vein, a copy of a

490 Hofman "Chapter 17: South Africa" 689
491 2005 4 All SA 657 (C) at [678-679]
492 2005 4 All SA 657 (C) at [678 c]
493 2005 4 All SA 657 (C) at [678 d]

data message necessarily connotes an electronic copy rather than a piece of paper.[494] In the same way, an "extract" from a data message is part of the message and must be in electronic form.[495] A printout, on the other hand, would be, according to Van Reenen J, an original document printed from a computer capable of converting a data message into written hardcopy form.[496] Since none of the annexures were in electronic form, the question of analysis was to determine whether they could be admissible as printouts of data messages. It was held that, for a printout to be a "printout" of a data message, it must be shown prior to the printing that electronic representations of information were generated, sent, received, or stored by electronic means.[497] Consequently, it was held that the mere creation of a written document by typing on an electronic typewriter or on a personal computer does not involve the creation of "data messages", and, accordingly, the resultant document cannot be regarded as a "printout" or a "data message".[498] In the present case, no evidence was given as to how the annexures to Mr Lee's letter came into existence. At least one of the documents, moreover, purported to be a facsimile, and a number of others were not sent electronically. It was further stressed that, even if the content of the annexures existed as a data message, it does not mean that the annexures are "printouts" of data messages in terms of section 15(4)[499] since a "printout", under this subsection, is the very document generated by a computer in a printed form.[500] In addition, for the printout to be admissible, it must be certified as correct by an officer in the service of the person who made the data message. In this instance, none of the annexures, it was held, appeared to be printouts in the sense of the above subsection and not even copies made directly from original printouts since it was pointed out that they were copied from microfiche records, which are themselves photographic copies of something else.[501] So a certification that the annexures were true copies meant simply that they were true copies of the microfiche records, since nobody had certified that the documents on which the microfiche records were based were correct printouts of data messages.[502] For the certification to be valid it, furthermore, must emanate from

494 2005 4 All SA 657 (C) at [678 e]
495 2005 4 All SA 657 (C) at [678 e]
496 2005 4 All SA 657 (C) at [678 e]
497 2005 4 All SA 657 (C) at [678 g]
498 2005 4 All SA 657 (C) at [678 h]
499 2005 4 All SA 657 (C) at [679 a]
500 2005 4 All SA 657 (C) at [679 a]
501 2005 4 All SA 657 (C) at [679 a-b]
502 2005 4 All SA 657 (C) at [679 b]

an officer in the service of the person who made the data message. In this instance, the certification came from an alleged official of a company called HSBC, and, so, the respondents who produced the certification had to prove by means of admissible evidence that the underlying data messages were made by HSBC. They failed to adduce such evidence. Some of the documents had been made by a company called BNP, while others, it is suggested, were made by an intermediary organisation facilitating electronic communication between banks. In the light of the above, the court concluded that the annexures to Mr Lee's letter were not admissible in terms of the ECT Act.[503]

Section 15(4) was also considered in *Ndlovu v Minister of Correctional Services and another*.[504] In contrast to the position of Van Reenen J in *Trend Finance (Pty) Ltd and another v Commissioner for SARS and another*,[505] it was held in the present case that a printout is clearly a data message.[506] It was further noted that section 15(4) creates an exception to the manner of proof and evidential weight ordinarily accorded to a data message.[507] Two situations were thus highlighted with regard to the admissibility of a data message on its mere production in terms of section 15(4). The first situation relates to "a data message made by a person in the ordinary course of business", which clearly refers to original data if juxtaposed with the words that follow [in the subsection], and which is admissible on mere production.[508] The second situation relates to a copy or printout or an extract from such data which is admissible on mere production only if it is certified as correct by an officer in the service of such person.[509] From this distinction, it can be affirmed that the correctness of a data message in the first situation does not require certification to be admissible contrary to the second situation where certification is a requisite. This view is supported by Van der Merwe.[510] The wording of section 15(4), however, is

503 2005 4 All SA 657 (C) at [679 e-f]
504 2006 4 All SA 165 (W)
505 2005 4 All SA 657 (C) at [678-679]
506 2006 4 All SA 165 (W) at [172 e]
507 2006 4 All SA 165 (W) at [172 j]
508 2006 4 All SA 165 (W) at [173 a]
509 2006 4 All SA 165 (W) at [173 b]
510 Van der Merwe *Information and Communications Technology Law* (2nd ed) 2016 (hereafter referred to as Van der Merwe *Information and Communications Technology Law* (2016)) 120

susceptible to confusion. This led Collier to argue that section 15(4) could also be interpreted as requiring certification of both types of documents identified by the court.[511]

Another comment by Collier, this time with regard to the definition of data message, was considered by Hofman.[512] According to Hofman, Collier expressed the viewpoint[513] that the definition of a data message in terms of the ECT Act is wide enough to include hearsay evidence and, thus, all data messages are admissible.[514] He criticises this view, rightfully so as submitted by Van der Merwe,[515] for failing to distinguish between form and content.[516] Hofman indeed explains that the ECT Act as the UNCITRAL Model Law on E-commerce defines data as "electronic representations of information in any form" and a data message as "data generated, sent, received, or stored by electronic means". This definition refers to the form in which information is kept and not to the content of the message.[517] He adds further that a document is excluded as hearsay because doubt exists as to the reliability of its content and not because of doubts as to the reliability of the technology used to record that content.[518] He attributes Collier's erroneous view to a misreading of the definition of data. He submits that Collier must have read the definition of data as electronic representations of information *of* any form instead of *in* any form.[519]

This point on the comment by Collier concludes the discussion on the major statutes regulating hearsay in South Africa and brings to an end the section on electronic evidence and hearsay in general. The section has discussed comparatively the regime of hearsay in England and South Africa which has been amended significantly in both jurisdictions through legislative intervention. England has adopted an inclusionary approach toward hearsay making almost all hearsay admissible,[520] while South Africa is still preferring an exclusionary approach but much

511 Collier "Evidently not so simple: Producing computer print-outs in court" 2005 *Juta's Bus L* 13(1) 6 (hereafter referred to as Collier "Evidently not so simple") 8-9

512 Hofman "Electronic Evidence in criminal cases" 264

513 The viewpoint was expressed according to Hoffman in Collier "Machine-generated evidence and related matters" in Schwikkard & Van der Merwe *Principles of Evidence* (2nd ed) 2002 (379 at 385)

514 Hofman "Electronic Evidence in criminal cases" 264

515 Van der Merwe *Information and Communications Technology Law* (2008) 125

516 Hofman "Electronic Evidence in criminal cases" 264

517 Hofman "Electronic Evidence in criminal cases" 264

518 Hofman "Electronic Evidence in criminal cases" 264

519 Hofman "Electronic Evidence in criminal cases" 264 in the footnotes

520 S 1(1) of the Civil Evidence Act 1995

more flexible to allow the admission of more hearsay evidence.[521] In consequence electronic hearsay is well accommodated under the regime currently existing in both England and South Africa. The choice to discuss hearsay separately from documentary evidence below was made out of convenience. It is true that these two concepts are closely connected and should have been discussed together. It is, however, submitted that dealing with them separately make the discussions more focused. Hence, after dealing with hearsay, it is appropriate to discuss now documentary evidence.

3.4 Admissibility and weight of electronic evidence as documentary evidence

Issues addressed in this section have been encountered previously, especially when dealing with hearsay evidence. The present section, however, deals with these issues in more detail, considering their great relevance when one deals with electronic evidence. Undoubtedly, electronic evidence shares many features with documentary evidence. As a consequence, electronic evidence is equalled to documentary evidence most of the time. It is, therefore, appropriate to explore the rules, principles, and provisions pertaining to documentary evidence which are relevant for electronic evidence as well as special provisions regulating electronic evidence.

The admissibility of electronic evidence as documentary evidence is envisaged not only with regard to English and South African law, but also with reference to the rules on E-commerce of the United Nations Commission on International Trade Law.

3.4.1 England

It is proposed here to discuss the admissibility and weight of electronic evidence in England through the following pieces of legislation: the Bankers' Books Evidence Act 1879; the Civil Evidence Act 1995; and the Criminal Justice Act 2003.

[521] The Law of Evidence Amendment Act 45 of 1988 in general

3.4.1.1 The Bankers' Books Evidence Act 1879

This Act stipulates that "[s]ubject to the provisions of this Act, a copy of any entry in a banker's book shall in all legal proceedings be received as *prima facie* evidence of such entry, and of the matters, transactions, and accounts therein recorded."[522]

For a copy of an entry in a book to be received in evidence under this Act, it must be proved that the book was, at the time of making the entry, one of the ordinary books of the bank, that the entry was made in the usual and ordinary course of business, and that the book is in the custody or in the control of the bank.[523] In addition it must be proved that the copy has been examined with the original entry and is correct.[524]

This Act defines "bankers' books" as including ledgers, day books, cash books, account books, and other records used in the ordinary business of the bank whether those records are in written form or are kept on microfilm, magnetic tape, or any other form of mechanical or electronic data retrieval mechanism.[525]

This definition was adopted 100 years after the original definition which restricted "bankers' books" to ledgers, day books, cash books, account books, and other books used in the ordinary business of the bank. It was earlier pointed out that, despite this restricted definition, the court in *Barker v Wilson*[526] did not find any difficulty in applying a robust construction to accept a microfilm as being part of "bankers' books" in terms of the original definition.[527] This was backed by Tapper who recommended the same judicial flexibility when dealing with the applicability of the amended definition of "bankers' books" to newer techniques.[528]

3.4.1.2 The Civil Evidence Act 1995

The Civil Evidence Act 1995 was discussed in a previous paragraph.[529] There is, therefore, no need to repeat what has been already said. Certain aspects, however, need to be considered in

522 S 3
523 S 4(1)
524 S 5(1)
525 S 9(2)
526 1980 2 All E.R. 81
527 For more details see Ch 3 par 3.3.3.3.1 above
528 Tapper *Computer Law* 408
529 See Ch 3 par 3.3.3.3.2

more detail because either they were discussed in passing only or they were not even discussed. In a section dealing with the interaction between electronic evidence and documentary evidence, it is of paramount importance to analyse, amongst others, section 7(2), section 8, and section 9.

A. Section 7(2)

Section 7(2) provides as follows:

> The common law rules effectively preserved by section 9(1) and (2)(a) of the Civil Evidence Act 1968, that is, any rule of law whereby in civil proceedings –
>
> (a) published works dealing with matters of public nature (for example histories, scientific works, dictionaries and maps) are admissible as evidence of facts of public nature stated in them;
>
> (b) public documents (for example, public registers and returns made under public authority with respect to matters of public interest) are admissible as evidence of facts stated in them; or
>
> (c) records (for example the records of certain courts, treaties, Crown grants, pardons and commissions) are admissible of facts stated in them,
>
> shall continue to have effect.

These three types of documents admissible as evidence of facts stated in them are discussed in points (a), (b) and (c) below.

(a) Published works dealing with matters of a public nature

Public works referred to under this heading include histories and historical events, maps, and dictionaries, to name but a few.

1. Histories and historical events

Approved public and general histories are admissible to prove facts of a public or general nature. This exception is useful in that it allows the proof of historical events in spite of the absence of any witness to the event or the account of any eye-witness or film or radio records of the event.[530] The fact that these histories can be found in electronic format either because they have

[530] Pattenden "Common law exceptions to the rule against hearsay: Evidence of reputation or family tradition; bankers' Books; ancient documents" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 910 (hereafter referred to as Pattenden "Common law exceptions to the rule against hearsay") 932

been digitised or because they have been produced in that format make them worth mentioning in this research. There seems to be no reason why such documents or historical treatises in electronic format will not benefit from this exception to the hearsay rule. This exception was creatively addressed in the Canadian case of *R v Zundel*,[531] as pointed out by Pattenden.[532] In this case for Holocaust denial, a professional historian was called as a witness. The historian had written a book on the subject from documents used in the Nuremberg trials. On appeal, it was contended that the historian's evidence was founded on hearsay.[533] The Court held that two exceptions to the hearsay rule were relevant in this case. The first is that events of general history may be proved by accepted historical treatises on the basis that they represent community opinion or reputation with respect to an historical event of general interest.[534] Some conditions must be satisfied, however, namely that the historical event must be one to which it would be unlikely that living witnesses could be obtained, and, secondly, the historical event must deal with a matter of general interest, where there is a high probability that the matter underwent general scrutiny as the reputation, evidenced by the historical treatises, was formed.[535] The court further held that, if an historical treatise is admissible to prove an historical fact of general public interest, it should logically follow, if the conditions for this exception to the hearsay rule are met, than an expert historian may testify as to the existence of an historical event relying upon material to which any careful and competent historian would resort.[536] In the court's view, the testimony of an expert historian was even superior to the admission of an historical treatise, because the expert could be cross-examined.[537]

2. Maps

Like historical treatises, published maps are admissible, on similar grounds, to show the relative positions of towns, countries, and other matters of geographical notoriety.[538] With the development of technology, maps will be readily available in electronic format, for example

---

531 1987 75 C.C.C. (3d) 449
532 Pattenden "Common law exceptions to the rule against hearsay" 932
533 Pattenden "Common law exceptions to the rule against hearsay" 932
534 *R v Zundel*, 1987 75 C.C.C. (3d) 449 at 144-145
535 *R v Zundel*, 1987 75 C.C.C. (3d) 449 at 144-145
536 *R v Zundel*, 1987 75 C.C.C. (3d) 449 at 144-145
537 *R v Zundel*, 1987 75 C.C.C. (3d) 449 at 144-145
538 Pattenden "Common law exceptions to the rule against hearsay" 933

Google maps. In principle, there should not be any difficulty in extending the published works exception to digital maps.

3. Dictionaries

Dictionaries are another category of published works admissible as an exception to the hearsay rule. They are admissible to show the meaning of words. This view was endorsed in *R v Peters*,[539] as reported by Pattenden. The court held that it is a well-known rule of courts of law that words should be taken to be used in their ordinary sense, and, therefore, reference must be made to dictionaries for instruction.[540] As with historical events and maps, it is submitted that dictionaries in electronic format constitute an exception to the hearsay rule as much as traditional dictionaries.

(b) Public documents

Public documents are documents prepared by public officials.[541] They are assumed to be reliable because most of them are made in circumstances of routine or of a repetitive nature, they are made by agents of the public acting under a duty; and they deal with facts of public interest or notoriety.[542] This led the common law to recognise an exception to the hearsay rule for public documents.[543] This exception is now preserved by section 7(2) of the Civil Evidence Act 1995. With the advent of ICTs, the likelihood that public documents will be in electronic format is high. For example, the following represents a sample of public documents published electronically: Statutes, Gazettes, and Public Registers.

1. Statutes

Statutes are electronically published on www.legislation.gov.uk by and under the authority of the Controller of Her Majesty's Stationary Office (HMSO) in its capacity as the Queen's Printer of Acts of Parliament and Government Printer of Northern Ireland. The HMSO is part of the National Archives and is in charge of publishing all UK legislation. The website is managed by

539 1886 16 Q.B.D. 636, 641
540 Pattenden "Common law exceptions to the rule against hearsay" 935
541 Pattenden "Common law exceptions to the rule against hearsay" 936
542 Pattenden "Common law exceptions to the rule against hearsay" 936
543 Pattenden "Common law exceptions to the rule against hearsay" 936

the National Archives on behalf of Her Majesty's Government.[544] There is no valid reason why these electronic statutes should not be admissible as evidence of facts stated in them.

2. Gazettes

The Government Gazettes of London, Edinburgh, and Belfast are admissible (and sometimes conclusive) evidence of the public matters contained therein.[545]

In common law, the Gazette is evidence of Acts of State, for example addresses to the Crown.[546] By statute, the Gazette is expressly rendered evidence of various public matters.[547] In terms of section 2 of the Documentary Evidence Act 1868 as amended by section 2 of the Documentary Evidence Act 1882, the Gazette is *prima facie* evidence of any proclamation, order, or regulation issued by Her Majesty, the Privy Council, or any of the principal departments of State.

Today the Gazette has undergone a digital transformation and is easily accessible and searchable via https://www.thegazette.co.uk . It is published by The Stationary Office (TSO)[548] on behalf of The National Archives.[549]

Nothing above appears to exclude the admissibility of Electronic Gazettes as evidence of the facts stated and provided in them, as long as they relate to matters of public interest.

3. Public Registers

In common law, public registers are admissible (but not generally conclusive) proof of the facts recorded therein, provided the book is required by law to be kept for public information or reference and the entry has been made promptly and by the proper officer.[550] By statute also, the registers and other documents kept by many public or semi-public departments or bodies are frequently accepted as *prima facie* or conclusive evidence of matters recorded in them.[551] In spite of digital transformation, entries in public registers remain valid only in paper form. In other

544 Available at http://www.legislation.gov.uk/aboutus (accessed on 26/11/2013)
545 Pattenden "Common law exceptions to the rule against hearsay" 938
546 Pattenden "Common law exceptions to the rule against hearsay" 939
547 Pattenden "Common law exceptions to the rule against hearsay" 939
548 TSO is the British publishing company that was created in 1996 when the publishing arm of HMSO was privatised
549 Available at https://www.thegazette.co.uk/all-notices/content/93 (accessed on 26/11/2013)
550 Pattenden "Common law exceptions to the rule against hearsay" 940
551 Pattenden "Common law exceptions to the rule against hearsay" 940

words, although it is possible to apply online for a certificate, such as a certificate for birth, death, or marriage, current legislation in England does not permit the register entries (certificate information) to be made available online; that can be provided only in the form of a certificate.[552]

Point (b) has discussed three categories of public documents, namely Statutes, Gazettes and Public Registers and how the electronic version of these documents may be accommodated by section 7(2) of the Civil Evidence Act 1995. After completing point (b) one may now deal with the last type of documents admissible as evidence of facts stated in them in point (c) below.

(c) Records

Records, such as treaties, Crown grants, pardons, and commissions are provable in common law by the production of the original, by exemplifications,[553] or by examined copies.[554] If it were to be assumed that some of the above documents existed in electronic format, one could argue that they should be able to benefit from the exception to the hearsay rule provided by section 7(2) (c) of the Civil Evidence Act 1995.

Besides section 7(2) (c) discussed above, another section of the Civil Evidence Act 95 calls for attention in the analysis of electronic evidence and documentary evidence, it is section 8 discussed in the following lines.

B. Section 8

Section 8 provides as follows:

(1) Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved:

(a) by the production of that document; or

(b) whether or not that document is still in existence, by the production of a copy of that document or the material part of it,

552 See http://www.gro.gov.uk/gro/content/certificates/most_customers_want_to_know.asp (accessed on 27/11/2013)

553 An exemplification, obsolete medium of proof, is a copy of the whole of a record set out either under the Great Seal, or under the seal of the court in which the record is preserved. Pattenden "Common law exceptions to the rule against hearsay" 1197

554 Pattenden "Common law exceptions to the rule against hearsay" 1213

authenticated in such manner as the court may approve.

(2) It is immaterial for this purpose how many removes there are between a copy and the original.

"Statement" is defined under this Act as any representation of fact or opinion, however made.[555] As already mentioned, "document" and "copy", on the other hand, refer respectively to anything in which information of any description is recorded and to anything onto which information recorded in the document has been copied, by whatever means and whether directly or indirectly.[556]

There is no doubt that, in terms of section 13, anything in which digital data is recorded will qualify as a document under the 1995 Act and anything onto which digital data recorded in the document has been copied will qualify as a copy under the said Act.

Since it is not always easy to determine the original as far as digital data is concerned, it is to be welcomed that section 8(1)(b) accepts proof of a statement by the production of an authenticated copy of the document. Furthermore section 8(2) makes it clear that copies of copies may be used.

Apart from sections 7(2) (c) and 8, the last section of interest in the Civil Evidence Act 1995 and relevant to the discussion of electronic evidence and documentary evidence is section 9. It is dealt with in what follows.

C. Section 9

Section 9 deals with the proof of the records of business or public authority and provides that:

(1) A document which is shown to form part of the records of a business or public authority may be received in evidence in civil proceedings without further proof.

(2) A document shall be taken to form part of the records of a business or public authority if there is produced to the court a certificate to that effect signed by an officer of the business or authority to which the records belong.

For this purpose –

(a) a document purporting to be a certificate signed by an officer of a business or public authority shall be deemed to have been duly given by such an officer and signed by him;

555 S 13
556 S 13

(b) a certificate shall be treated as signed by a person if it purports to bear a facsimile of his signature.

(3) The absence of an entry in the records of a business or public authority may be proved in civil proceedings by affidavit of an officer of the business or authority to which the records belong.

(4) In this section—

"records" means records in whatever form;

"business" includes any activity regularly carried on over a period of time, whether for profit or not, by any body (whether corporate or not) or by an individual;

"officer" includes any person occupying a responsible position in relation to the relevant activities of the business or public authority or in relation to its records; and

"public authority" includes any public or statutory undertaking, any government department and any person holding office under Her Majesty.

(5) The court may, having regard to the circumstances of the case, direct that all or any of the above provisions of this section do not apply in relation to a particular document or record, or description of documents or records.

With reference to electronic evidence this section should be interpreted as meaning that an electronic document shown to form part of the records of a business or public authority may be received without further proof. The electronic document will be taken to form part of the records of a business or public authority if a certificate to that effect signed by an officer of the business or authority to which the records belong is produced to the court. The court, however, has the discretion not to apply any of the above provisions to a particular document, such as an electronic document.[557] Whale explains that this discretion was recommended by the Law Commission as it recognised that not all business records are reliable.[558]

This concludes the discussion on the Civil Evidence Act 1995 under the section of electronic evidence and documentary evidence. The next statute discussed is the Criminal Justice Act 2003.

557 S 9(5)

558 Whale "Hearsay in Civil Proceedings" 825

3.4.1.3 The Criminal Justice Act 2003

The inclusionary approach taken by the Criminal Justice Act 2003 towards hearsay evidence has already been documented in this thesis.[559] Indeed, in terms of section 114(1) of the above Act "in criminal proceedings a statement not made in oral evidence in the proceedings is admissible as evidence of any matter stated if, but only if— (a) any provision of this Chapter[560] or any other statutory provision makes it admissible, (b) any rule of law preserved by section 118 makes it admissible, (c) all parties to the proceedings agree to it being admissible, or (d) the court is satisfied that it is in the interests of justice for it to be admissible."

Two sections are particularly relevant for documents in electronic format, namely section 117, which provides for the admissibility of documents created in the course of a trade, business, profession or other occupation, and section 118, which preserves certain common law categories of admissibility. Section 116, however, may also be mentioned.

A. Section 116

This section permits oral as well as documentary out-of-court statements of a person (X) who is unavailable[561] (but identifiable to the court's satisfaction)[562] to be introduced as evidence of any matter stated,[563] provided that, at the time of making the statement, X was a competent[564] witness and would have been allowed to give oral evidence of its contents.[565]

B. Section 117

Section 117 deals with business and other documents and reads as follows:

559 See Ch 3 par 3.3.3.3.5

560 This chapter deals with hearsay evidence

561 The reasons for the unavailability are listed in S 116(2) as follows: (a) the relevant person is dead; (b) the relevant person is unfit to be a witness because of his bodily or mental condition; (c) the relevant person is outside the United Kingdom and it is not reasonably practicable to secure his attendance; (d) the relevant person cannot be found although such steps as it is reasonably practicable to take to find him have been taken; (e) through fear the relevant person does not give (or does not continue to give) oral evidence in the proceedings, either at all or in connection with the subject matter of the statement, and the court gives leave for the statement to be given in evidence

562 S 116(1)(b)

563 S 116(1)

564 S 123

565 S 116(1)(a)

(1) In criminal proceedings a statement contained in a document is admissible as evidence of any matter stated if—

(a) oral evidence given in the proceedings would be admissible as evidence of that matter,

(b) the requirements of subsection (2) are satisfied, and

(c) the requirements of subsection (5) are satisfied, in a case where subsection (4) requires them to be.

(2) The requirements of this subsection are satisfied if—

(a) the document or the part containing the statement was created or received by a person in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office,

(b) the person who supplied the information contained in the statement (the relevant person) had or may reasonably be supposed to have had personal knowledge of the matters dealt with, and

(c) each person (if any) through whom the information was supplied from the relevant person to the person mentioned in paragraph (a) received the information in the course of a trade, business, profession or other occupation, or as the holder of a paid or unpaid office.

(3) The persons mentioned in paragraphs (a) and (b) of subsection (2) may be the same person.

(4) The additional requirements of subsection (5) must be satisfied if the statement—

(a) was prepared for the purposes of pending or contemplated criminal proceedings, or for a criminal investigation, but

(b) was not obtained pursuant to a request under section 7 of the Crime (International Co-operation) Act 2003 (c. 32) or an order under paragraph 6 of Schedule 13 to the Criminal Justice Act 1988 (c. 33) (which relate to overseas evidence).

(5) The requirements of this subsection are satisfied if—

(a) any of the five conditions mentioned in section 116(2) is satisfied (absence of relevant person etc), or

(b) the relevant person cannot reasonably be expected to have any recollection of the matters dealt with in the statement (having regard to the length of time since he supplied the information and all other circumstances).

(6) A statement is not admissible under this section if the court makes a direction to that effect under subsection (7).

(7) The court may make a direction under this subsection if satisfied that the statement's reliability as evidence for the purpose for which it is tendered is doubtful in view of—

(a) its contents,

(b) the source of the information contained in it,

(c) the way in which or the circumstances in which the information was supplied or received, or (d) the way in which or the circumstances in which the document concerned was created or received.

Analysing electronic documents with reference to section 117, it is worth noting that a statement contained in an electronic document seeking to be admitted in terms of the said section must first relate to any matter whose oral evidence given in the proceedings would be admissible as evidence of that matter.[566] Secondly, the electronic document or part of it must have been created, or received, by a person in the course of a trade business, profession, or other occupation, or as the holder of a paid or unpaid office.[567] Thirdly, the statement contained in the electronic document must have been supplied by a person who had or may reasonably be supposed to have had personal knowledge of the matters dealt with.[568] And, finally, each person (if any) through whom the information was supplied must have received the information in the course of trade, business, profession, or other occupation, or as the holder of a paid or unpaid office.[569]

566 S 117(1)(a)
567 S 117(2)(a)
568 S 117(2)(b)
569 S 117(2)(c)

An electronic document, however, prepared for the purposes of pending or contemplated criminal proceedings, or for a criminal investigation, but not obtained pursuant to a request under section 7 of the Crime (International Co-operation Act) or an order under paragraph 6 of Schedule 13 to the Criminal Justice Act 1988 must, furthermore, comply with criteria set out in subsection 5.[570]

Notwithstanding the above conditions, section 117(6) provides for the discretion to the court to refuse to admit evidence under this section. The court may, moreover, make a direction in terms of section 117(7) when there is doubt as to the statement's reliability for evidence purposes.

Brown v Secretary of State for Social Security[571] considered the older version of section 117, section 24 of the Criminal Justice Act 1988, now repealed. As reported by Mason, in this case the Secretary of the State introduced evidence of statements from computer records by way of two witnesses where the identity of the persons who supplied the information could not be ascertained.[572] It was submitted by the Secretary of the State that the statements were admissible by virtue of section 24(4) since the person who made the statement could not reasonably be expected (having regard to the time which had elapsed since he made the statement and to all the circumstances) to have any recollection of the matters dealt with in the statement. The admissibility of the two statements was opposed on behalf of the appellant for not complying with the terms of section 24.[573] The court agreed that the statements were not admissible under section 24(4) of the Criminal Justice Act 1988 as no evidence was given to suggest that the makers of the statements would have no recollection of the matters referred to in their statements.[574] In contrast, in *R v Derodra*,[575] the contents of a police "CRIS" report, a computerized record of incidents of crime, were admitted under section 24 to the delight of Mason.[576] In this case, the person who reported the case to the police could not be found to give

---

570 S 117(4). Under S 117(5) the criteria set out relate mainly to the absence of the relevant person or to the incapacity of the person to have any recollection of the matters dealt with in the statement.

571 1995 C.O.D. 260

572 Mason *Electronic Evidence* (2010) 343

573 S 24 dealt with business and other documents. It made a statement in a document admissible in criminal proceedings as evidence of any fact of which direct oral evidence would be admissible, provided certain conditions are satisfied. These conditions are similar to those of S 117 of the Criminal Justice Act 2003

574 1995 C.O.D. 260 at 262

575 2001 1 Cr App R 41

576 Mason *Electronic Evidence* (2010) 343

evidence of his complaint. The statement of that person was relied upon testimonially rather than the report of the police officer who made the relevant entry.[577]

In *R v Humphris*,[578] the Crown sought to adduce evidence of the appellant's previous convictions in terms of provisions of section 117 of the Criminal Justice Act 2003. For that purpose, they relied on a statement by an officer of the Essex Police who retrieved relevant records from the computer facility available to the Essex Police. The contents of the records were derived from various members of staff who work for the Essex Police and acted under a duty to record information and who had, or may reasonably be supposed to have had, personal knowledge of the matters stated in the records. Since all conditions for the admissibility of evidence under this section were not satisfied, the evidence could not be accepted in terms of section 117. It was, however, admissible under section 101(1)(d).[579]

C. Section 118

Section 118 provides for the preservation of certain common law categories of admissibility. The following is a selection of categories of admissibility relevant for documents in electronic format. Rules preserved in terms of section 118(1) relevant to electronic documents include *inter alia* rules relating to public information and rules relating to *res gestae*. With regard to the first category, the preservation concerns any rule of law under which in criminal proceedings: (a) published works dealing with matters of a public nature (such as histories, scientific works, dictionaries and maps) are admissible as evidence of facts of a public nature stated in them;[580] (b) public documents (such as public registers, and returns made under public authority with respect to matters of public interest) are admissible as evidence of facts stated in them;[581] (c) records (such as the records of certain courts, treaties, Crown grants, pardons and commissions) are admissible as evidence of facts stated in them.[582]

577 Mason *Electronic Evidence* (2010) 343
578 2005 EWCA Crim 2030
579 For more details, see Mason *Electronic Evidence* (2010) 344
580 S 118(1)1(a)
581 S 118(1)1(b)
582 S 118(1)1(c)

Rules relating to public information preserved by section 118 of the Criminal Justice Act 1988 were addressed under the discussion of the Civil Evidence Act 1995.[583]

In respect of the rule governing *res gestae*, section 118(1) 4 preserves it under the following terms:

> Any rule of law under which in criminal proceedings a statement is admissible as evidence of any matter stated if—
>
> > (a) the statement was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion can be disregarded,
> >
> > (b) the statement accompanied an act which can be properly evaluated as evidence only if considered in conjunction with the statement, or
> >
> > (c) the statement relates to a physical sensation or a mental state (such as intention or emotion).

Section 118(1) 4 is, according to Rosemary Pattenden, a "restatement of the common law rule that a relevant spontaneous statement made during the drama of an event is admissible in evidence to prove the matter stated provided the risk of concoction or distortion can be excluded."[584] The admissibility of spontaneous statements to prove what was said is based on the theory that an utterance "made under the immediate and uncontrolled domination of the senses and during the brief period when consideration of self-interest could not have been fully brought to bear by reasoned reflection…may be taken as particularly trustworthy (or at least lacking the usual grounds of untrustworthiness),and thus as expressing the real tenor of the speaker's belief as to the facts just observed by him."[585]

It is easily conceivable that such rule can apply in an era where technology is at the heart of human activities. More and more people tend to express their anger or frustration on social networks, such as Facebook or Twitter. There should, therefore, be no difficulty in the admission of a statement posted on these platforms as evidence of a matter stated therein if the statement

583 See Ch 3 par 3.4.1.2

584 Pattenden "Res gestae and certain other exceptions to the hearsay rule in criminal proceedings" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 877 (hereafter referred to as Pattenden "Res gestae and other exceptions to the hearsay rule") 879

585 *Wigmore on Evidence*, Charbourn rev (Boston 1976) §1747, cited by Pattenden"Res gestae and other exceptions to the hearsay rule" 879

was made by a person so emotionally overpowered by an event that the possibility of concoction or distortion could be disregarded. This can be viewed as a modern form of *res gestae*.

The admissibility and weight of electronic evidence as documentary evidence has been discussed in England through the following pieces of legislation: the Bankers' Books Evidence Act 1879; the Civil Evidence Act 1995; and the Criminal Justice Act 2003. All these statutes permit the admission of electronic evidence as a form of documentary evidence. For example the definition of "document" in terms of the Civil Evidence Act 1995 is so broad that it can easily accommodate electronic documents.[586] What is the situation in South Africa? It is discussed below.

3.4.2 South Africa

The analysis of electronic evidence with reference to documentary evidence is divided here into two parts. The first part discusses the general provisions governing the admissibility of documentary evidence in general, and the second part deals with special provisions regulating specifically the admissibility of electronic evidence. In addition, however, a brief discussion on electronic evidence as *sui generis* evidence is included.

3.4.2.1 General provisions

Under this heading the analysis focuses on the admissibility of documentary evidence under the common law and under general legislation.

3.4.2.1.1 Common law

As already mentioned, the general rule governing the admissibility of documents at common law is that three rules must be complied with for a document to be admissible in evidence. Firstly, the original must be produced, subject to exceptions. Secondly, the document must be authenticated. Finally, the document may have to be stamped in accordance with the Stamp Duties Act 77 of 1968.[587] These three rules will be discussed below.

---

586 S 13

587 Zeffertt & Paizes *The SA Law of Evidence* 828;Schwikkard & Van der Merwe *Principles of Evidence* (2002) 404; see Ch 2 par 2.2.4.3

A. Original

The general rule is that no evidence is ordinarily admissible to prove the contents of a document except the original document itself.[588] Schwikkard notes, however, that, despite the long history of the existence of this requirement, it is not always easy to identify an original document.[589] This situation is further exacerbated with regard to electronic documents. It is, indeed, very difficult to distinguish between the original electronic document and a copy of an electronic document on the face of it. Apparently the criterion used traditionally to identify the original document is by referring to the original source of recording.[590] The original document will thus be the document whose contents must be proved according to substantive law and the issues raised in the trial.[591] If the contents of a telegram, therefore, are relied on to prove the guilt of the accused, the form he filled in at the post office and not the resultant telegram constitutes the original document.[592] The original document in the case of a contract concluded by telegram, however, will depend on whether the sender or receiver is required to bear the risk of errors in transmission in terms of the substantive law.[593]

In respect of electronic documents, it was held in *S v Koralev and Another*[594] that the images found on the appellant's computer were not original images, as they had either been downloaded from the Internet or transferred from a digital camera. The original images, it was further held, would be those contained in the camera or in the original source from which they had been loaded on the Internet site.[595] In contrast, surprisingly, it was held, in *Botha v S*,[596] that the fact that many of the documents adduced in evidence by the State were computer-generated, it could not be said that the documents were not the originals.

In *Ndlovu v Minister of Correctional Services and Another*,[597] there was no objection during the course of evidence that a computer printout was not an original since it was referred to freely in

588 *Standard Merchant Bank Ltd v Creaser* 1982 4 SA 671 (W) at 674B
589 Schwikkard & Van der Merwe *Principles of Evidence* (2002) 405
590 Schwikkard & Van der Merwe *Principles of Evidence* (2002) 405
591 Zeffert & Paizes *The SA Law of Evidence* 830
592 *R v Regan* 1887 16 Cox CC 203
593 Zeffert & Paizes *The SA Law of Evidence* 830
594 2006 2 SACR 298 at 300
595 2006 2 SACR 298 at 300
596 2010 2 All SA 116 (SCA) at par 27
597 2006 4 All SA 165 (W)

cross-examination by plaintiff's counsel who raised the issue only during argument. This prompted Gautschi AJ to say that since the printout was treated as the best evidence throughout the trial, even though it may not have been, it was not open to a party to complain that a copy was not the best evidence.[598]

In light of the above cases, it must be right to say that the traditional notion of original cannot extend efficiently to electronic information. It is therefore important when dealing with electronic evidence to focus more on the functions of an original and determine whether the electronic evidence at issue satisfies such functions.[599]

B. Authenticity

As already pointed out, a party who produces a document in evidence is ordinarily required to adduce evidence to satisfy the court of its authenticity, in other words proving that the document was written or executed by the person who purports to have done so.[600] While the authenticity of traditional documents can easily be proved by calling the writer to identify the document or presenting the evidence of a person who saw him sign or write it or can identify his handwriting, establishing the authenticity of electronic documents, however, is much more complex and requires a mix of different authentication techniques, such as the electronic document's distinctive characteristics, or a process or system used to produce a result and showing that the process or the result produces an accurate result.[601] A good example of a process used to authenticate electronic documents is an electronic signature. Electronic signatures and other processes used in the authentication of electronic documents will be developed at length in chapter 4.

C. The Stamp Duties Act 77 of 1968

This Act was discussed in chapter 2 par 2.2.4.3.3. It serves no purpose to repeat here what was said there, except to stress, in respect of electronic documents, that the Act envisaged the possibility of stamping by electronic means. It stipulated that, where a person meets the requirements for the stamping of an instrument by electronic means, any electronic payment

598 *Ndlovu v Minister of Correctional Services and Another* 2006 4 All SA 165 (W) at 171

599 Ch 3 par 3.4.2.1.1 B

600 Zeffert & Paizes *The SA Law of Evidence* 837. See also Ch 2 par 2.2.4.3.2

601 See in general Goode "The Admissibility of Electronic Evidence"

made by that person may be acknowledged by means of the issue of an electronic receipt, and any such instrument which bears on its face the words "duly paid" shall for the purposes of this Act be deemed to be duly stamped to the value of that electronic receipt.[602]

The Stamp Duties Act 77 of 1968 was repealed by section 108 of the Revenue Laws Amendment Act 60 of 2008.

These common-law requirements for the admission of documents in evidence are complemented by statutory requirements which include general legislation on the one hand and special legislation on the other hand. General legislation, which follows under the heading "General provisions" is discussed below.

3.4.2.1.2 General legislation

General legislation discussed successively in the following lines include the CPEA and the CPA. The choice of these Acts is justified by the fact that they are the main statutes governing documentary evidence in South Africa.

A. The Civil Proceedings Evidence Act 25 of 1965

Parts V and VI of the CPEA regulate documentary evidence. The former deals with special provisions applicable to bankers'books, including section 28 and the latter deals with miscellaneous provisions, including section 34.

1. Part V

Section 28 provides for the admissibility of entries in bankers' books. It reads as follows:

> 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 banks, 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.

602 S 5(1)(iv)

As its English counterpart,[603] the above section provides for the admissibility of entries in bankers' books as *prima facie* evidence of information therein recorded, provided that an affidavit or other evidence certifies that the said books were the ordinary books of such bank; that the entry was made in the usual and ordinary course of business; and that the books are in, or come immediately from, the custody or control of such bank. Thus, the South African and English provisions are very similar. They differ slightly, however, in that the affidavit referred to in the South African Act must be given in writing and originates from a director, manager, or officer of the bank while in the English context proof may be given by a partner or officer of the bank orally or by an affidavit sworn before any commissioner or person authorised to take affidavits.[604]

In both countries, entries in bankers' books may be proved by examined copies.[605] While the English Act provides that proof by the person who examined the copy with the original entry may be given either orally or by an affidavit sworn before any commissioner or person authorised to take affidavits,[606] the CPEA, however, provides for proof to be given by means of an affidavit of a person who has examined the original entry, stating the fact of the examination and that the copies sought to be put in evidence are correct.[607]

Unlike England, which has adopted a specific definition of "bankers' books" and one broad enough to encompass bank records in written form or on microfilm, magnetic tape, or any other form of mechanical or electronic data retrieval mechanism,[608] South Africa does not take the same approach. In spite of this, however, section 28 is without any doubt applicable to bank electronic records, as was suggested in *Nedbank Ltd v Mashiya and Another*.[609] Hofman concurs.[610] But it will not be applicable if the bank wanting to produce the evidence is itself party to the proceedings.[611]

603 S 3 of Bankers' Books Evidence Act, 1879
604 S 4(2) of Bankers' Books Evidence Act, 1879
605 S 5(1) of Bankers' Books Evidence Act, 1879 and S 29 of the CPEA
606 S 5(2) of Bankers' Books Evidence Act, 1879
607 S 29 of the CPEA
608 S 9(2) of Bankers' Books Evidence Act, 1879
609 2006 4 SA 422 at [33]and [35]
610 Hofman "Chapter 17: South Africa" 687
611 S 32 of the CPEA.See also *Narlis v South African Bank of Athens* 1976 2 SA 573 (A)

2. Part VI

Section 34 deals with the admissibility of documentary evidence as to facts in issue and reads as follows:

(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 circumstances of the case he is satisfied that undue delay or expense would otherwise be caused, admit such 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)…

(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 recognised by him in writing as one for the accuracy of which he is responsible.

The first time the admissibility of electronic evidence came before South African courts was in terms of section 34 of the CPEA in *Narlis v South African Bank of Athens*.[612]

This case was an appeal from a decision in the Transvaal Provincial Division where the respondent (bank) successfully sued the appellant as surety and co-principal debtor in respect of an overdraft debt held to be due by the Springbok Café. The amount of the judgment was R2 000 with interest. The trial court ruled that the ledger card and account were admissible as *prima facie* evidence of the statements contained therein in terms of sections 28 and 30 of the CPEA, alternatively under the discretion vested in the trial judge in terms of section 34(2) of the CPEA.[613] On appeal, the issue was whether the bank had proved the existence of the principal debt. The bank claimed that it had granted certain overdraft facilities to the Springbok Café, that it had honoured cheques totalling R7 555,13 by 22 June 1974, that, in regard to the overdraft, the appellant on 11 January 1973 bound himself in writing as surety and co-principal debtor in the sum of R2 000, and that the appellant had failed or neglected to pay this amount notwithstanding demand.[614] The appellant denied any knowledge of the said overdraft and the alleged indebtedness of Springbok Café and put the bank to the proof thereof.[615]

At the trial in the Court *a quo* the plaintiff (respondent on appeal) called three witnesses, including a manager in the bank. The manager handed in certain ledger sheets and computerised bank statements. The question then was whether these bank documents constituted proof of their contents.

The Court *a quo* relied on section 28 of the CPEA which makes entries in bankers' books admissible in certain cases. As correctly pointed out by Holmes JA, however, the trial judge erred in doing so, as section 32 of the CPEA prevents a bank party to the proceedings from relying on that section.[616]

The learned judge also held that the ledger cards and statements were admissible as *prima facie* evidence of the contents, under the discretion vested in him in terms of section 34(2) of the

612 1976 2 SA 573 (A)
613 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 573 G
614 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 575 H
615 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 575 H
616 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 577 E and F

CPEA.[617] Holmes JA examined the validity of this ruling and held that, before discretion in terms of section 34(2) can be exercised, reference must be made to subsection 34(1) which refers only to "any statement made by a person in a document". This prompted Holmes JA to make this famous statement, "Well, a computer, perhaps fortunately, is not a person."[618] He concluded by holding that there was no basis for any discretionary admissibility of the computerised statements under section 34(2) of the Act.[619]

An interesting point raised by Holmes JA is that section 34 of the CPEA was modelled on section 1 of the English Evidence Act 1938.[620] Tapper found the definition of document which, as in the CPEA, was defined as including books, maps, plans, drawings and photographs,[621] to be the principal obstacle to the application of this legislation to computers.[622] In addition, Tapper noted, the requirements of authentication by the maker, of continuity of the record, of personal knowledge at no more than one remove, and of the necessity of calling the maker if he can be identified, in spite of the fact he might not be able to remember anything of the transaction, all militate against the application of the Act to computer-based systems.[623] Clearly this Act was not designed to cater for evidence derived from computers; it could be applied to them only with the greatest difficulty and inconvenience.[624] The English Law Reform Commission found the 1938 legislation defective in excluding many business records, particularly under modern systems of record-keeping.[625] In response, the English Civil Evidence Act 1968 was adopted and included a specific section to regulate the admissibility of evidence derived from computers.[626] The South African Law Reform Commission came to the same conclusion and found section 34 of the CPEA unsuitable for computer records for the same reasons pointed out by Tapper above and

617 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 577 G

618 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 577 H

619 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A) at 578 B

620 This Act applied to admit statements in documents as evidence, provided that the original document is produced, and provided also that the maker of the statement in the document had personal knowledge of the matters dealt with, or that the document is part of a continuous record made by a person with a duty to record a statement made by someone with personal knowledge, and provided that the maker is called as a witness, subject to various reasons for non-appearance. See Tapper *Computer Law* 383

621 S 6(1) of the Evidence Act 1938; Tapper *Computer Law* 383

622 S 6(1) of the Evidence Act 1938; Tapper *Computer Law* 383

623 Tapper *Computer Law* 383-384

624 Tapper *Computer Law* 384

625 The Law Reform Committee 13th report par 16(a) cited by Tapper *Computer Law* 384

626 See Ch 3 par 3.3.3.3.2

recommended specific legislation with regard to this matter.[627] This followed in the shape of the Computer Evidence Act 57 of 1983.[628]

The weight to be attached to evidence admissible under this part is regulated by section 35 as follows:

> (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 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 the 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.

B. The Criminal Procedure Act 51 of 1977

Three sections in the CPA call for close scrutiny: sections 221,222 and 236.

1. Section 221

Section 221 deals with the admissibility of certain trade or business records and reads as follows:

> (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

627 Van der Merwe "Documentary evidence (with specific reference to hearsay)" 1994 *Obiter* (hereafter referred to as Van der Merwe "Documentary evidence") 80

628 This Act is discussed below in Ch 3 par 3.4.2.1.3. A

(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.

This section differs from its civil counterpart in a certain number of aspects. Firstly, it is interesting to note that section 221(1) of the CPA refers to "any statement contained in a document" whereas section 34(1) of the CPEA refers to "any statement made by a person in a document". The admissibility of trade or business records without the requirement that the statement be made by a person under section 221(1) of the CPA means that, if it were to be applied in the *Narlis* case,[629] it would have excluded the whole argument against the admission of electronic evidence, expressed in that case by Holmes JA in the following terms, "Well, a computer, perhaps fortunately, is not a person." There is therefore a need to harmonise these definitions. Secondly, unlike section 34(1)(a)(ii), a document in terms of the CPA is not required to form part of a continuous record; it needs merely to be a trade or business record or a part of it.[630] Thirdly, section 221 does not require the record to be compiled by a person who had personal knowledge of the matters dealt with in the information. What is required is personal knowledge by the person who supplied that information.[631]

A number of cases have considered section 221 while dealing with electronic evidence. The following provides an overview of these cases.

S v Harper and Another [632] considered the admissibility of computer printouts in terms of section 221 of the CPA. In the process, it dealt with the meaning of document in terms of subsection 221(5). For the purposes of section 221, "document" is defined as including any device by means of which information is recorded or stored.[633] Reflecting on the question of knowing whether a computer fell under the above extended definition of document, Milne J pointed out that the computers in that case do not fall within the definition of "document" under section 221(5) as

629 *Narlis v South African Bank of Athens* 1976 2 SA 573 (A)
630 *S v Ndiki and Others*, 2007 2 All SA 185 (Ck) at par 50
631 *S v Ndiki and Others*, 2007 2 All SA 185 (Ck) at par 51
632 1981 1 SA 88 (D)
633 S 221(5)

they do more than recording and storing information; they, in addition, *inter alia*, sort and collate information and make adjustments.[634] He held that the extended definition of "document" is clearly not wide enough to cover a computer, at any rate where the operations carried out by it are more than the mere storage or recording of information.[635] He went on to say that, if a computer were a document as envisaged in section 221(5), how would it be produced as section 221(1) does not refer to the product of the device, nor to any document produced by the device, but refers to the document itself being produced?[636] He further noted that the wording of the section, read with the extended definition contained in subsection (5), is entirely appropriate to the production of microfilm as evidence since the microfilm itself can be produced.[637] More than thirty years after this case and the stage of the development of technology humankind finds itself in, however, the second argument of Milne J can be discarded easily as it is now possible to produce a computer as this device has become easier to carry. With regard to the first argument that a computer must not do more than the mere storage or recording of information, with the sophistication of computers nowadays it is unlikely than one finds computers today that satisfy the extended definition of subsection (5). Commenting on the exclusion of a computer which does more than the mere storage and recording of information from the subsection (5) definition, Hofman submits that "if a data message is excluded from the definition of a document made by a person on the grounds that the information in the data message has been processed, few data messages would nowadays be admissible."[638] He suggests as a better view to make data messages of any sort admissible provided they comply with the requirements of subsection (1).[639] What Hofman seems to have missed, however, is that Milner J's contention on that specific point refers only to the fact that a computer does not fall within the extended definition of "document" in subsection (5) when it does more than the storage or recording of information, which in effect will exclude most of modern computers. Milner at that stage did not deal with data messages or product of computers.

The next question dealt with by Milner J was whether or not a computer printout is a document within the ordinary grammatical meaning of the word. He held that the computer printouts

634 *S v Harper and Another* 1981 1 SA 88 (D) at 95 D
635 *S v Harper and Another* 1981 1 SA 88 (D) at 95 F
636 *S v Harper and Another* 1981 1 SA 88 (D) at 95 H
637 *S v Harper and Another* 1981 1 SA 88 (D) at 95 H
638 Hofman "Chapter 17: South Africa" 687
639 Hofman "Chapter 17: South Africa" 687

consist of typed words and figures and would, *prima facie*, clearly fall within the ordinary meaning of the word "document". [640] Computer printouts are, therefore, admissible in terms of section 221.[641]

The conclusion of Milne J was endorsed by O'linn J and Teek J in *S v De Villiers*.[642] This is a Namibian case which dealt with the admissibility of, amongst other things, computer printouts in terms of section 221 of the CPA which was then applicable in Namibia. The appellant appeared before a regional court magistrate on various charges of fraud and theft, was acquitted on all charges of fraud, and found guilty on the count of theft. He appealed against his conviction and sentence on amongst other grounds that the honourable magistrate erred in deciding that the evidence regarding computer printouts of bank statements is admissible evidence.[643] The defence in the court *a quo* as well as on appeal relied strongly on the alleged inadmissibility of the bank statements on the authority of *S v Harper and Another* 1981 1 SA 88 (D) and a passage in Hoffman and Zeffertt *South African Law of Evidence* 4th ed where the learned authors, relying on the decision in the *Harper* case (95 H), held that a computer printout produced by a computer that sorted and collated information would be inadmissible.[644] O'linn J correctly noted that the learned authors had misread the *dictum* of Milne J who had instead said that computer printouts are documents as contemplated by section 221 and are admissible.[645] O'linn J fully agreed with the approach of Milne J and held that the computer printouts before the court, certified as authentic, were in fact duplicate originals and admissible in evidence.[646]

The decision in *S v Harper and Another* [647] was also applied in *S v Mashiyi and Another*.[648] The latter case concerned the admissibility of a large number of computer-generated documents. Some documents were disputed, while others were not. The first category was disputed on the basis that information it contained did not only reflect the information supplied to the computer

640 *S v Harper and Another* 1981 1 SA 88 (D) at 96 D

641 *S v Harper and Another* 1981 1 SA 88 (D) at 97 H

642 1993 1 SACR 574 (Nm)

643 *S v De Villiers* 1993 1 SACR 574 (Nm) at 575 h

644 *S v De Villiers*1993 1 SACR 574 (Nm) at 577 f-h

645 *S v De Villiers* 1993 1 SACR 574 (Nm) at 577 h-j.It should be noted that this mistake was later acknowledged by the learned authors (at least Zeffertt, since Hoffmann was no longer involved in the future versions of the book) who said with Paizes that" a computer print-out produced by a computer that sorted and collated information *would* be admissible under this section." Zeffert & Paizes *The SA Law of Evidence* 430

646 *S v De Villiers* 1993 1 SACR 574 (Nm) at 579 d

647 1981 1 SA 88 (D)

648 2002 2 SACR 387

at the input stage, it also reflected information which had been created and calculated by the computer itself. The output contained in the printouts was not the same as the information that had been fed into the computer.[649] Miller J was correct in holding, on the authority of *Harper*'s case,[650] that the computers in this instance did not satisfy the definition of "document" under subsection (5) as they did more than the mere recording and storing of information.[651] He did not, however, consider the possibility of admitting the computer printouts as documents in the ordinary meaning of the word "document" in accordance with *Harper*'s case.[652] He ruled rather that documents which contain information that has been processed and generated by computers are not admissible as evidence in a criminal trial.[653] On the other hand, he held that documents which have been scanned to produce an electronic image of the original, such that the image is an exact image, are admissible.[654]

In *S v Ndiki and Others*,[655] Van Zyl J was satisfied that a computer printout produced by a computer that sorted and collated information would be admissible under section 221 if the foundation requirements thereof have been satisfied.[656] The printouts in the present case were held to be documents within the ordinary meaning of that word.[657]

2. Section 222

Section 222 provides as follows:

> 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.

The provisions referred to in section 222 have been analysed above in greater depth.[658]

649 *S v Mashiyi and Another* 2002 2 SACR 387 at 391 i
650 *S v Harper and Another* 1981 1 SA 88 (D)
651 *S v Mashiyi and Another* 2002 2 SACR 387 at 392 a
652 *S v Harper and Another* 1981 1 SA 88 (D)
653 *S v Mashiyi and Another* 2002 2 SACR 387 at 387 j
654 *S v Mashiyi and Another* 2002 2 SACR 387 at 388 a
655 2007 2 All SA 185 (Ck)
656 *S v Ndiki and Others* 2007 2 All SA 185 (Ck) at 199 par [50]
657 *S v Ndiki and Others* 2007 2 All SA 185 (Ck) at 199 par [50]
658 Ch 3 par 3.4.2.1.2 A

3. Section 236

Section 236 deals with the proof of entries in accounting records and documentation of banks, and it provides as follows:

> (1) The entries in the accounting records of a bank, and any document which is the possession of any bank and which refers to the said entries or to any business transaction of the bank, 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 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 of 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) 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.

(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 print-out 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.

The provisions of section 236 are similar to the provisions relating to bankers' books in terms of the CPEA.[659] It is, furthermore, submitted that, in view of the definition of document in subsection (5), these provisions will apply to banking records in the form of a data message.[660]

Section 236A extends the ambit of section 236 to entries in accounting records and documents of banks in foreign countries which are "similar" to banks in South Africa.[661]

After discussing general legislation dealing with documentary evidence, one can now deal with special legislation governing electronic evidence specifically. It includes the Computer Evidence Act 57 of 1983 and the ECT Act. These statutes are successively discussed below.

3.4.2.2 Special provisions

Provisions discussed under this heading include the provisions contained in special legislation such as the Computer Evidence Act 57 of 1983 and the ECT Act.

A. The Computer Evidence Act 57 of 1983

As already noted, the Computer Evidence Act was enacted as a result of the outcome of the *Narlis* case.[662] This Act provided for the admissibility in civil proceedings of evidence generated by computers, and for matters connected therewith.

---

659 S 28 in particular analysed at Ch 3 par 3.4.2.1.2 A

660 Hofman "Chapter 17: South Africa" 688

661 Zeffert & Paizes *The SA Law of Evidence* 437

662 *Narlis v South African Bank of Athens* 1976(2) SA 573(A).For more details on the analysis of this case see Ch 3 par 3.4.2.1.2 A

Section 3 dealt with the admissibility of authenticated computer printouts and provided as follows:

> (1) In any civil proceedings an authenticated computer print-out shall be admissible on its production as evidence of any fact recorded in it of which direct oral evidence would be admissible.
>
> (2) It shall suffice for the purposes of subsection (1) if an affidavit which accompanies the computer print-out in question as contemplated in the definition of "authenticated computer print-out" in section 1 (1), on the face of it complies with the provisions of section 2 which apply to an affidavit of the nature in question.

The evidential weight of authenticated computer printouts was regulated in terms of section 4 which stated that:

> (1) An authenticated computer print-out shall have the evidential weight which the court in all the circumstances of the case attaches to it.
>
> (2) In order to assess the evidential weight of an authenticated computer print-out, the court may-
>
> (a) take account of anything contained in the authenticating affidavit or a supplementary affidavit;
>
> (b) on the application of any party to the proceedings require the deponent to the authenticating affidavit or a supplementary affidavit or any other person to testify orally on any topic relevant to such question, whether or not any such affidavit covered it.

The terms and phrases below were defined under section 1 (1) of this Act as follows:

> 'authenticated computer print-out' means a computer print-out accompanied by the authenticating affidavit which relates to it and by such supplementary affidavit or affidavits as may be required by section 2 in connection with the authenticating affidavit;
>
> 'authenticating affidavit' means an affidavit which authenticates a computer print-out in compliance with section 2;

'computer' means any device or apparatus, whether commonly called a computer or not, which by electronic, electro-mechanical, mechanical or other means is capable of receiving or absorbing data and instructions supplied to it, of processing such data according to mathematical or logical rules and in compliance with such instructions, of storing such data before or after such processing, and of producing information derived from such data as a result of such processing;

'computer print-out' means the documentary form in which information is produced by a computer or a copy or reproduction of it, and includes, whenever any information needs to be transcribed, translated or interpreted after its production by the computer in order that it may take a documentary form and be intelligible to the court, a transcription, translation or interpretation of it which is calculated to have that effect;

'information' includes any information expressed in or conveyed by letters, figures, characters, symbols, marks, perforations, patterns, pictures, diagrams, sounds or any other visible, audible or perceptible signals;

'processing' includes treating or, as the context may require, treatment by calculation, compilation, arrangement, sorting, comparison, analysis, synthesis, classification, selection, summarizing or consolidation;

'supplementary affidavit' means a supplementary affidavit required by section 2 (4) (b) or an affidavit which supplements an authenticating affidavit in compliance with section 2 (7).

Subsection (2), with reference to a combination or sequence of computers, provided for the following:

Whenever separate devices or apparatuses have been operated in combination or sequence to perform the functions of a computer, as described in the definition of 'computer' in subsection (1), such combination or sequence of devices or apparatuses shall be regarded for the purposes of this Act as a single computer.

The procedure for the authentication of computer printouts and safeguards with regard to the accuracy of the facts to which the printouts deposed was provided under section 2 as follows:

(1) Subject to the other provisions of this section, a computer print-out may be authenticated for the purposes of this Act by means of an affidavit which shall-

(a) identify the computer print-out in question and confirm that it is a computer print-out as defined in this Act which has been produced by a computer as likewise defined;

(b) identify such copy, reproduction, transcription, translation or interpretation of information produced by the computer as the computer print-out may comprise or contain, and confirm that it is a true copy, reproduction, transcription, translation or interpretation of such information;

(c) describe in general terms the nature, extent and sources of the data and instructions supplied to the computer, and the purpose and effect of the processing of the data by the computer;

(d) certify that the computer was-

(i) correctly and completely supplied with data and instructions appropriate to and sufficient for the purpose for which the information recorded in the computer print-out was produced;

(ii) unaffected in its operation by any malfunction, interference, disturbance or interruption which might have had a bearing on such information or its reliability;

(e) certify that no reason exists to doubt or suspect the truth or reliability of any information recorded in or result reflected by the computer print-out.

The Act also required that the authenticating affidavit be given by some person who is qualified to give the testimony it contains by reason of (a) his knowledge and experience of computers and of the particular system by which the computer in question was operated at all relevant times, and (b) his examination of all relevant records and facts which are to be made available concerning the operation of the computer and the data and instructions supplied to it.[663]

According to Van der Merwe, reaction to the Computer Evidence was overwhelmingly negative.[664] He pointed out that French,[665] Skeen,[666] Steele,[667] Delport,[668] Ebden,[669] and he

663 S 2(3)

664 Van der Merwe *Information and Communications Technology Law* (2016) 112

665 "The admissibility of computer records in the SA law of evidence – a comparative survey" 1982-1983 *Natal University Law Review* 123

666 "Evidence and computers" 1984 *SALJ* 675

667 "Computer-produced print-out reliable as evidence" 1983 *SALJ* 510

668 "Die Wet op Rekenaargetuienis" 1983 *Obiter* 140

669 "Computer evidence in court" 1985 *SALJ* 687

himself,[670] amongst others, published comment critical of the legislation.[671] French feared to get into a situation where it becomes difficult to find a person who qualifies to make the "authenticating affidavit".[672] Skeen, with reference to the contents of the affidavit as prescribed by section 2 of the Act, mentioned that errors in the output of a computer could develop in a number of ways and be caused by unrelated factors such as faulty air-conditioning and changes in voltage. He further noted that some faults could develop only when particular software is interacting with particular hardware, making it impossible for anyone to certify that "the computer was unaffected by any malfunction, interference, disturbance or interruption which might have had a bearing on such information or its reliability" as required by section 2(1)(d)(ii), especially when the guarantee has to cover a fair span of time.[673] Steele felt that, whereas it might be appropriate for the physical printout merely to be identified by means of an affidavit "it certainly seems inappropriate for the accuracy and reliability of its contents to be authenticated by this means".[674] Van der Merwe reported that Delport's criticism was even harsher, as this learned author, after analysing the Act with a fine-tooth comb, found confusion. He expressed the view that the legislator should have concentrated on the authenticity of the information contained in the affidavit rather than focusing too much on the technically interpreted "print-out", which was the only way to adduce evidence in court.[675] The most cogent criticism of the Act, according to Van der Merwe, was expressed by a computer scientist, Ebden, who asked, "When your house is not in order, do you put it in order, or do you change the law so as to define it as being in order? It is remarkable that the draftsmen of the new legislation appear to have ignored an avalanche of evidence that the house of computing is not necessary in order".[676]

In *Ex Parte Rosch*,[677] although neither of the respondents placed any reliance on the Computer Evidence Act as a basis for the admissibility of computer printouts, the court considered whether these printouts were excluded by the above Act, and it held that "the statute does not require that

670 "Documentary evidence"
671 Van der Merwe *Information and Communications Technology Law* (2016) 112
672 Van der Merwe *Computers and the Law* 1986 123
673 Van der Merwe *Computers and the Law* 1986 123
674 Van der Merwe *Computers and the Law* 1986 124
675 Van der Merwe *Computers and the Law* 1986 124
676 Van der Merwe *Computers and the Law* 1986 124
677 1998 1 All SA 319 (W)

whatever is retrieved from a computer can only be used if the statute's requirements have been met. It is a facilitating Act not a restricting one".[678]

In contrast, in *S v Mashiyi and Another*,[679] it was held that the Computer Evidence Act did not overcome problems relating to the admissibility of computer printouts in terms of section 34 of the CPEA, as held in the *Narlis* case.[680] Its repeal by the ECT Act was, therefore, welcomed. The ECT Act is discussed below.

B. The Electronic Communications and Transactions Act 25 of 2002

This Act constitutes a landmark statute as it made a huge step forward from the Computer Evidence Act by introducing the concept of intangible "data messages". It, therefore, moved away from the idea of paper and computer printouts to embrace the digital transformation. Evidence in the form of data messages can, thus, be produced in court by means of an output device other than paper. As the ECT Act emanates from the UNCITRAL Model Law on Electronic Commerce, it seems appropriate first to examine this instrument before dealing with the ECT Act *per se*.

1. The UNCITRAL Model Law on Electronic Commerce

This Model Law was adopted by the UN General Assembly Resolution 15/162 of 16 December 1996. It applies to any kind of information in the form of a data message used in the context of commercial activities.[681] Nothing in the Model Law should, however, prevent an enacting State from extending the scope of the Model Law to cover uses of electronic commerce outside the commercial sphere.[682]

Article 5 deals with the legal recognition of data messages, and it provides that information shall not be denied legal effect, validity, or enforceability solely on the grounds that it is in the form of a data message. In other words, article 5 means that the form in which certain information is

678 *Ex Parte Rosch* 1998 1 All SA 319 (W) at 327 h
679 2002 2 SACR 387
680 *S v Mashiyi and Another* 2002 2 SACR 387 at 390 f-g
681 Art 1 sphere of application
682 Par 26 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity, or enforceability.[683] This does not, however, mean that article 5 should be interpreted as establishing the legal validity of any given data message or of any information contained therein.[684]

Article 9 is the heart of the Model Law on Electronic Commerce as far as the admissibility and the evidential weight of data messages are concerned. It provides as follows:

> (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is 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 shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

The purpose of article 9 is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value. The drafters of the Model Law felt it necessary to establish expressly that data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form because the admissibility of evidence is an area which can give rise to particularly complex issues in certain jurisdictions.[685]

As regards the assessment of the evidential weight of a data message, paragraph (2) provides useful guidance as to how the evidential value of data messages should be assessed (e.g., depending on whether they were generated, stored, or communicated in a reliable manner).[686]

It is worthwhile noting that the Model Law defines a "data message" as meaning information generated, sent, received, or stored by electronic, optical, or similar means including, but not

683 Par 46 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
684 Par 46 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
685 Par 70 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
686 Par 71 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

limited to, electronic data interchange (EDI), electronic mail, telegram, telex, or telecopy.[687] EDI, on the other hand, is defined as meaning the electronic transfer from computer to computer of information using an agreed standard to structure the information.[688]

The notion of "data message" in terms of the Model Law is not limited to communication, but it also intends to encompass computer-generated records that are not intended for communication. Thus, the notion of "data message" includes the notion of "record".[689]

The reference to "similar means" in the definition of "data message" indicates that the Model Law should not be restricted to existing communication techniques; rather, it must be able to accommodate foreseeable technical developments.[690] The aim of the definition is, thus, to include all types of messages that are generated, stored, or communicated in essentially paperless form.[691]

2. Chapter III of the ECT Act

Chapter III of the ECT Act aims at facilitating electronic transactions in South Africa. It provides for various legal requirements for data messages,[692] including the legal recognition of data messages,[693] the requirement in law of writing,[694] of signature,[695] of original,[696] and the admissibility and evidential weight of data messages.[697]

(a) Legal recognition of data messages

Data messages are given legal recognition by section 11(1) which provides that information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of

687 Art 2(a)
688 Art 2(b)
689 Par 30 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
690 Par 31 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
691 Par 31 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
692 Part 1
693 S 11
694 S 12
695 S 13
696 S 14
697 S 15

a data message. This subsection is based on article 5 of the Model Law on E-commerce and should be interpreted in the same way.[698]

(b) Writing

Section 12 provides with regard to writing 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.

Section 12 originates from article 6(1) of the Model Law on E-commerce which, like section 12, defines the basic standard to be met by a data message in order to be considered as meeting a requirement in law that information be retained or presented "in writing".[699]

During the preparation of the Model Law on E-commerce, different functions traditionally performed by writings in a paper-based environment were considered, and the following non-exhaustive list was identified: "(1) to ensure that there would be tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) to help the parties be aware of the consequences of their entering into a contract; (3) to provide that a document would be legible by all; (4) to provide that a document would remain unaltered over time and provide a permanent record of a transaction; (5) to allow for the reproduction of a document so that each party would hold a copy of the same data; (6) to allow for the authentication of data by means of a signature; (7) to provide that a document would be in a form acceptable to public authorities and courts; (8) to finalise the intent of the author of the 'writing' and provide a record of that intent; (9) to allow for the easy storage of data in a tangible form; (10) to facilitate control and

698 See Ch 3 par 3.4.2.1.3 B 1. Hofman recommends an interpretation of Ch III of the ECT Act consistent with the Model Law on E-commerce in compliance with S 233 of the Constitution which provides that a South African court interpreting any South African legislation "must prefer any reasonable interpretation of the legislation that is consistent with international law".Hofman "Chapter 17: South Africa" 678.See also Dunlop "Chapter 20: South Africa" in Campbell (ed) *E-Commerce and the Law of Digital Signatures* 2005 (hereafter referred to as Dunlop "Chapter 20: South Africa") 563

699 Par 47 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

subsequent audit for accounting, tax or regulatory purposes; and (11) to bring legal rights and obligations into existence in those cases where a 'writing' was required for validity purposes."[700]

Article 6 does not intend to establish a requirement that, in all instances, data messages should fulfil all the conceivable functions of a "writing", but, rather, to guarantee that the information can be reproduced and read.[701] Indeed, existing requirements for data to be presented in written form often associate the requirement of a "writing" with concepts distinct from writing, such as signature and original. The requirement for data to be presented in written form ("threshold requirement") should, thus, be clearly distinguished from more stringent requirements such as "signed writing", "signed original" or "authenticated legal act".[702]

In *Mafika v SABC Ltd,*[703] the court considered whether a short message service (SMS) message was a"writing" in terms of the ECT Act. The court held that an SMS satisfies the requirement of writing in terms of the ECT Act as it is a data message and is capable of being saved on a cellphone and retrieved.[704]

An SMS message was also considered in *Jafta v Ezemvelo KZN Wildlife,*[705] where the following questions were raised: Does acceptance of an offer of employment sent by e-mail or SMS result in a valid contract? When is an acceptance of an offer sent by e-mail or SMS received? Is an SMS an electronic communication? What is an electronic communication?[706] To answer these questions, the court looked to the ECT Act, the Model Law on E-commerce, and foreign law.[707] Although an SMS is not defined by the ECT Act, the court accepted that an SMS was a data message and, in consequence, communication by means of SMS falls within the ambit of electronic communication in terms of the ECT Act.[708] In addition, the court held that acceptance [of an offer] by SMS was not without legal force and effect merely on the grounds that it was in

700 Par 48 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
701 Par 50 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
702 Par 49 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
703 2010 5 BLLR 542 (LC)
704 *Mafika v SABC Ltd* 2010 5 BLLR 542 (LC) at [18].See also Meintjes- Van der Walt "Electronic Evidence" in Papadopoulos and Snail (ed) *Cyberlaw@ SA III, The Law of the Internet in South Africa* 2012 (hereafter referred to as Meintjes- Van der Walt "Electronic Evidence") 320
705 2008 10 BLLR 954 (LC)
706 *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) at 956 [1]
707 *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) at 956 [1]
708 *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) at 975 [112]

the form of an SMS. The court further held that an SMS is as effective a mode of communication as an e-mail or a written document.[709]

Section 12 of the ECT Act was also discussed in the more recent case of *Spring Forest Trading v Wilberry*.[710] In fact the Court and all parties agreed that a requirement for a cancellation to be in writing in terms of a non-variation clause in a contract could be satisfied by an email.[711] However, the dispute was on whether the signature used was valid.[712]

(c) Signature

In terms of section 13(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. According to subsection (1) where the law requires the signature of a person without specifying the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.[713] Where an advanced electronic signature has been used, such a signature is regarded as being a valid electronic signature and to have been applied properly, unless the contrary is proved.[714]

Electronic signatures will be discussed at length and in much detail in chapter 4 which deals with the challenges and responses to electronic evidence.

(d) Original

Section 14 provides the following with regards to the original:

709 *Jafta v Ezemvelo KZN Wildlife* 2008 10 BLLR 954 (LC) at 976 [113]

710 (725/13) [2014] ZASCA 178

711 Spring Forest Trading v Wilberry (725/13) [2014] ZASCA 178 at [17]

712 Spring Forest Trading v Wilberry (725/13) [2014] ZASCA 178 at [17]; for a discussion on this aspect, see Ch 4 par 4.3.2.3.1

713 S 13(1).This requirement is more stringent than the Model Law on E-commerce which provides under art 7(1) that where the law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. If the signature is, however, required by the parties to an electronic transaction without specifying the type, then the above method described by art 7(1) of the Model Law on E-commerce will be applicable as specified by S13(3) of the ECT Act.

714 S 13(4)

(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.

Like article 8 of the Model Law on E-commerce, section 14 of the ECT Act requires two conditions for information to be considered in original form. Firstly, there must be a guarantee of integrity and, secondly, the information must be capable of being displayed or produced to the person to whom it is to be presented. Both article 8 and section 14 clearly deviate from the traditional meaning of "original" defined as a medium on which information was fixed for the first time, and they prefer a functional equivalent of originality; indeed, if the traditional definition of "original" was retained, it would be impossible to say that a data message is in original form, since the recipient of a data message would always receive a copy thereof.[715] The notion of "original" as envisaged in article 8 and section 14 is, thus, useful in overcoming the requirement for the presentation of originals which constitutes one of the main obstacles that the Model Law attempted to remove in promoting e-commerce.[716] In addition there exists different technical means able to certify the contents of a data message and thus confirm its "originality".[717] Meintjes-Van der Walt suggests as a means of proving the integrity of data messages to establish a chain of custody by way, for example, of demonstrating the existence of established company policies regarding electronic storage and restricted access, the use of

715 Par 62 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
716 Par 62 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
717 Par 63 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

devices that limit access through passwords and encoding and entry logs indicating when and by whom documents have been accessed or changed.[718]

S v Koralev and Another,[719] *Botha v S,*[720] and *Ndlovu v Minister of Correctional Services and Another,*[721] have dealt in one way or another with the originality of electronic documents.[722]

(e) Admissibility and evidential weight of data messages

(i) Section 15

The provisions relating to the admissibility and evidential weight of data messages are set by section 15 as follows:

> (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.

---

718 Meintjes- Van der Walt "Electronic Evidence" 322

719 2006 2 SACR 298

720 2010 2 All SA 116 (SCA)

721 2006 4 All SA 165 (W)

722 For more details see Ch 3 par 3.4.2.1.1 A

> (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.

As article 9 of the Model Law on E-commerce, section 15(1) provides expressly that data messages should not be denied admissibility as evidence in legal proceedings on the sole grounds that they are in electronic form. It does not, however, make every data message admissible, as data message are subject to normal rules of evidence[723] which can exclude evidence from admissibility on other grounds such as that the evidence is hearsay or is not relevant or in original form. With regard to original, section 15(1)(b) exempts data messages from the requirement of original form if the data message is the best evidence that the person adducing it could reasonably be expected to obtain.

Hofman notes that it is possible to argue, on various grounds,[724] that the ECT Act makes all data messages admissible.[725] He gives three reasons for rejecting this position at the present state of the South African law of evidence: "first, it would go against the functional equivalence between data messages and documents by treating their evidential value differently because not all documents are admissible; second, it will go beyond the purpose of the ECT Act which is to regulate electronic commerce and not reform the law of evidence; and third, it would attribute to Parliament the intention to use detail buried in the ECT Act to bypass the wider debate about the admissibility of documentary evidence."[726] Hofman is further correct in expressing the view that, except where the ECT Act changes it, the ordinary South African law on the admissibility of evidence applies to data messages,[727] as agreed by Gautschi AJ in *Ndlovu v Minister of*

---

723 S 3 of the ECT Act provides that the ECT 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.The wording of S 15(1) supports S 3 by stating that the [normal] rules of evidence must not be applied so as to exclude data messages in evidence.

724 For example from the differences between the wording of S 15(3) and (4) and art 9 of the Model Law on E-commerce or from the argument that the definition of data message in the ECT Act makes hearsay data messages admissible.Hofman "Chapter 17: South Africa" 682 (references). For the discussion on the hearsay nature of data messages, see Ch 3 par 3.3.2.3.4

725 Hofman "Chapter 17: South Africa" 681

726 Hofman "Chapter 17: South Africa" 682-683

727 Hofman "Chapter 17: South Africa" 682

Correctional Services and Another.[728] Data messages, depending on the circumstances, can, thus, be the functional equivalent of either documentary evidence or real evidence.[729]

(ii) Data messages as the functional equivalent of documents

Data messages as the functional equivalent of documents, except where the ECT Act exempts them, must satisfy the following requirements for the admissibility of documents under the South African law of evidence, production, original form, authenticity, the provisions of the Stamp Duties Act (repealed).These rules deal only with the situation where evidence is adduced to prove the content of a document, and not whether statements of fact in a document can be used to prove that those facts are true.[730]

The rules regulating the presentation and admission of documents vary depending on the (public or private) nature of the document in question.[731] Public documents are not subject to the above requirements while private documents are.

- **Public documents**

A public document is a document made by a public officer in the execution of a public duty, which is intended for public use and to which the public has a right of access.[732] Official documents usually require the signature or seal of an official.[733] The ECT Act provides for the electronic notarisation, certification, and sealing of data messages.[734]

Section 18 reads as follows:

> (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

728 2006 4 All SA 165 (W)

729 Hofman "Chapter 17: South Africa" 682.Data messages (or electronic evidence in general) as real evidence were discussed in Ch 3 par 3.2

730 Watney "Admissibility of electronic evidence in criminal proceedings: an outline of the South African legal position" 2009 *JILT* 1 (hereafter referred to as Watney "Admissibility of electronic evidence in criminal proceedings") 6; read also De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" 558

731 Watney "Admissibility of electronic evidence in criminal proceedings" 5

732 Watney "Admissibility of electronic evidence in criminal proceedings" 5

733 Watney "Admissibility of electronic evidence in criminal proceedings" 5

734 S 18 and S 19(3)

> 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.

In addition, section 19(3) provides as follows:

> 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.

- **Private documents**

A private document is a document that is not a public document.[735] Most documents, including data messages, will fall under this category, and they will need to comply with the requirements listed above to be admissible in evidence, namely production, original form, authenticity and the provisions of the Stamp Duties Act. These will be discussed below.

(1) Production

To qualify as evidence, a document must be produced.[736] When applying this rule to data messages, it needs to be stressed that given the fact that human senses cannot directly perceive the electronic signals that make up a data message, a data message can be produced as evidence only by using an output device such as computer screen, printer, or data projector.[737] Questions

735 Watney "Admissibility of electronic evidence in criminal proceedings" 5
736 Hofman "Chapter 17: South Africa" 682
737 Hofman "Chapter 17: South Africa" 682

about the reliability of a particular output device may be raised;[738] Hofman suggests they be dealt with as part of the process of production, while questions requiring the testimony of a witness be dealt with as part of the process of authentication.[739]

Section 17 of the ECT Act allows for production in electronic form and reads as follows:

> (1) Subject to section 28,[[740]] 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.

(2) The original form

The rule that no document is ordinarily admissible to prove the contents of a document except the original document itself has been mentioned more than once in this thesis.[741] It applies to

738 These questions will be addressed in Ch 4 and 5 below

739 Hofman "Chapter 17: South Africa" 682

740 S 28 of the ECT Act deals with the requirements that may be specified for e-government services, such as the filing and the issuing of documents. This section will be dealt with in more detail below in Ch 5.

741 See Ch 2 par 2.2.4.3.1 and Ch 3 par 3.4.2.1.1 A and par 3.4.2.1.3 B 2 (d)

data messages which will satisfy the requirements of original form if they meet the conditions in section 14 of the ECT Act.[742]

(3) Authenticity

The rule in respect of authenticity has been stressed many times in this thesis.[743] It provides that anyone who wants to use a document as evidence must satisfy the court that it is authentic, that the document is what it claims to be.[744] The authenticity of electronic evidence, more than any other evidence, must be proved because of the high degree of volatility of this type of evidence. Indeed electronic evidence can easily be manipulated, altered, or damaged after its creation.[745] Meintjes-Van der Walt reports that, according to Mason, "the authenticity of a digital object is preserved by the use of techniques to prevent the data from being manipulated, altered or falsified deliberately or inadvertently. Such methods include proving audit trails of transmissions and maintaining records of encryption. A number of attributes, taken together, provide evidence of authenticity: the mode, status and form of transmission together with the way in which the data is preserved and it is managed."[746] The techniques and other methods used to prove the authenticity of electronic evidence are discussed at length in chapter 4 below.

In the meantime, it is important to stress that section 15(4) of the ECT Act provides for authenticating a data message made in the course of business by certificate. No general exemption for data messages from this rule is, however, created by the ECT Act.[747]

Section 15(4) of the ECT Act was interpreted in both *Trend Finance (Pty) Ltd and another v Commissioner for SARS and another*,[748] and *Ndlovu v Minister of Correctional Services and another*.[749] These two cases are discussed in detail above.[750]

---

742 For a discussion on S 14 of the ECT Act see Ch 3 par 3.4.2.1.3 B 2 (d)

743 See Ch 2 par 2.2.4.3.2 and Ch 3 par 3.4.2.1.1 B

744 Hofman "Chapter 17: South Africa" 683

745 Watney "Admissibility of electronic evidence in criminal proceedings" 7

746 Mason "The evidential foundations" in Mason (ed) *Electronic Evidence: disclosure, discovery and admissibility* 2007 6 (hereafter referred to as Mason "The evidential foundations") quoted by Meintjes- Van der Walt "Electronic Evidence" 323

747 Hofman "Chapter 17: South Africa" 683

748 2005 4 All SA 657 (C) at [678-679]

749 2006 4 All SA 165 (W)

(4) Provisions of the Stamp Duties Act 77 of 1968

The Stamp Duties Act 77 of 1968 was repealed by section 108 of the Revenue Laws Amendment Act 60 of 2008.[751]

(f) Other relevant provisions of chapter III of the ECT Act

(i) Retention

With regard to retention, the ECT Act provides as follows:

> 16. (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 ina 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.

(ii) Other requirements

Section 19 provides for various cases where data messages can fulfil a certain requirement in law. Subsection (1) reads as follows:

> 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.

---

750 Ch 3 par 3.3.2.3.4

751 For more details see Ch 2 par 2.2.4.3.3 and Ch 3 par 3.4.2.1.1 C

Subsection (2) states that:

> An expression in 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.

Finally subsection (4) provides as follows:

> 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.

(g) Chapter III of the ECT Act beyond commercial matters

The SALRC issued for comment the following question relating to the adequacy of the ECT Act to govern the use and admissibility of electronic evidence in criminal and civil proceedings:[752]

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

To answer this question, it is imperative, firstly, to determine why the Model Law restricted its scope to commercial activities. The obvious reason is the fact that the Model Law is the product of a UN body whose mandate is international trade law;[753] hence, the commercial focus. The Model Law, however, states clearly that there is nothing in the Model Law that prevents an enacting country to extend its scope to activities beyond the commercial sphere.[754] In other words, there are no substantive grounds for why the Model Law could not be extended to civil or

752 SALRC Issue Paper 27, *Review of the Law of Evidence* (2010) 30

753 United States Commission on International Trade Law established by the United Nations General Assembly by resolution 2205 (XXI) of 17 December 1966 (*A Guide to UNCITRAL: Basic facts about the United Nations Commission on International Trade Law* 2013 available at http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf (accessed on 1/10/2015)

754 Par 26 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

criminal proceedings, for example. The South African ECT Act clearly extends its scope beyond commercial activities.[755]

The concern of the SALRC is, therefore, not really on the validity of section 15 of the ECT Act; in fact, it is satisfied about its adequacy in dealing with electronic evidence. The problem lies instead with the inconsistency in the approach between the CPA and CPEA in dealing with electronic evidence in criminal and civil proceedings respectively. In the light of this, the SALRC asks whether it is adequate for section 15 to remain in the ECT Act or whether it should be part of a general Act dealing with documentary evidence inclusive of the relevant provisions of the CPA and CPEA with the necessary adjustments.[756]

The majority of respondents did not feel it necessary to remove section 15 from the ECT Act.[757] Despite this, The SALRC recommends the adoption of a single statute to deal with documentary evidence or hearsay and documentary evidence,[758] and it proposes a draft law of evidence bill.[759]

The recommendation is commendable. One may, however, ask whether it is not possible to reach the desired objective with less effort, for example by amending and supplementing existing provisions.[760]

The discussion on the ECT Act would not be complete without referring to the Cybercrimes and Cybersecurity Bill 2015[761] which copies and pastes the evidence provisions of the ECT Act.

3. The Cybercrimes and Cybersecurity Bill 2015

The admissibility of electronic evidence is governed by section 63 of the Cybercrimes and Cybersecurity Bill. This section is a faithful reproduction of section 15 of the ECT Act, except that it is restricted to criminal proceedings on the one hand, and on the other hand, although like

755 S 4(1)

756 SALRC *Discussion Paper 131 on the review of the law of evidence*(2015) 51

757 Position shared by the Law Society of South Africa, Advocate Eiselen and the National Prosecutions Authority.The only dissenting voice came from Legal Aid SALRC; See *Discussion Paper 131 on the review of the law of evidence* (2015) 51

758 SALRC *Discussion Paper 131 on the review of the law of evidence* (2015) 51

759 SALRC *Discussion Paper 131 on the review of the law of evidence* (2015) Annexure A

760 Alternative to a single-statute approach shared by the majority of respondents; SALRC *Discussion Paper 131 on the review of the law of evidence* (2015) 51

761 Hereafter referred to as the Cybercrimes and Cybersecurity Bill

the ECT Act, it accepts that a copy or printout of data or a data message is rebuttable proof of the contents of such data or data message, it differs from the ECT Act, however, in the fact that it requires that the copy or printout be accompanied by a declaration that is authenticated—

> (a) in the manner prescribed in the rules of court for the authentication of documents executed outside the Republic;
>
> (b) by a person, and in the manner, contemplated in section 7 or 8 of the Justices of the Peace and Commissioners of Oaths Act, 1963 (Act No. 16 of 1963); or
>
> (c) in terms of the laws of the foreign State regulating the integrity and correctness of the data or data message and the correctness of the copy or printout.[762]

In addition, section 63 of the Cybercrimes and Cybersecurity Bill is complementary to section 15 of the ECT Act and any other law providing for the admissibility of data or a data messages as evidence in any proceedings. It does not replace them.[763] Given the similarities between both sections, remarks on section 15 of the ECT Act can apply *mutatis mutandis* to section 63 of the Cybercrimes and Cybersecurity Bill.[764]

The ECT Act has been discussed thoroughly under the special provisions heading as it constitutes the most important statute as far as electronic documents are concerned in South Africa, in particular because it is the first statute to recognise electronic evidence in electronic form. The ECT Act originates from the Model Law on E-commerce; hence it was right to discuss this instrument as well to better understand the ECT Act. In respect of the admissibility and weight of data messages, similarly to the Model Law, the ECT Act accepts such category of evidence provided that it respects the normal rules of evidence which should not, however, deny them admissibility in evidence only because they are in electronic format. This is a big step forward from the much criticised Computer Evidence Act 57 of 1983 which focused too much on authenticated computer printouts. Its repeal by the ECT Act was therefore welcome. Reference was also made to the Cybercrimes and Cybersecurity Bill as it reproduces evidence provisions of the ECT Act. Apart from the discussion on special legislation, the section in

762 S 63(4) of the Cybercrimes and Cybersecurity Bill
763 S 63(5) of the Cybercrimes and Cybersecurity Bill
764 Ch 3 par 3.3.2.3.4 & 3.4.2.2. B 2 (e) (i)

respect of South Africa has discussed also general legislation including the CPEA and CPA as well as common law. From this discussion it can be highlighted that all these rules are applicable to electronic documents, however, not all them can be applied satisfactory, for example section 34 of the CPEA fell short to deal with electronic documents in *Narlis v South African Bank of Athens,*[765] because of a definition of document too limited.[766] This is in contrast with section 13 of the English Civil Evidence Act 1995 which defines document widely enough to accommodate easily electronic documents. Other statutes discussed under the English jurisdiction, namely the Bankers' Books Evidence Act 1879 and the Criminal Justice Act 2003 permit also the admission of electronic evidence as a form of documentary evidence.

3.4.2.3 Sui generis evidence

It can be argued that electronic evidence may in some circumstances be considered as a *sui generis* form of evidence.[767] The reason for this is that, because of the special characteristics of electronic information, traditional rules of evidence alone are inefficient in dealing with electronic evidence in digital format. The characteristics include the dependence on machinery and software, the mediation of technology, the technical obsolescence, the high volume and easy replication of information, the nature of the storage medium, the difficulty of deletion and destruction of electronic information and the existence of metadata.[768] When applying traditional principles and rules to electronic evidence, therefore, one must not ignore the special nature of such evidence and the necessity to take into account the principle of functional equivalence.[769]

3.5 Conclusion

This chapter has discussed at length the admissibility and weight of electronic evidence in essentially two jurisdictions, those of England and South Africa. The analysis was undertaken in three steps. Firstly, it discussed the relationship between electronic evidence and real evidence, secondly, the focus was on the interaction between electronic evidence and hearsay, and, finally, the chapter discussed the relationship between electronic evidence and documentary evidence.

---

765 1976 2 SA 573 (A)
766 Ch 3 par 3.4.2.1.1 A
767 Ch 1 par 1.2
768 Ch 2 par 2.3.2
769 Ch 3 par 3.4.2.1.3 B

With regard to the first step, it was noted that electronic evidence both in analogue and digital format is accepted as real evidence when it is generated without the intervention of the human mind; in other words, when it is automatically produced.[770] The review of cases in both the English and South African jurisdictions shows that traditional rules on real evidence are able to accommodate electronic evidence generated automatically without the intervention of a human being.[771]

In respect of the relationship between hearsay and electronic evidence, it was pointed out that the regime of hearsay in England and South Africa was amended significantly through legislative intervention. England has adopted an inclusionary approach toward hearsay making almost all hearsay admissible,[772] while South Africa is still preferring an exclusionary approach but much more flexible to allow the admission of more hearsay evidence.[773] In consequence electronic hearsay is well accommodated under the regime currently existing in both England and South Africa.[774]

Finally, given the fact that the relationship between electronic evidence and documentary evidence is the strongest, this part has enjoyed greater attention. The admissibility and weight of electronic evidence as documentary evidence was discussed in England through the following pieces of legislation: the Bankers' Books Evidence Act 1879; the Civil Evidence Act 1995; and the Criminal Justice Act 2003. All these statutes permit the admission of electronic evidence as a form of documentary evidence. For example the definition of "document" in terms of section 13 of the Civil Evidence Act 1995 is so broad that it can easily accommodate electronic documents. In respect of the South African jurisdiction, the discussion has covered common law, the CPEA, the CPA on the one hand and the Computer Evidence Act 57 of 1983 and the ECT Act on the other hand. The rules provided by these Acts are applicable to electronic documents, however, not all them can be applied satisfactory, for example section 34 of the CPEA fell short to deal

770 See the English case *The Statue of Liberty* 1968 1 WLR 739. This case has been used as an authority in South Africa as well.For a discussion on the admissibility and weight of electronic evidence as real evidence see in general Ch 3 par 3.2

771 Ch 3 par 3.2

772 S 1(1) of the Civil Evidence Act 1995

773 The Law of Evidence Amendment Act 45 of 1988 in general

774 See Ch 3 par 3.3 on the relationship between the admissibility and weight of electronic evidence and the hearsay rule

with electronic documents in *Narlis v South African Bank of Athens*,[775] because of a definition of document too narrow in scope.[776] The Computer Evidence Act 57 of 1983, which was adopted in response to the above case, was very much criticised because it put too much emphasis on authenticated computer printouts. Its repeal by the ECT Act was welcome. The ECT Act is a big step forward, like the Model Law on E-commerce from which it originates, it provides for the admissibility of data messages in evidence as long as they respect the normal rules of evidence which should not, however, deny them admissibility in evidence only because there are in electronic format. For example, if a data message is accepted as the functional equivalent of documentary evidence, to be admissible it must satisfy the ordinary requirements for the admissibility of documents.[777]

In addition the chapter also examined the adequacy of the ECT Act to govern electronic evidence outside the commercial sphere in accordance with the SALRC question issued for comment.[778] After reviewing the Model Law on E-commerce, the conclusion was reached that there are no substantive grounds for why the Model Law which is restricted to commercial activities could not be extended to civil and criminal proceedings as has been done by the ECT Act. Regarding the recommendation of the SALRC to enact a single statute containing all provisions pertaining to electronic evidence in terms of the ECT Act, the CPA and the CPEA, it was submitted, in line with the majority of the respondents, that it was not necessary as the ECT Act is fine, and any inconsistencies between the CPA and CPEA in dealing with electronic evidence could easily be removed by amending and supplementing existing provisions in terms of both Acts.[779]

Lastly the chapter has argued that electronic evidence may in some circumstances be considered as a *sui generis* form of evidence.[780] The reason for this is that, because of the special characteristics of electronic information, traditional rules of evidence alone are inefficient in dealing with electronic evidence in digital format. The characteristics include the dependence on machinery and software, the mediation of technology, the technical obsolescence, the high volume and easy replication of information, the nature of the storage medium, the difficulty of

---

775 1976 2 SA 573 (A)

776 Ch 3 par 3.4.2.1.2 A

777 The admissibility and weight of electronic evidence as documentary evidence is dealt with in Ch 3 par 3.4

778 Ch 3 par 3.4.2.1.3 B 2 (g)

779 Ch 3 par 3.4.2.1.3 B 2 (g)

780 Ch 1 par 1.2 and Ch 3 par 3.4.2.1.4

deletion and destruction of electronic information and the existence of metadata.[781] When applying traditional principles and rules to electronic evidence, therefore, one must not ignore the special nature of such evidence and the necessity to take into account the principle of functional equivalence.[782]

This brings an end to Chapter 3, attention may now be given to techniques and other methods used to prove the authenticity of electronic documents, discussed at length in chapter 4 below which deals with the challenges raised by electronic evidence and their responses in the form of electronic signatures.

781 Ch 2 par 2.3.2

782 Ch 3 par 3.4.2.1.3 B

CHAPTER 4 ELECTRONIC SIGNATURE, A RESPONSE TO THE CHALLENGES OF ELECTRONIC EVIDENCE

4.1 Introduction

Some issues have been identified in the previous chapter regarding the challenges affecting electronic evidence. These challenges revolve around the notions of authenticity, integrity, and the non-repudiation of electronic evidence. Traditionally, the above features of documents have been safeguarded by putting requirements that tend, if not to eliminate completely the risks of tampering with evidence, at least to reduce them to a very low level. These requirements include the necessity of producing a written document in original form and bearing a signature. With the dematerialisation of documents, these requirements become difficult to apply to electronic documents. This chapter attempts to analyse this situation. It, firstly, discusses the above-mentioned notions briefly from a general point of view, and then the discussion becomes more specific in relation to the digital world with techniques and other methods used to safeguard the authenticity, integrity, and non-repudiation of electronic evidence. Electronic signatures can play such a role, so they are discussed in great detail in this chapter. The discussion includes not only a technical outline but also an overview of the law pertaining to electronic signatures. Legal instruments considered in the discussion include, amongst others, the UNCITRAL Model Law on Electronic Signatures, the EU Directive on Electronic Signatures, the English Law on Electronic Signatures, as well as the Singapore Electronic Transactions Act 2010, and the ECT Act. In addition, a review of the case law is undertaken.

4.2 Analysis of traditional paper-based requirements

The analysis of the traditional requirements for paper documents is important in that it reveals the purposes and functions of these requirements and how they can be fulfilled in the case of electronic documents. A paper document can serve various functions, such as: "to provide that a document will be legible to 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."[783] In other words, these functions can ensure the authenticity, integrity, and non-repudiation of paper documents. It is, thus, worthwhile to explore briefly the following concepts, "writing", "original", and "signature".

4.2.1 Writing[784]

The first concept of paper-based documents to be analysed is the aspect of "writing". "Writing" is defined in law in England and South Africa as including typing, printing, lithography, and other modes of representing or reproducing words in visible form.[785]

When analysing the requirement in law of "writing", one needs to refer to the law of contract. Although, as a general rule, writing is not essential to contractual validity in terms of the law of contract, it offers obvious advantages such as giving the parties time to consider their positions during the preparation of the contract before signing, or by simplifying the burden of proof by making it easier for the party who alleges the existence of a contract to prove it, and also by making the scope for possible disagreement about the terms of the contract much narrower, as the terms are in writing for all to see.[786] This is why parties may sometimes require their contract to be in writing, and, in that case, there will be no binding obligation until the terms have been reduced to writing and signed.[787] Another exception to the above general rule that writing is not essential to contractual validity can be made by statute; indeed a statute may impose the requirement of writing or some higher degree of formality for certain types of contracts.[788] Christie and Bradfield claim that the only justification for prescribing formalities, which dates back to the 17th century in England, can be to ensure reliable evidence of the terms of the contract and to prevent wasteful litigation owing to faulty memory or attempts to maintain

783 Par 16 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

784 The requirement of writing in law is dealt with in more detail in Ch 3 par 3.4.2.1.3 B 2 (b)

785 S 5 of the Schedule 1 of the Interpretation Act 1978 and S 3 of the Interpretation Act 33 of 1957 respectively

786 Christie & Bradfield *Christie's The Law of Contract in South Africa* (6th ed) 2011 (hereafter referred to as Christie & Bradfield *Christie's The Law of Contract in South Africa*) 109

787 Christie & Bradfield *Christie's The Law of Contract in South Africa* 109.See also *Goldblatt v Fremantle* 1920 AD 123 and *Woods v Walters* 1921 AD 303 cited by Christie & Bradfield *Christie's The Law of Contract in South Africa* 110

788 Christie & Bradfield *Christie's The Law of Contract in South Africa* 109

fraudulent claims or defences.[789] At a time where England was facing high levels of the above abuses, the Statute of Frauds of 1677 was enacted, according to both authors, as a means to address the abuses and it prescribed the formality of writing for certain types of contract which were then leading to the most noticeable abuses.[790] Although the statute served a useful purpose in eliminating many fraudulent claims and defences, it did not achieve its goal. In fact, it promoted more frauds than it prevented. This was due, admittedly, to its poor drafting.[791]

In South Africa, successive legislatures prescribed the formality of writing for an increased number of classes of contract, first at provincial level and later at national level.[792] This approach is viewed by Christie and Bradfield as contrary to what happened in England where the legislature was progressively phasing out the infamous Statute of Frauds. They criticise the South African approach for increasing the scope of generally similar legislation to the English Statute of Frauds as it produces a crop of unnecessary litigation.[793]

The following is a non-exhaustive list of contracts for which the requirement of writing is prescribed in South Africa: alienation of land; executory donations; and suretyship. These will be discussed below. Apart from these, other aspects of miscellaneous contracts will be discussed as well.

4.2.1.1 Alienation of land

Section 2 (1) of Act 68 of 1981 provides as follows:

789 Christie & Bradfield *Christie's The Law of Contract in South Africa* 113

790 Christie & Bradfield *Christie's The Law of Contract in South Africa* 113

791 Christie & Bradfield *Christie's The Law of Contract in South Africa* 114; on Statute of Frauds read also Wright & Winn *The Law of Electronic Commerce* 14-10 to 14-13

792 For instance, sales of land were required to be in writing in terms of S 30 of the Transvaal Proclamation 8 of 1902 and S 49 of the Free State Ordinance 12 of 1906. These sections were later repealed and replaced by S 1 of Act 68 of 1957 which extended the requirement of the writing to the whole of the then Union. Other repeals followed by various laws and eventually the requirement of writing was extended to the whole country; Christie & Bradfield *Christie's The Law of Contract in South Africa* 114

793 Christie & Bradfield *Christie's The Law of Contract in South Africa* 115

> No alienation[794] of land after the commencement of this section shall, subject to the provisions of section 28, be of any force or effect unless it is contained in a deed of alienation signed by the parties thereto or by their agents acting on written authority.

The wording of this section, as noted by Christie and Bradfield, leaves no room for the argument that the section can be waived by either party.[795] If the contract has, however, been fully performed by both parties in spite of its not being in writing, it will not be upset.[796]

4.2.1.2 Executory donations

In terms of section 5 of the General Law Amendment Act 50 of 1956,

> No donation concluded after the commencement of this Act shall be invalid merely by reason of the fact that it is not registered or notarially executed: Provided that no executory contract of donation entered into after the commencement of this Act shall be valid unless the terms thereof are embodied in a written document signed by the donor or by a person acting on his written authority granted by him in the presence of two witnesses.

The second part of this section prescribes the requirement of writing for the validity of a donation. It is submitted that this section applies only to a *donatio mera* resting solely on the generosity of the donor who bears the onus to prove that the contract falls within the section.[797] Furthermore, to determine what an executory contract of donation is, Christie and Bradfield suggest making a distinction, as in *Barrett v Executors of O'Neil* 1879 K 104 109, between "an accepted promise to donate giving the promissee a personal right of action against the donor to compel him to fulfil his promise by the delivery or the passing of transfer, and a donation completed by delivery or transfer, which gives the donee a right *in rem*."[798] The latter, that is, the

---

794 "Alienation" in terms of S 1(1) means sale, exchange or donation, irrespective of whether it is subject to a suspensive or resolutive condition

795 *Wilken v Kohler* 1913 AD 135 142 as reported by Christie & Bradfield *Christie's The Law of Contract in South Africa* 6 116 (footnotes)

796 *Wilken v Kohler* 1913 AD 135 144 as reported by Christie & Bradfield *Christie's The Law of Contract in South Africa* 6 116 (footnotes)

797 Christie & Bradfield *Christie's The Law of Contract in South Africa* 129

798 Christie & Bradfield *Christie's The Law of Contract in South Africa* 129

completed donation, is not an "executory contract of donation" and therefore falls outside the section.[799]

4.2.1.3 Suretyship[800]

Section 6 of the General Law Amendment Act 50 of 1956 provides as follows:

> No contract of suretyship entered into after the commencement of this Act shall be valid, unless the terms thereof are embodied in a written document signed by or on behalf of the surety: Provided that nothing in this section contained shall affect the liability of the signer of an aval under the laws relating to negotiable instruments.

It is suggested that the enactment of this section was meant to achieve certainty as to the true terms agreed upon and, thus, avoid or reduce the possibility of perjury or fraud and unnecessary litigation as with contracts for sale of land.[801] In addition, it could have been influenced by the fact that because surety is an onerous obligation, as it involves the payment of another's debts, "would-be sureties should be protected against themselves to the extent that they should not be bound by any precipitate verbal undertakings to go to surety for another but would be bound only after their undertakings had been recorded in a written document and signed by them or on their behalf."[802]

4.2.1.4 Miscellaneous contracts

Section 17(3) of Act 97 of 1998 requires certain learnership contracts to be in writing and registered. Section 22(3) of Act 98 of 1978 requires an assignment of copyright to be in

799 Christie & Bradfield *Christie's The Law of Contract in South Africa* 130

800 "Suretyship is an accessory contract by which a person (the surety) undertakes to the creditor of another (the principal debtor),that the principal debtor, who remains bound, will perform his obligation to the creditor and, secondarily, that, if and so far as the principal debtor fails to do so, the surety will perform it or, failing that, indemnify the creditor." Forsyth & Pretorius *Cane's The Law of Suretyship* at par 28 quoted by Christie & Bradfield *Christie's The Law of Contract in South Africa* 130

801 *Fourlamel (Pty) Ltd v Maddison* 1977 1 SA 333 (A) 342-343 as cited by Christie & Bradfield *Christie's The Law of Contract in South Africa* 130

802 *Fourlamel (Pty) Ltd v Maddison* 1977 1 SA 333 (A) 342-343 as cited by Christie & Bradfield *Christie's The Law of Contract in South Africa* 130

writing.[803] Other contracts, such as negotiable instruments and insurance policies, must, by custom (in most cases confirmed by statute), be in writing.[804]

There is another category of contracts which does not require the contract to be reduced to writing for the purpose of validating the agreement or for its efficacy in relation to third parties, but simply to inform consumers and provide them with a measure of protection; this is the case of consumer contracts.[805] For example, in a case of a lease of premises for residential purposes, the lease does not need to be in writing in terms of section 5(2) of the Rental Housing Act 50 of 1999, but the lessor has an obligation to reduce it to writing if requested to do so by the lessee in accordance with the above section.[806] Regarding credit agreements governed by the National Credit Act 34 of 2005, a credit provider is required to deliver a copy of the document recording their agreement to a consumer in terms of section 93(1) of the Act. In both cases, however, non-compliance with these requirements does not invalidate the agreement.[807] This is also the case with the Consumer Protection Act 68 of 2008 which provides, in section 50(1), that the relevant Minister may prescribe categories of consumer agreements to which the Act will apply that are required to be in writing. Non-compliance with this requirement does not, however, invalidate the contract.[808]

The requirement of writing has been discussed by looking at the law of contract. Although generally it is not a condition for the validity of a contract, it offers a lot of advantages that make it an important element.[809] It is often related to another concept, original, briefly discussed below.

4.2.2 Original[810]

The second concept of paper-based documents to be analysed is the aspect of originality. The requirement of "original" in law has been addressed in the previous two chapters. Without

803 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
804 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
805 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
806 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
807 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
808 Christie & Bradfield *Christie's The Law of Contract in South Africa* 134
809 Ch 4 par 4.2.1
810 See Ch 2 par 2.2.4.3.1 and Ch 3 par 3.4.2.1.1 A and par 3.4.2.1.3 B 2 (d)

repeating what has already been said, it is, however, important to highlight that the general rule with regard to the original is that no evidence is ordinarily admissible to prove the contents of a document except the original document itself.[811] This rule mainly affects private documents. Munday contends in that regard that the general proposition developed by the law of evidence is that a private document must be proved by primary evidence; in other words, the original ought to be produced before the court.[812]

The original document rule is preserved for criminal proceedings by section 252 of the CPA and for civil proceedings by section 42 of the CPEA.[813] Zeffertt and Paizes point out that this rule is principally illustrated by a number of criminal cases in which appeals were successful because the prosecution did not produce the original in its attempt to prove the terms of a document.[814] They refer, amongst others, to the following cases, *R v Pelunsky*[815] and to *R v Nhlanhla*.[816] In the first case, the accused was charged with conspiring to defraud the Johannesburg municipality of livestock dues by falsifying certain tickets which were supposed to record the number of sheep which he had brought into the municipal market. The prosecution relied on the counterfoils which had been filled at the same time as the tickets to prove the entries on the tickets. On Appeal, it was held that, in the absence of any explanation of why the original tickets would not be produced, the secondary evidence provided by the counterfoil should have been excluded.[817] In the second case, the accused was charged with contravening certain sections of the Native Trust and Land Act 18 of 1936. The prosecution was required to prove that the land on which the alleged offence had been committed was not registered in the name of the South African Native Trust. To that effect, the court held that it had to produce the title deeds, the register kept by the Registrar of Deeds, or secondary evidence of these documents made admissible by statute. The oral evidence of an official who said that it was not trust land was held, therefore, not to be admissible.[818]

811 *Standard Merchant Bank Ltd v Creaser* 1982 4 SA 671 (W) at 674B
812 Munday *Evidence* (4th ed) 2007 (hereafter referred to as Munday *Evidence*) 583
813 Zeffertt & Paizes *The SA Law of Evidence* 829
814 Zeffertt & Paizes *The SA Law of Evidence* 829
815 1914 AD 360
816 1960 3 SA 568 (T)
817 Zeffertt & Paizes *The SA Law of Evidence* 829
818 See Zeffertt & Paizes *The SA Law of Evidence* 829-830

Generally what makes a document to be seen as an original is the affixing of a signature on it. This concept is discussed thoroughly below.

4.2.3 Signature

The last concept of paper-based documents to be analysed is the aspect of signature. The discussion of signature under this heading includes a first part dealing with a certain number of definitions; a second part on the form of a signature versus its function; and finally the third and last part deals with signatures under analogue technologies.

4.2.3.1 Definitions

In order to apprehend what constitutes an electronic signature, it is important to understand the function of a signature and how judges have responded to changes in technology over the generations.[819] A brief history of the signature reveals that different technologies and methods have been used throughout history to make signatures. As noted by Mason, the function performed by a signature "remains as valid in the electronic age as when the use of an impression of a seal was considered to be the best means of authentication before the advent of widespread literacy."[820]

A signature is a handwritten (and often stylised) depiction of someone's name, nickname, or even a simple "X" or other mark, that a person writes on documents as a proof of identity and intent.[821] In other words it is a person's name written in a distinctive way with the objective to authenticate a document, authorise a transaction, or identify oneself as the writer or sender of a letter. It may also be a distinctive mark or cross serving this purpose.[822]

Buckley *et al* remark that in the United States the common law recognises not one but a virtually limitless number of possible ways of signing.[823] This includes various symbols, devices, and

819 Mason *Electronic Signatures in Law* (2012) 1

820 Mason *Electronic Signatures in Law* (2012) 1

821 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/179546?rskey=7lZuiO&result=1#eid (accessed on 28/03/2014)

822 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/179546?rskey=7lZuiO&result=1#eid (accessed on 28/03/2014)

823 Buckley, Tank, Whitaker and Kromer *The Law of Electronic Signatures and Records* 2004 (hereafter referred to as Buckley *et al The Law of Electronic Signatures and Records*) 1.1-2

procedures which have been held by the courts to constitute valid signatures,[824] for example a traditional, wet pen and ink, handwritten signature, a mark such as a "X" or thumbprint, a printed name, a stamped name, a typewritten name, a facsimile containing a name, a telegram, and a telex.[825] A signature is, thus, "whatever mark, symbol, or device one may choose to employ as representative of himself."[826] A fictitious name can be used as a signature if it is adopted as a substitute for the signer's name; similarly mere initials have been held to be valid as a signature.[827]

In England, Reed notes, that there is a shortage of definitions of signature although signing a document is a fundamental legal act and many statutes impose requirements for signatures.[828] He asserts that the paradigm case of signature is the signatory's name, written in his or her hand, on a paper document ("manuscript signature").[829] And this process, he notes, is universally understood by lawyers and non-lawyers alike.[830] Other methods of signing, however, have been considered by English courts, according to Reed, and these include crosses,[831] initials,[832] pseudonyms,[833] identifying phrases,[834] printed names,[835] seals,[836] and rubber stamps.[837] All these methods of signing have been held valid by drawing an analogy with a manuscript signature.[838] The approach adopted by the courts in the various cases dealing with the above signature methods was to determine whether the particular form of signature adopted had already been

824 Buckley *et al The Law of Electronic Signatures and Records* 1.1-2

825 Buckley *et al The Law of Electronic Signatures and Records* 1.1-2

826 *Griffith v Bonawitz*, 73 Neb. 622, 103 NW 327 (1905) cited by Buckley et al *The Law of Electronic Signatures and Records* 1.1-3

827 Buckley *et al The Law of Electronic Signatures and Records* 1.1-3

828 Reed "What is a signature?" 2000 *JILT* 3 *(*hereafter referred to as Reed "What is a signature?") 1.1, available at http://elj.warwick.ac.uk/jilt/00-3/reed.html/ (accessed on 01/04/2014)

829 Reed "What is a signature?" 1.1

830 Reed "What is a signature?" 1.1

831 *Baker v Dening* (1838) 8 A & E 94

832 *Hill v. Hill* [1947] Ch 231

833 *Redding, in re* (1850) 14 Jur 1052, 2 Rob Ecc 339

834 *Cook, In the Estate of (Deceased) Murison v Cook and Another* [1960] 1 All ER 689 (holograph will signed 'your loving mother')

835 *Brydges v Dix* (1891) 7 TLR 215; *France v Dutton*, [1891] 2 Q.B. 208. Typewriting has also been considered in *Newborne v Sensolid (Great Britain), Ltd* [1954] 1 QB 45

836 *in re Doe d Phillips v Evans* 2 LJ Ex 193 (signature by seal valid for purposes of Insolvency Act); *in re Byrd* 3 Curt 117 (signature by seal invalid for purposes of Wills Act)

837 *Lazarus Estates, Ltd v Beasley* [1956] 1 QB 702; *London County Council v. Vitamins, Ltd., London County Council v Agricultural Food Products, Ltd.* [1955] 2 QB 218

838 Reed "What is a signature?" 1.1

recognised as valid in previous decisions, and, if not, to decide whether it was acceptable in the particular circumstances of each case. To ascertain this, judges apparently determined whether the method adopted achieved the same authentication functions as a manuscript signature, and, if this was the case, the method was accepted as a valid signature.[839]

In South Africa, the perceptive comments from the sound dissenting judgment of Bell J in 1855 in *Van Vuuren v. Van Vuuren*,[840] at 121 can give an insight into the definition of signature. Bell J held, in that passage, that the expression "to sign" a document has no strict legal or technical meaning different from the popular meaning, namely to authenticate by that which stands for, or is intended to represent, the name of the person who is to authenticate.[841] To sign a document can, therefore, be done by putting a cross to it, by putting the initial capital letters of one's Christian and surname, or even by producing a scrawl more or less legible.[842]

This position was endorsed by Marray J in *Van Nierkerk v Smith*,[843] who held that:

> "Signature does not necessarily mean writing a person's Christian and surname but any mark which identifies it as the act 'of the party' – *Morton v Copeland*, 16 CB 517 per Maule J at p 535. To sign, as distinguishing from writing one's name in full, is to make such a mark as will represent the name of the person signing. (*In re Trollip*, 12 SC 243 at p 246, per Lord de Villiers.) See also *R v Matanda*, 1923 AD at p 436. Pencil signatures, signatures by initials or by means of a stamp, or by mark, or by a party's writing below a printed heading are all sufficient under the Statute of Frauds (*vide* Halsburg, *Laws of England*, vol. 7, para. 179, Hailshamed.)."[844]

4.2.3.2 Form versus function

The validity and effectiveness of a signature can be tested using two different approaches. The first approach consists of determining whether the signature has the required form and that will entail a list of acceptable forms of signature at the top of which will be the manuscript

839 Reed "What is a signature?" 2

840 2 Searle 116

841 *Van Vuuren v Van Vuuren* 2 Searle 116 at 121 quoted by Mason *Electronic Signatures in Law* (2012) 3

842 *Van Vuuren v Van Vuuren* 2 Searle 116 at 121 quoted by Mason *Electronic Signatures in Law* (2012) 3-4

843 1952 3 SA 17 (T)

844 *Van Nierkerk v Smith* 1952 3 SA 17 (T) 25 as quoted by Christie & Bradfield *Christie's The Law of Contract in South Africa* 120

signature.[845] The list could be extended if necessary to include new forms of signature which are sufficiently similar to those already on the list.[846] The second approach, on the other hand, is to identify the functions performed by a signature, and, then, to provide that all signature methods which perform those functions will be treated for legal purposes as valid signatures.[847] According to Reed, English law initially determined the validity of signatures by referring to their form, before starting assessing validity according to the functions performed by the signature method.[848] If, thus, a signature performs the functions prescribed by the law, it will be valid, irrespective of the form it takes, unless the signature is required to satisfy the formal requirement of a mark.[849] The primary function a signature must perform, according to case law, is evidential. Additional requirements are, however, provided by statutory law.[850] Before dealing with the functions of a signature, it is important to deal with the requirements of form first.

4.2.3.2.1 Requirements of form

As far as form is concerned, two requirements deserve a closer look, namely personal signatures and marks.

A. Personal signatures

A personal signature can be defined as a signature requiring the signatory to write his name or some equivalent in his own handwriting.[851] The courts have, in some instances where the context of the applicable legislation demanded a personal signature, ruled that the signature must take the form of a manuscript signature.[852] It is suggested, additionally, that to ascertain whether a personal signature is required one needs either to examine the wording of the statue, or to look at the context in which the requirement for a signature is imposed.[853] Thus, in *Goodman v. J.*

845 Reed "What is a signature?" 1.3
846 Reed "What is a signature?" 1.3
847 Reed "What is a signature?" 1.3
848 Reed "What is a signature?" 1.3
849 Reed "What is a signature?" 3
850 Reed "What is a signature?" 3
851 Reed "What is a signature?" 2.3
852 Reed "What is a signature?" 2.3
853 Reed "What is a signature?" 2.3. Reed lists the following statutes and Statutory Instruments as containing wording which appears to require a personal signature: Trade Marks Rules 1994 (SI 1994 No 2583) rule 46;s 82 (Form TM33);Child Support Appeal Tribunals (Procedure) Regulations 1992 (SI 1992 No 2641) reg. 3;

EbanLtd.,[854] the Court of Appeal, after reviewing relevant authorities, was satisfied that a solicitor's bill did not require a personal signature, and, thus, a rubber stamp was a valid signature. In contrast, the Court of Appeal adopted a restrictive view in *Firstpost Homes Ltd. v. Johnson and others*.[855] Analysing section 2 of the Law of Property (Miscellaneous Provisions) Act 1989 and the type of signature applicable in this context, the court held that the underlying philosophy of the legislation required the contract to be in writing and signed and since extrinsic evidence of the terms of the contract or its signature was not allowed in determining whether such a written and signed contract was created, it ruled that "signature" had to be construed in the manner in which an ordinary man would understand it, that is, as a personal signature.[856]

B. Marks

In addition to the requirement of a signature to take the form of a personal signature, there is also a requirement for a signature to take the form of a mark on a document. There is, according to Reed however, ambiguous authority that a mark is an essential element of all signatures.[857] In *Morton v. Copeland*,[858] Maule J stated that signing:

> [D]oes not necessarily mean writing a person's Christian and surname, but any mark which identifies it as the act of the party.[859]

In *Goodman v. J. Eban Ltd.*,[860] Sir Raymond Evershed MR adopted the definition of signature provided by the *Shorter Oxford English Dictionary*, 2nd ed., vol. 2, p. 1892: "(ii) to place some

---

Family Proceedings Rules 1991 (SI 1991 No 1247) rules 2.2, 2.10;Companies (Forms Amendment No 2 and Company's Type and Principal Business Activities) Regulations 1990 (SI 1990 No 1766) Sch 2, Form 10; Copyright (Librarians and Archivists) (Copying of Copyright Material) Regulations 1989 (SI 1989 No 1212) Sch 2, Forms A & B; County Court (Forms) Rules 1982 (SI 1982 No 586) Schedule, Form N117 General Form of Undertaking Order 29, rule 1(a);Imprisonment and Detention (Air Force) Rules 1980 (SI 1980 No 2005) Sch 1, Part I Forms 1-11;Imprisonment and Detention (Army) Rules 1979 (SI 1979 No 1456) Sch 1, Part I Forms 1-11;Conveyance by Rail of Military Explosives Regulations 1977 (SI 1977 No 889) reg. 7;Practising Certificate Regulations 1976, Schedule, Form PCR2; see Reed "What is a signature?" footnote 42

854 [1954] 1 QB 550

855 [1995] 1 WLR 1567

856 [1995] 1 WLR 1567 at p. 1575 per Peter Gibson LJ, adopting the formulation of Denning LJ in *Goodman v. J. Eban, Ltd.* [1954] 1 QB 550, 561-2 – see Reed "What is a signature?" 2.3 and footnote 41

857 Reed "What is a signature?" 2.4

858 (1855) 16 CB 517, 535

859 Reed "What is a signature?" 2.4

860 [1954] 1 QB 550 at 557

distinguishing mark upon (a thing or person)... (iv) to attest or confirm by adding one's signature; to affix one's name to (a document, etc.)."[861]

The requirement for signatures to take the form of a mark is also found in section 1(4) of the Law of Property (Miscellaneous Provisions) Act 1989 which reads as follows:

> In subsections (2) and (3) above "sign", in relation to an instrument,[862] includes making one's mark on the instrument and 'signature' is to be construed accordingly.

In concluding, Reed notes that, if this requirement still subsists, it will be difficult to sign most electronic documents.[863]

4.2.3.2.2 Functions of a signature

A signature can fulfil various functions. These functions are discussed below under points A to C with A dealing with the primary function of a signature which is evidential, B the subsidiary functions of a signature and C the dispute of a signature.

A.Primary function of a signature: evidential

When looking at the history of the requirements of form for documentary transactions, it is suggested that the reason why the law required a signature is for the purposes of authentication.[864] Indeed, a signature serves primarily to authenticate or to prove the identity of the signatory. [865] It usually incorporates the name of the signer to make it easier to identify such person.[866] However, even if the name is not incorporated into the signature or is illegible, it is

---

861 Reed "What is a signature?" 2.4

862 Reed notes that the term "instrument" is normally used only in the sense of a hard copy document, and that with regard to transactions in land ss. 2(1) and 2(3) of the Act require a signed writing, which again implies a hard copy document; Reed "What is a signature?" footnote 51

863 Reed "What is a signature?" 2.4

864 Identify the person and attribute the document to him, see Forder & Quirk *Electronic Commerce and the Law* 2001 (hereafter referred to as Forder & Quirk *Electronic Commerce and the Law)* 87; Reed "What is a signature?" 3.1

865 When a document contains a manuscript signature, one just needs to adduce evidence of the alleged signatory's normal signature and its similarity to the signature on the document, the burden of proof will then pass on the alleged signatory to prove forgery; *Saunders v. Anglia Building Society* [1971] AC 1004 quoted by Reed "What is a signature?" 3.1.3

866 Forder & Quirk *Electronic Commerce and the Law* 87

common practice to have the name printed near the signature.[867] In addition, a signature serves also to prove the intention to sign by the signatory[868] as well as to indicate that the signatory approves and adopts the contents of the document.[869] The formal requirement of a signature, which can be traced back mostly to the Statute of Frauds1677, was, therefore, imposed to ensure the evidential reliability of documents before courts.[870] According to Mason, this comprises the following elements: to provide tangible evidence that the signatory approves and adopts the contents of the document; to indicate the signatory's approval of the content of the document and his or her intention to be bound by the document which shall have legal effect; and to remind the signatory of the significance of the act and the necessity to act in compliance with the document.[871]

Goodman v J Eban Ltd, [872] sets out the modern standard test for the validity of signatures. The issue in contention was whether a solicitor's bill "signed" with a facsimile of the firm's name imposed by means of a rubber stamp was validly signed. It was argued by the defendant, a client of the firm, that the bill was unenforceable because it had not been signed validly.[873] The Court of Appeal disagreed and held the bill to be properly signed as it accepted that the rubber stamp was placed on the bill by the solicitor with the intention of authenticating the document as his own. Sir Raymond Evershed MR expressed this in the following terms:

867 Forder & Quirk *Electronic Commerce and the Law* 87

868 It proves assent, this can be illustrated by distinguishing between an autograph that does not intend to have legal effects and a signature affixed on a contract which does.(Forder & Quirk *Electronic Commerce and the Law* 88); Reed reports that this principle was explained in *Pryor v. Pryor* (1860) 29 LJPM&A 114. The court held in that case that a will signed by a wife in her husband's name was not a valid attestation because she had no intent to sign for herself; her intent was to make it appear that her husband had signed; Reed "What is a signature?" 3.1.3

869 Reed "What is a Signature?" 3.1;This is the attribution function of a signature (Forder & Quirk *Electronic Commerce and the Law* 87)

870 Salmond "The Superiority of written evidence" (1890) 6 LQR 75 quoted by Reed "What is a Signature?" 3.1

871 Mason *Electronic Signatures in Law* (2012) 9

872 [1954] 1 QB 550

873 As required by S 65(2)(i) of the Solicitors Act, 1932, the legislation then governing solicitors' bills, which provided:
'(1) Subject to the provisions of this Act, no action shall be brought to recover any costs due to a solicitor until one month after a bill thereof has been delivered in accordance with the requirements of this section.
(2) The said requirements are as follows: (i) The bill must be signed by the solicitor, or, if the costs are due to a firm, one of the partners of that firm, either in his own name or in the name of the firm, or be enclosed in, or accompanied by, a letter which is so signed and refers to the bill…'; quoted by Reed "What is a signature?" 3.1.1

> It follows, then, I think, that the essential requirement of signing is the affixing, either by writing with a pen or pencil or by otherwise impressing on the document, one's name or "signature" so as personally to authenticate the document.[874]

Romer LJ concurred by stating that the first impression that people have of a rubber stamp is that it does not constitute a signature. However, taking into account authority and the function of a signature, one comes to a different conclusion. In the present case the type-written letter concluded with the typed words "Yours faithfully, Goodman, Monroe & Company" followed by a rubber stamp with the same words. Romer LJ was thus satisfied that the plaintiff's intention in imposing the rubber stamp was that the rubber stamp be regarded as a signature for the purpose of authenticating the letter.[875]

As correctly noted by Reed, it is clear from this judgment that the validity of a particular signature method depends on the functions it performs.[876] "The purported signature will be therefore valid if it provides evidence of authentication of the document by the purported signatory."[877] Reed remarked further that the above case does not require a signature to be in the form of a natural person; the name of an organisation will be a valid signature when one is signing on behalf of that organisation.[878] In addition, the signature is not required to be in handwriting form; it can be affixed to the document mechanically by any means such as a rubber stamp,[879] printing,[880] or typewriting.[881]

Apart from the requirement of signature imposed by case law as discussed above, a signature can also have a statutory origin. According to Reed, the statutory provisions which require signatures

874 [1954] 1 QB 550 at 557 as quoted by Reed "What is a signature?" 3.1.1

875 [1954] 1 QB 550 at 563

876 Reed "What is a signature?" 3.1.1

877 Reed "What is a signature?" 3.1.1

878 Reed "What is a signature?" 3.1.1

879 *Beauvais v Green* 22 TLR 816; *Bennett v Brumfitt* (1867) L.R. 3 CP 30; *British Estate Investment Society, Ltd v Jackson (H.M. Inspector of Taxes)* [1956] TR 397, 37 Tax Case 79, 35 ATC 413, 50 R&IT 33, High Court of Justice (Chancery Division); *Lazarus Estates, Ltd. v Beasley* [1956] 1 QB 702; *London County Council v Vitamins, Ltd, London County Council v Agricultural Food Products, Ltd* [1955] 2 QB 218 ; all quoted by Reed "What is a signature?" 3.1.1

880 *Brydges v. Dix* (1891) 7 TLR 215; *France v. Dutton*, [1891] 2 Q.B. 208;all quoted by Reed "What is a signature?" 3.1.1

881 *Newborne v Sensolid (Great Britain), Ltd.* [1954] 1 QB 45; all quoted by Reed "What is a signature?" 3.1.1

for evidential purposes fall into two broad categories.[882] The first category comprises provisions which make signed documents either admissible as evidence or create evidential presumptions in relation to them. In terms of these presumptions a document is either conclusive proof of its contents or it is *prima facie* evidence of the facts set out in it.[883] The second category is made of provisions requiring documents to be signed for the purpose of authentication. The purpose of authentication can be provided expressly by the legislation or it can be inferred from the context.[884]

B. Subsidiary functions of a signature

A signature can serve as subsidiary functions to validate an official action or for consumer protection purposes.

With regard to the function of validating an official action, a signature can be provided by legislation to validate the exercise of powers granted to a judicial or administrative body by the legislation. This is commonly the case with documents recording or certifying the decisions of judicial bodies or of persons exercising statutory powers.[885] The requirement of a signature will be even more important (or common) if, in the absence of the statute, the action to be validated will infringe human rights or property rights.[886] A signature is, therefore, necessary for the following actions: the temporary imprisonment of army personnel;[887] the convening of a court martial,[888] or the delaying of the discharge of service personnel;[889] as well as the entry into premises[890] or the detention of shipping.[891]

As far as consumer protection is concerned, a signature performs the secondary function of evidence of the informed consent to the transaction by the consumer in English law.[892] In other

882 Reed "What is a signature?" 3.1.2
883 Reed "What is a signature?" 3.1.2
884 Reed "What is a signature?" 3.1.2
885 Reed "What is a signature?" 3.2.1
886 Reed "What is a signature?" 3.2.1
887 Reed "What is a signature?" fn 93
888 Reed "What is a signature?" fn 94
889 Reed "What is a signature?" fn 95
890 Reed "What is a signature?" fn 96
891 Reed "What is a signature?" fn 97
892 Reed "What is a signature?" 3.2.2

words, the consumer's signature provides evidence that the other party has supplied the required information and that the consumer has agreed to the terms.[893]

Mason highlights other functions a signature can perform as including a cautionary function, a protective function, a channelling function, or a record-keeping function.[894]

The cautionary function serves as a means of reinforcing the legal nature of the signed document by calling the signatory to exercise care before committing himself to the contents of the document.[895]

The protective function, however, operates at the other end of the relationship, namely by assuring the receiving party that the other party signed the document after giving full attention to its contents. The identity of the signatory is also assured as well as the source and contents of the document.[896]

As to the channelling function, Mason notes that a manuscript signature helps to clarify the point at which a person recognises that the act has become legally significant. In addition, the recording of the content of the document on a durable format serves to concentrate the mind on the legally nature of the document, and, therefore, reducing the risks of oral recollections.[897]

With regard to the record keeping function, finally, a signed document contained in a physical carrier can serve as a durable record of the contents of the document.[898]

In a nutshell, a signature can perform various functions, such as: to identify a person; to provide certainty as to the personal involvement of that person in the act of signing; and to associate that person with the content of a document. A signature might, furthermore, attest to *inter alia*: the intent of a party to be bound by the content of a signed contract; the intent of a person to endorse authorship of a text; the intent of a person to associate himself with the content of a document

893 Reed "What is a signature?" 3.2.2
894 Mason *Electronic Signatures in Law* (2012) 10
895 Mason *Electronic Signatures in Law* (2012) 10
896 Mason *Electronic Signatures in Law* (2012) 10
897 Mason *Electronic Signatures in Law* (2012) 10
898 Mason *Electronic Signatures in Law* (2012) 10

written by someone else; and the fact that, and the time when, a person had been present at a given place.[899]

C. Dispute of a signature

To dispute a manuscript signature one must establish defences such as the fact that: the signature is a forgery; the signature was conditional; the signature was obtained as a result of misrepresentation; the signature was obtained in such circumstance that it was not the act of the person signing (*non est factum*); there was mental incapacity; it was a mistake; a party unilaterally added material terms to the writing after the other's signature; the person signing the document did not realise the document he signed was a contractual document; and it is by statute unreasonable or unfair.[900]

To address the issue of forgery of signatures, as well as to test the validity and effectiveness of a manuscript signature, it is required for certain documents to affix a signature in the presence of a witness or an authorised official, such as a notary.[901]

In addition, when a manuscript signature on a document is challenged, evidence must be provided to show that the signature affixed to the document is that of the signatory.[902] This process is achieved by comparing the signature on the document to other samples of the signatory's signatures.[903] A handwriting analyst will, thus, be called to perform the comparison or software can be used, such as the Forensic Information System for Handwriting (FISH) used by the US Secret Service, according to Mason.[904] If it is shown that the manuscript signature is similar to the sample signatures, the evidential burden will then pass to the alleged signatory to prove that the signature was forged.[905] Notwithstanding proof of similarity, however, evidence must be adduced to show that the signatory intended to sign the document.[906]

899 Buckley *et al The Law of Electronic Signatures and Records* 1.1-2;Par 53 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
900 Mason *Electronic Signatures in Law* (2012) 10-11
901 Mason *Electronic Signatures in Law* (2012) 11
902 Mason *Electronic Signatures in Law* (2012) 11
903 Mason *Electronic Signatures in Law* (2012) 11
904 Mason *Electronic Signatures in Law* (2012) 11
905 Mason *Electronic Signatures in Law* (2012) 12
906 Mason *Electronic Signatures in Law* (2012) 12

4.2.3.2.3 Signatures under analogue technologies

Although it is accepted that legal principles apply to new technology in the same way that they apply to older ways of conducting business, their application to new technology is not without challenges as can be seen from the following discussion in respect of typewriting, telegram and facsimile.[907]

A. Typewriting

As far as the value of a typed signature is concerned, Mason suggests referring to the case from the American State of Indiana of 1905 *Ardery v Smith*.[908] In this case, an attorney, with the authority to sign a remonstrance against the issue of a liquor license for and on behalf of voters, caused his names to be typed in his presence and under his supervision because of erysipelas in his right hand. It was held that it was immaterial that the names were added by means of a typewriter. It is necessary, however, to provide evidence that a typed signature was adopted by the person whose name was typed on the document.[909]

B. Telegram

As with the Internet today, the advent of telegraphy in the early nineteenth century created similar problems for judges as they were required to adapt old laws to new technologies on a very large scale.[910] Indeed the telegram and its various technologies, such as the telex, were widely used from the outset. A telegram is a message sent by telegraph,[911] which itself is "an apparatus for transmitting messages to a distance, usually by signs of some kind."[912] The word "telegraphy", stemming from the Greek words *tele*, meaning at a distance, and *graphein*,

907 Mason *Electronic Signatures in Law* (2012) 59

908 35 Ind App 94, 73 N.E. 840; Mason *Electronic Signatures in Law* (2012) 59

909 *Landeker v Co-operative Bldg. Bank* 130 N.Y. Supp. 780 where it was held that that it is necessary to link the application of the typewritten name to prove that the name was typed with authority and intent; Mason *Electronic Signatures in Law* (2012) 60

910 Mason *Electronic Signatures in Law* (2012) 66

911 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/search?searchType=dictionary&q=telegram&_searchBtn=Search (accessed on 16/02/14)

912 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/198686?rskey=Er1v0s&result=1#eid (accessed on 16/02/14)

meaning to write, is the long-distance transmission of textual or symbolic messages without the physical exchange of an object bearing the message.[913]

The acceptance of an offer to buy a property transmitted by telegraph was examined in *Godwin v Francis*,[914] where it was held that a telegram written out and signed by the telegraph clerk, if done with the authority of the vendors, would have been a sufficient signature within the Statute of Frauds.[915] The same conclusion was reached in *McBlain v Cross*,[916] where a signature in a telegram was held to be sufficient to come within the Statute of Frauds. Willes J, in the latter case, was clearly not prepared to let technology impede the way the law was interpreted.[917]

Telegrams were widely used in South Africa as in any jurisdiction.[918] They were considered in, amongst other cases, *Hersch v Nel*,[919] *Luttig v Jacobs*,[920] and *Balzun v O'Hara*.[921]

In the first mentioned case, the concern was whether an acceptance by a cessionary communicated by telegram was valid. The Appeal court found that the communication of the acceptance by telegram was sufficient compliance with the requirements of section 49 of Ordinance 12 of 1906 (OFS).[922]

In contrast, the second case considered the validity of an offer contained in a telegram. It was, however, never contended by the defendant that an option to purchase was invalid because it was in the form of a telegram. Brink J accepted this to be the correct interpretation, especially considering the fact that a copy of the option annexed to the declaration indicated that the original had been signed by the defendant.[923]

---

913 http://dictionary.reference.com/browse/telegraphy (accessed on 16/02/14)

914 (1870) LR 5 CP 295

915 *Godwin v Francis* (1870) LR 5 CP 295 at 301-302; see also Wright & Winn *The Law of Electronic Commerce* 14-13

916 (1872) LT 804

917 Willes J in *McBlain v Cross* (1872) LT 804 at 806 stressed that, "If we did not hold such to be the law, the convenience which the modern invention of the electric telegraph has bestowed upon mankind would be in a great measure subverted."

918 Mason *Electronic Signatures in Law* (2012) 68

919 1948 (3) SA 686 (AD)

920 1951 (4) SA 563 (OPD)

921 [1964] 3 All SA 368 (T)

922 *Hersch v Nel* 1948 (3) SA 686 (A.D.) at 702

923 *Luttig v Jacobs* 1951 (4) SA 563 (O.P.D.) at 567

In the last case, finally, the question for consideration was whether a telegram can constitute "written authority" within the meaning of section 1(1) of Act 68 of 1957. The court, applying the same reasoning as in the two previous cases, held that the statutory requirement of a writing was satisfied by a telegram, even if a signature is a necessary part of such writing.[924]

C. Facsimile

Documents sent by facsimile transmission have generally been accepted in common law jurisdictions.[925] In the Singapore case of *Chua Sock Chen v Lau Wai Ming*,[926] it was held that a notice to complete a transaction was properly served when sent by means of a facsimile transmission and where the original papers were subsequently sent by post to arrive the day after transmission. In the English case of *Re a debtor* (No. 2021 of 1995), *ex parte, Inland Revenue Commissioners v The debtor; Re a debtor* (No. 2022 of 1995), *ex parte, Inland Revenue Commissioners v The debtor*;[927] it was held that a proxy sent by facsimile transmission was not signed as required by rule 8.2(3) of the Insolvency Rules 1986. The decision was, however, reversed on appeal where a proxy form was held acceptable when sent by facsimile transmission.[928] Similarly, in *PNC Telecom plc v Thomas*,[929] the service of a notice sent by facsimile transmission for an extraordinary general meeting on a members' requisition under section 368 of the Companies Act 1985 was held to be valid.

Signatures under facsimile technology conclude this brief section on signatures under analogue technologies which has also discussed typed signatures and signatures contained in telegrams. This discussion shows that, despite a few challenges here and there, signatures under analogue technologies have been accepted as valid signatures in many instances in various jurisdictions, including England and South Africa.[930]

The discussion of signatures under analogue technologies falls under the heading "Signature" which includes also a first part dealing with definitions of a signature and a second part

924 *Balzun v O'Hara* [1964] 3 All SA 368 (T) at 371
925 Mason *Electronic Signatures in Law* (2012) 75
926 [1989] SLR 1119
927 [1996] 2 All ER 345, Ch D
928 Mason *Electronic Signatures in Law* 3 76
929 [2003] BCC 202
930 See in general Ch 4 par 4.2.3.2.3

addressing the form of a signature versus its function. In respect of the first part it should be noted that although signature is often understood as a handwritten or manuscript signature, this first part's discussion has revealed a virtually limitless number of possible ways of signing, including various symbols, devices and procedures which have been accepted as valid signatures by many courts in various common law countries such as England and South Africa.[931] Regarding the second part, it was pointed out that the function played by the signature is the main criterion used to determine the validity of a signature irrespective of the form it takes; and the major function played by a signature is evidential.[932]

Apart from signature discussed as the last item in point 4.2, two other traditional paper-based requirements were addressed, they include writing and original. With regard to writing the discussion was focused on the law of contract and various statutes providing for the requirement of writing for certain categories of contract. As a general rule, however, writing is not a condition for the validity of a contract, but it offers a lot of advantages that make it an important element.[933] In respect of original, it was stressed that since this concept was discussed elsewhere,[934] there was no need to repeat what had been already said; except to highlight the general rule that no evidence is ordinarily admissible to prove the contents of a document except the original document itself.[935] In addition it was pointed out that generally what makes a document to be seen as an original is the affixing of a signature on it.

The discussion of traditional paper-based requirements in general and of signature in particular has paved the way to the discussion on electronic signatures that follows.

4.3 Electronic signatures

A review of the history of signature has given valuable insight into this concept and it provides a strong basis from which electronic signatures can now be discussed. As illustrated above, signatures have evolved with human development. Indeed, different technologies and methods have been used throughout history to make signatures. This is the case of a handwritten

931 Ch 4 par 4.3.2.1
932 Ch 4 par 4.2.3.2.2
933 Ch 4 par 4.2.1
934 Ch 2 par 2.2.4.3.1 and Ch 3 par 3.4.2.1.1 A and par 3.4.2.1.3 B 2 (d)
935 *Standard Merchant Bank Ltd v Creaser* 1982 4 SA 671 (W) at 674B

signature, an "X", or thumbprint mark, a printed name, a stamped name, a typewritten name, a facsimile containing a name, a telegram, or a telex. The advent of the Internet has now given rise to a new method of signing, which is the electronic signature. It is assumed that an electronic signature can guarantee the authenticity, integrity, and non-repudiation of electronic evidence.

The electronic signature was largely defined in chapter 2 of this thesis which provided definitions from various jurisdictions.[936] These definitions do not, therefore, need to be repeated at this stage. They will, however, be discussed during the analysis of electronic signatures in the selected jurisdictions. This analysis will include international initiatives, on the one hand, and the state of the question in the jurisdictions of Singapore, England, and South Africa, referred to as national initiatives on the other hand.

4.3.1 International initiatives

International initiatives are divided into two: United Nations' initiatives; and European Union's initiatives.

4.3.1.1 United Nations' initiatives

These initiatives are discussed below under the heading of the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures respectively, as well as the 2005 United Nations Convention on the Use of Electronic Communications in International Contracts.

4.3.1.1.1 The Model Law on E-commerce

Article 7 provides the following with regard to signature:

> (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

[936] Ch 2 par 2.4.1

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following: [...].

The wording of the first paragraph clearly accepts any method able to identify the signatory and to indicate his approval of the content of a data message as an appropriate signature in terms of the law, provided that it is reliable. This is the so-called functional equivalence approach adopted by the Model Law. The basis of article 7 is, indeed, the recognition of the functions played by a signature in a paper-based environment. Although many functions were considered in the preparation of the Model Law, article 7 relies on the two basic functions of a signature, namely to identify the author of a document and to confirm that the author approved the content of that document.[937] Both functions guarantee the authenticity of the data concerned. They were adopted to prevent electronic documents required to be authenticated to be denied legal validity for the sole reason they were not authenticated in a manner peculiar to paper documents.[938] This comprehensive approach of article 7 establishes the general conditions under which data messages would be regarded as authenticated with sufficient credibility and would be enforceable.

Article 7 did not intend to develop functional equivalents for the various types and levels of signature requirements in existence in spite of the fact that it would have increased the level of certainty of substitutes of handwritten signatures used in electronic commerce because developing rules on methods to be used as substitutes for handwritten signatures was seen as being susceptible to leading to the risk of tying the legal framework to a particular state of technical development.[939]

To determine whether the method of identification is reliable and appropriate for the purpose for which the data message is generated or communicated, the Model Law set out a number of legal, technical, and commercial factors that should be taken into account. They include the following: (1) the sophistication of the equipment used by each of the parties; (2) the nature of their trade activity; (3) the frequency at which commercial transactions take place between the parties; (4)

937 Par 53 & 56 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
938 Par 56 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
939 Par 55 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)

the kind and size of the transaction; (5) the function of signature requirements in a given statutory and regulatory environment; (6) the capability of communication systems; (7) compliance with authentication procedures set forth by intermediaries; (8) the range of authentication procedures made available by any intermediary; (9) compliance with trade customs and practice; (10) the existence of insurance coverage mechanisms against unauthorized messages; (11) the importance and the value of the information contained in the data message; (12) the availability of alternative methods of identification and the cost of implementation; (13) the degree of acceptance or non-acceptance of the method of identification in the relevant industry or field both at the time the method was agreed upon and the time when the data message was communicated; and (14) any other relevant factor.[940]

It should be noted that the Model Law does not impose the use of an electronic signature for all transactions. It leaves discretion under paragraph (3) of article 7 to states to provide for exceptions.

To increase certainty with regard to the operation of the article 7's flexible approach for the recognition of an electronic signature as functionally equivalent to a handwritten signature, the Model Law on Electronic Signatures was adopted. This instrument is discussed below.

4.3.1.1.2 The Model Law on Electronic Signatures

The Model Law on Electronic Signatures was a response to the need for a specific legal framework given the increased use of electronic authentication techniques as substitutes for handwritten signatures and other traditional authentication procedures in order to reduce uncertainty as to the legal effect that might result from the use of such modern techniques, generally referred to as "electronic signatures".[941] Relying on the fundamental principles underlying article 7 of the Model Law on E-commerce, this Model Law offers practical standards against which the technical reliability of electronic signatures may be measured. It further provides a link between such technical reliability and the legal effectiveness that might be expected from a given electronic signature.[942] Interestingly, under the new Model Law, the legal effectiveness of a given electronic signature technique might be predetermined (or assessed prior

940 Par 58 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce (1996)
941 Par 3 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)
942 Par 4 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

to its being used).[943] The Model Law on Electronic Signatures initiative must, therefore, be praised as it contributes to enabling or facilitating the use of electronic signatures and provides equal treatment to both users of paper-based documentation and users of computer-based information.

A certain number of provisions in the Model Law on Electronic Signatures are discussed in the following lines. They include in particular article 2 on definitions and article 6 dealing with the compliance with a requirement for signature. Lastly articles 7, 8, 9 and 11 are discussed in passing.

A. Article 2 Definitions

In terms of article 2(a) an electronic signature means "data in electronic form in, affixed to, or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message."[944]

This definition relies on the functional equivalent approach and is wide enough to cover all traditional uses of a handwritten signature for legal effect, although it specifically provides only for the functions of identifying the signatory and indicating his approval. It is suggested that these functions are merely illustrative as they constitute the smallest common denominator of the various approaches to "signature" found in the various legal systems.[945] Functions of a signature have been discussed in the analysis of article 7 of the Model Law on E-commerce above.[946]

According to the Model Law on Electronic Signatures, a distinction should be made between the legal notion of "signature" and the technical notion of "electronic signature", the latter covering practices that do not necessarily lead to the generation of legally significant signatures. Indeed, a risk of confusion exists as the same technical tool can be used for the production of a legally meaningful signature and for other authentication or identification functions.[947] This leads to the question of the legal implications of electronic signature techniques made without clear intent by

943 Par 4 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)
944 See Ch 2 par 2.4.1.1
945 Par 93 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)
946 Ch 4 par 4.3.1.1.1
947 Par 94 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

the signatory of becoming legally bound by approval of the information being electronically signed. In response, it is suggested that to replicate in an electronic environment the legal consequences of the use of a handwritten signature, that is the appending of a signature (whether handwritten or electronic) to certain information, should create a presumption that the signatory approved the linking of his or her identity to this information; whether such a linking should produce legal effects shall be determined according to the applicable law.[948]

B. Article 6 Compliance with a requirement for a signature

Article 6 provides as follows:

1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(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.

4. Paragraph 3 does not limit the ability of any person:

948 Par 120 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

(a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or

(b) To adduce evidence of the non-reliability of an electronic signature.

5. The provisions of this article do not apply to the following: [...].

Article 6 is one of the core provisions of the Model Law. It is strongly interrelated with article 7 of the Model Law on E-commerce upon which it builds. Indeed, it reproduces most of the provisions of article 7,[949] and it provides guidance as to how the test of reliability in paragraph 1 (b) of article 7 can be satisfied. To pass this test, an electronic signature must comply with the conditions listed under paragraph 3 which are discussed below.

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person.

The meaning of the expression "signature creation data" varies according to the context in which it is used. When used in the context of electronic signatures which are not digital signatures, it refers to secret keys, codes, or other elements which, in the process of creating an electronic signature, are used to provide a secure link between the resulting electronic signature and the person of the signatory.[950] Thus, in the context of electronic signatures relying on biometric devices, for example, the essential element would be the biometric indicator, such as a fingerprint or retina-scan data.[951] In the context of digital signatures relying on asymmetric cryptography, only the private key is covered by the description of "signature creation data".[952]

As to the requirement of a linkage between the signature creation data and the signatory and no other person, it must be stressed, in the context of the first scenario, that only those core elements which should be kept confidential to ensure the quality of the signature process should be taken into account in establishing the linkage, to the exclusion of any other element that, although it might contribute to the signature process, could be disclosed without jeopardizing the reliability

949 Provisions of paragraphs (1)(b),(2) and (3) of article 7 are reproduced respectively by paragraphs 1,2 and 5 of article 6.In addition par 1(a) of article 7 is included in the definition of "electronic signature" under article 2 (a)

950 Par 97 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

951 Par 97 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

952 Par 97 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

of the resulting electronic signature.[953] While certain electronic signature creation data may be shared by a variety of users, for example where several employees would share the use of a corporate signature creation data, that data must be capable of identifying one user unambiguously in the context of each electronic signature.[954] This logic applies in respect of digital signatures as well. Although both the public key and the private key are linked to the signatory in the context of digital signatures, the fact that the public key is public and can be disclosed without compromising the reliability of the resulting electronic signature has as a consequence that only a private key must be used to establish the link with the signatory. As to the public key, its link with the signatory can be confirmed by a certificate which certifies that the public key belongs to the signatory.[955]

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person.

This condition is self-explanatory. It simply means that those core elements we referred to in the previous paragraph, such as secret keys and codes, must be under the sole control of the signatory. The signatory is, however, entitled to authorise another person to use the signature creation data on his behalf as long as he maintains control over the signature creation data.

(c) Any alteration to the electronic signature, made after the time of signing, is detectable.

This condition deals with the integrity of the electronic signature and sets forth the criterion to be met in order to demonstrate that a particular method of electronic signature is reliable enough to satisfy a requirement of law for a signature.[956]

(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.

This condition deals with the integrity of the information being signed electronically. Its purpose is to ensure that the electronic signature used is reliable enough to detect any interference with the information to which it relates.

953 Par 97 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

954 Par 121 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

955 "Certificate" is defined under article 2 as meaning "a data message or other record confirming the link between a signatory and signature creation data."

956 Par 124 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

It must be stressed, however, that the integrity of the electronic signature and that of information is not always easy to distinguish. Indeed, they are so closely related that it is difficult to conceive of one without the other. The reason why this distinction was adopted was essentially to conform to the Model Law on E-commerce.[957]

Notwithstanding paragraph 3 above, the reliability of an electronic signature can be proved by any other method while its non-reliability can be proved by adducing any evidence.[958]

C. Other articles

In terms of article 7, any person, organ, or authority, whether public or private, specified by the enacting State as competent may determine which electronic signatures satisfy the provisions of article 6 of this Law. This determination must, however, be consistent with international standards. Ultimately, determining which electronic signature techniques satisfy the reliability criteria of article 6 will ensure certainty and predictability.

Articles 8, 9, and 11 describe the roles of various parties in the creation, and the use, of electronic signatures. In terms of article 8, the signatory is required to exercise reasonable care to avoid unauthorised use of its signature creation data,[959] and to notify any relevant person of any compromise of the signatory creation data.[960] In addition, where a certificate is used to support the electronic signature, the signatory must exercise reasonable care to ensure the accuracy and completeness of all material representations relevant to the certificate throughout its life cycle or that are to be included in the certificate.[961] The signatory is liable for failure to comply with the above requirements.[962]

Article 9 sets forth the conduct of the certification service provider where it provides services to support an electronic signature that may be used for legal effect as a signature,[963] and the legal consequences for its failure.[964] The certification service provider must, amongst other things,

957 Par 125 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)
958 Par 4 of art 6 of the UNCITRAL Model Law on Electronic Signatures (2001)
959 Par 1(a)
960 Par 1(b)
961 Par 1(c)
962 Par 2
963 Par 1(a)-(f)
964 Par 2

utilise trustworthy systems, procedures, and human resources in performing its services.[965] To determine this trustworthiness, a set of criteria must be considered.[966]

Lastly, the conduct of the relying party is dealt with in article 11 which makes that party liable for failing to take reasonable steps to verify the reliability of an electronic signature,[967] the validity of a certificate,[968] or any limitation with respect to the certificate.[969]

The Model Law on Electronic Signatures discussed above offers practical standards against which the technical reliability of electronic signatures may be measured. It further provides a link between such technical reliability and the legal effectiveness that might be expected from a given electronic signature.[970] It is an interesting initiative in that it contributes to enabling or facilitating the use of electronic signatures and provides equal treatment to both users of paper-based documentation and users of computer-based information. The last UN instrument of interest is discussed below; it deals with the use of electronic communication in international contracts.

4.3.1.1.3 The United Nations Convention on the Use of Electronic Communications in International Contracts[971]

Article 9 (3) of the Electronic Communications Convention provides as follows:

> 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

965 Par 1(f)

966 Art 10 lists the following factors: a) Financial and human resources, including existence of assets; (b) Quality of hardware and software systems; (c) Procedures for processing of certificates and applications for certificates and retention of records; (d) Availability of information to signatories identified in certificates and to potential relying parties; (e) Regularity and extent of audit by an independent body; (f) The existence of a declaration by the State, an accreditation body or the certification service provider regarding compliance with or existence of the foregoing; or(g) Any other relevant factor

967 Par (a)

968 Par (b) (i)

969 Par (ii)

970 Par 4 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

971 Hereafter referred to as the Electronic Communications Convention

(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.

This article follows the functional equivalence approach adopted by both Model Laws on E-commerce and Electronic Signatures. It reiterates the criteria to establish the functional equivalence between electronic authentication methods and handwritten signatures. There is, however, a slight difference in the wording of the present article and article 7(1) of the Model Law on E-commerce which, in contrast to "the party's intention" provided by article 9 (a) of the Electronic Communications Convention, refers to "the signatory's approval" of the information contained in the data message. This wording was preferred as it was felt that, in certain instances, although a law required a signature, that signature did not necessarily fulfil the function of indicating the signatory's approval of the information contained in the electronic communication. This is the case when a document is notarised by a notary or attested by a commissioner of oaths. In the context of this Convention, therefore, signature does not necessarily imply a party's approval of the entire content of the communication to which the signature is attached.[972]

Paragraph 3(b)(i) above significantly reproduces article 6(1) of the Model Law on Electronic Signatures as well as article 7(1)(b) of the Model Law on E-commerce. It establishes a reliability test to ensure the correct interpretation of the principle of functional equivalence for electronic signatures.[973] The purpose of the reliability test is to remind courts of the necessity to take into account factors other than technology-related factors in determining whether the electronic signature used was sufficient to identify the signatory.[974] These factors include the purpose for which the electronic information was generated or communicated or the existence of an

[972] Par 160 of the Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

[973] Par 163 of the Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

[974] Par 163 of the Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

agreement between the parties to use simple signature methods,[975] and other legal, technical, and commercial factors that may be taken into account in determining the reliability of the method used which are mentioned elsewhere in this text.[976]

It should be stressed, however, that any attempt by a party to use the reliability test to repudiate its signature in instances where the actual identity of the party and its actual intention could be proved is forbidden by the Convention. The court, or any trier of fact, is thus expected not to invalidate an entire contract because of an unreliable electronic signature used if there is no dispute as to the authenticity of that electronic signature. Paragraph 3(b)(ii) is, therefore, useful in circumventing these situations as it accepts that the requirement of a signature in law can be met if the method used in the particular instance is proven to have satisfied the functions of identifying the party and indicating its intention.[977]

The discussion on the UN Convention on the Use of Electronic Communications in International Contracts concludes the section on the UN initiatives on electronic signatures which includes also the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures respectively. All these instruments recognise electronic signatures with the Model Law on Electronic Signatures providing practical standards against which the technical reliability of electronic signatures may be measured.[978] After discussing initiatives at the global level, it is right to look at efforts made at regional level in respect of electronic signatures. EU initiatives, given that they affect England, a member, are discussed below.

4.3.1.2 The European Union's initiatives

The EU initiatives discussed below include the E-commerce Directive and the eSignature Directive. The first Directive is discussed briefly, it servers more as a broad introduction to the discussion on the eSignature Directive.

---

975 Par 163 of the Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

976 Ch 4 par 4.3.1.1.1

977 See, in general, Par 164 of the Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts.

978 Ch 4 par 4.3.1.1.2

4.3.1.2.1 Directive 2000/31/EC on Electronic Commerce[979]

The objective of this Directive is to create a legal framework to ensure the free movement of information society services between Member States.[980] "Information society services" is defined in this context as encompassing any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing (including digital compression) and storage of data at the individual request of a recipient of a service.[981]

The E-commerce Directive is relevant to this discussion on electronic signatures in that it calls for Member States to ensure that contracts can be concluded by electronic means in their jurisdictions by removing all obstacles in the legal requirements excluding the use of electronic contracts or depriving them of legal effectiveness and validity because of their electronic nature.[982] Arguably, a signature is the biggest obstacle to the recognition of electronic contracts and the development of e-commerce. This explains why the European Commission has deemed it necessary to adopt a whole Directive to deal with this issue. The said Directive is analysed in detail in the following lines.

4.3.1.2.2 Directive 1999/93/EC on Electronic Signatures

The eSignature Directive is discussed in two points dealing respectively with definitions under A and article 5 under B.

A. Definitions

The purpose of this Directive is to facilitate the use of electronic signatures and contribute to their legal recognition. It creates a legal framework for electronic signatures and certain certification services in order to ensure the proper functioning of the internal market.[983] Two types of electronic signatures are recognised in terms of this Directive, "electronic signature" on the one hand, and "advanced electronic signature" on the other hand. It can be argued, however, that the Directive on Electronic Signatures provides for three types of electronic signatures.

979 Hereafter referred to as the E-commerce Directive
980 Recital 8 and Art 1(1)
981 Recital 17 and Art 2(a) of the E-commerce Directive and Art 1(2) of Directive 98/34/EC as amended by Directive 98/48/EC
982 Art 9(1)
983 Art 1

Mason, for example, has expressed different views in this regard. In an older edition of his book relating to this subject matter, he pointed out that the Directive provided for two types of electronic signature, an electronic signature and an advanced electronic signature.[984] Recently, however, he indicated that, according to the Directive, there are three types of electronic signature, an electronic signature, an advanced electronic signature, and a qualified electronic signature.[985] Although, strictly speaking, the Directive provides for only two types of electronic signature that it defines in article 2, this dichotomy of views is understandable. In this author's view, however, it appears more logical to divide electronic signatures as far as the Directive is concerned into two broad categories, electronic signatures on the one hand and advanced electronic signatures on the other hand, with the so-called "qualified electronic signature" falling under the second category as a subset. It should be acknowledged, nevertheless, that there is a general trend to refer to advanced electronic signatures based on a qualified certificate and created by a secure-signature-creation device as "qualified electronic signatures" although this terminology is not specifically used in the Directive.[986] These issues are discussed further at a later stage. But before that the requirements of an "electronic signature" and an "advanced electronic signature" are analysed.

"Electronic signature"

Electronic signature is defined as meaning "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."[987] This definition is very wide and is justified by the rapid technological development and the global nature of the Internet which requires an approach broad enough to include various technologies and services capable of authenticating data electronically.[988] Mason remarks that this definition fails to link the need for the electronic signature to authenticate the data to which

---

984 Mason *Electronic Signatures in Law* (2nd ed) 2007 [hereafter referred to as Mason *Electronic Signatures in Law* (2007))144

985 Mason *Electronic Signatures in Law* (2012) 112

986 Interdisciplinary Centre for Law and Information Technology (ICRI) *The Legal and Market Aspects of Electronic Signatures Final Report* Study for the European Commission – DG Information Society 2003 (hereafter referred to as ICRI *The Legal and Market Aspects of Electronic Signatures*) 49

987 Art 2 (1) of the Directive; see also Ch 2 par 2.4.1.1 of this thesis

988 Recital 8 of the Directive on Electronic Signatures

it is attached or with which it is logically associated.[989] He further observed that it is unclear whether the authentication referred to under the definition relates to the origin of the data or to the identity of a person or entity.[990] It is, however, suggested from the wording of recital 8 that the term "electronic signature" under the Directive refers exclusively to "data authentication" and does not include methods and technologies for "entity authentication".[991] Thus, the use of a PIN code to access a bank account will not fall within the ambit of the above definition of "electronic signature", while the same code used to confirm a financial transaction will qualify as an electronic signature under the eSignature Directive as it serves to authenticate data.[992]

"Advanced electronic signature"

An advanced electronic signature, on the other hand, is an electronic signature meeting the following four requirements: (a) uniquely linked to the signatory; (b) capable of identifying the signatory; (c) created using means that the signatory can maintain under his sole control; and (d) linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.[993]

Mason argues that, in essence, an advanced electronic signature is a digital signature in all but name. This view is justified, according to him, by the fact that it appears from the above definition that an advanced electronic signature is capable of existing only in a format over which in theory an individual has total physical control , as set out in article 2(2)(c).[994]

A report points out that, although these requirements are formulated in a very general and technology-neutral manner, in practice the definition refers mainly to electronic signatures based on digital signature technology, that is, using public key cryptography.[995]

Below is an analysis of the above four requirements that an electronic signature is expected to meet to qualify as an advanced electronic signature.

989 Mason *Electronic Signatures in Law* (2012) 115
990 Mason *Electronic Signatures in Law* (2012) 115
991 ICRI *The Legal and Market Aspects of Electronic Signatures* 29
992 ICRI *The Legal and Market Aspects of Electronic Signatures* 29
993 Art 2(2) of the Directive; see also Ch 2 par 2.4.1.2
994 Mason *Electronic Signatures in Law* (2012) 118
995 ICRI *The Legal and Market Aspects of Electronic Signatures* 30

Uniquely linked to the signatory

Mason is adamant that no form of electronic signature can comply with this requirement. He points out, for example, that a user relinquishes control over his scanned signature once it has been sent. In addition, he notes that a digital signature is not linked to the person creating it, affirming that the only unique link in this instance is made with the private key and not the user. He stresses, moreover, that nobody is capable of memorising a private key as it is far too complicated; these private keys must, therefore, be retained on a computer, disk, or smart card. For all these reasons Mason reckons that it is not possible to create an electronic signature that can be uniquely linked to the signatory.[996]

To understand the argument of Mason better, it is important to clarify the exact meaning of an "advanced electronic signature". Based on the definition of "electronic signature", it can be inferred that an "advanced electronic signature" means data in electronic form which are attached to, or logically associated with, other electronic data and which serve not only as a method of authentication, but also meet a certain number of requirements, including being uniquely linked to the signatory. Thus, the logical question arising from this is to determine whether it is possible for the above data to be uniquely linked to the signatory. To answer this question, one can analyse the example of digital signatures or electronic signatures relying on public key cryptography. This type of electronic signature makes use of a private key which contains certain data serving to link the data message to which it is affixed to the private key owner. At this point two scenarios can be envisaged. Firstly, if the private key owner and the signatory are different persons, then the private key will not be linked to the signatory. Secondly, however, if the private key owner and the signatory are the same person, then the private key will be linked to the signatory. Indeed the signatory is the person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents to generate a signature.[997] Unlike Mason's view, therefore, it is submitted that it is possible to envisage an electronic signature uniquely linked to the signatory as pointed out above. This will be even more the case when the electronic signature relies on biometric devices

996 Mason *Electronic Signatures in Law* (2012) 118

997 Art 2(3) of the eSignature Directive

as the biometric indicator, such as a fingerprint or retina-scan data, will uniquely link to the signatory.

Capable of identifying the signatory

This requirement is easy to comply with as any form of electronic signature is capable of identifying the person who made it.[998]

Created using means that the signatory can maintain under his sole control

According to the Forum of European Supervisory Authorities for Electronic Signatures (FESA), the creation of an advanced electronic signature using means that the signatory can maintain under his sole control "does not require the use of a special hardware device as a signature-creation device, but it requires – especially in the case where the private key is stored in software – the use of security measures by the signatory to maintain his control over the key (e. g. encryption of the file which stores the private key, restriction of access to the computer and this file)."[999]

The Forum further clarifies the meaning of "sole control" in the context of automatically signing systems maintained by several system administrators and relevant for systems that sign qualified certificates as well by stating that where the certificate is issued to a natural person, "the security concept and the configuration of the server must ensure that only this person has control over the private key." However, "if the certificate is issued to a legal person (which is not possible in most countries) the personnel of the legal person maintains 'sole control' over the private key by its security concept."[1000] In respect of signatures created automatically at a server, the signatory, who is usually not present in person, has the responsibility of selecting appropriate security measures to ensure control. In the case of server-based signature services, since the signatory is neither present nor in a position to select appropriate security measures, he only can decide whether or not to enlist these services. This decision shall be made after careful consideration of the security measures taken by the service provider by accessing a comprehensive version of the security concept and reaching a level of confidence that the service provider adheres to the

998 Mason *Electronic Signatures in Law* (2012) 121

999 Forum of European Supervisory Authorities for Electronic Signatures "Working Paper on Advanced Electronic Signatures" 12 October 2004 (hereafter referred to as FESA "Working Paper") 2

1000 FESA "Working Paper" 2-3

security concept "(confidence can be strengthened by audits performed by a trusted third party like an independent auditor or a supervisory authority)."[1001] In addition, the Forum notes that "sole control" requires certain cryptographic qualities of algorithms and of signature creation data. For all these reasons, it is submitted by FESA members that "sole control at least of the signature creation data can be achieved and that [of] advanced electronic signatures can be created by a server based signature service."[1002] However with regard to Germany, the Forum points out that " 'sole control' implies physical control and that therefore in Germany, server-based signature services cannot be used for creating advanced electronic signatures and definitely not for creating qualified electronic signatures."[1003] Mason supports the position in Germany and affirms that a different interpretation of "sole control" will distort this term beyond measure.[1004]

Linked to the data to which it relates in such a manner that any subsequent change of the data is detectable

This requirement can easily be fulfilled by using suitable cryptographic algorithms for hashing and signature creation.[1005]

After analysing the definitions of the different types of electronic signatures provided by the eSignature Directive, one can now deal with the main article of the Directive as far as the legal validity of electronic signatures is concerned, namely article 5.

B. Article 5

The core article of the eSignature Directive is article 5. It deals with the legal effects of electronic signatures and provides as follows:

1. Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device:

1001 Forum of European Supervisory Authorities for Electronic Signatures "Public Statement on Server Based Signature Services" 17 October 2005 (hereafter referred to as FESA "Public Statement on Server Based Signature Services") 1

1002 FESA "Public Statement on Server Based Signature Services" 2

1003 FESA "Public Statement on Server Based Signature Services" footnote 2

1004 Mason *Electronic Signatures in Law* (2012) 123

1005 FESA "Working Paper" 3

(a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and

(b) are admissible as evidence in legal proceedings.

2. Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:

— in electronic form, or

— not based upon a qualified certificate, or

— not based upon a qualified certificate issued by an accredited certification-service-provider, or

— not created by a secure signature-creation device.

Two aspects can be highlighted from this article. Paragraph 1 sets forth the requirements that advanced electronic signatures must meet to produce legal effects, while paragraph 2 deals with rules regulating electronic signatures in general.

With regard to advanced electronic signatures, two preconditions must exist. The advanced electronic signature must be based on a qualified certificate and created by a secure-signature-creation device. A qualified certificate is a certificate which meets the requirements laid down in Annex I,[1006] and it is provided by a certification-service-provider who fulfils the requirements laid down in Annex II.[1007] A secure-signature-creation device, on the other hand, means configured software or hardware used to implement the signature-creation data, that is, unique

[1006] Annex I states that qualified certificates must contain: (a) an indication that the certificate is issued as a qualified certificate; (b) the identification of the certification-service-provider and the State in which it is established;(c) the name of the signatory or a pseudonym, which shall be identified as such; (d) provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; (e) signature-verification data which correspond to signature-creation data under the control of the signatory; (f) an indication of the beginning and end of the period of validity of the certificate; (g) the identity code of the certificate; (h) the advanced electronic signature of the certification-service-provider issuing it; (i) limitations on the scope of use of the certificate, if applicable; and (j) limits on the value of transactions for which the certificate can be used, if applicable

[1007] Annex II lists a long list of requirements that the certification-service-providers must meet. They include *inter alia*: demonstrate the reliability necessary for providing certification services; ensure that the date and time when a certificate is issued or revoked can be determined precisely; use trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them; take measures against forgery of certificates; record all relevant information concerning a qualified certificate for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.[1008] According to recital 20, advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device can be regarded as legally equivalent to handwritten signatures only if the requirements for handwritten signatures are fulfilled. The second rule is for Member States to ensure that electronic signatures can be used in legal proceedings and, therefore, contribute to the general acceptance of electronic authentication methods. It must be stressed that the legal recognition of electronic signatures should be based upon objective criteria and not be linked to authorisation of the certification-service-provider involved.[1009] In a report analysing the legal and market aspects of electronic signatures in Europe, this rule was judged superfluous as it was noted that digital data, including electronic signatures, was already admissible in evidence in all Member States, the only issue remaining was the value of such evidence which varied between Member States.[1010] It was further submitted that this question of admissibility of electronic signatures was dealt with in each Member State on a case-by-case basis discretionary by the judge,[1011] which is in harmony with the provision of Recital 21 stating that the Directive does not affect the powers of national courts regarding the rules of evidence.

In respect of electronic signatures broadly speaking, the Directive requires from Member States not to deny them legal effectiveness and admissibility in legal proceedings merely because they are in electronic form or they are not "qualified electronic signatures". It is clear from the wording of this provision that Member States must abstain from promoting regulations or endorsing private rules excluding the use of an electronic authentication tool merely by virtue of its electronic format or non-qualified nature. There must be a substantive reason to any disqualification of electronic signatures, such as a lack of technological reliability, circumstantial impropriety, or accountability.[1012]

The eSignature Directive contains liability provisions for certification service providers when issuing qualified certificates. Articles 6(1) makes them liable for the accuracy and the

1008 Art 2(5) read with art 2(4)
1009 Recital 21 of the Directive on Electronic Signatures
1010 ICRI *The Legal and Market Aspects of Electronic Signatures* 50
1011 ICRI *The Legal and Market Aspects of Electronic Signatures* 50
1012 ICRI *The Legal and Market Aspects of Electronic Signatures* 51

completeness of the information contained in the qualified certificate at the time of issuance;[1013] for the assurance that, at the time of the issuance of the certificate, the signatory identified in the qualified certificate held the signature-creation data corresponding to the signature-verification data given or identified in the certificate;[1014] and for the assurance that the signature-creation data and the signature-verification data can be used in a complementary manner in cases where the certification service provider generates both of them.[1015] The certification service provider will be held liable unless it can prove that it has not acted negligently.[1016] The above liability provisions are the minimum liability Member States are expected to provide when implementing the Directive; they are not, however, prevented from introducing stricter liability or liability for instances where certification service providers are not issuing qualified certificates.[1017]

It was pointed out in a report analysing the state of implementation of the e Signature Directive in Europe that Finland was among the countries that transposed, in more or less literal terms, the provision of article 5.1.[1018] It is, thus, worthwhile to have a look at this jurisdiction to determine how courts have handled the issue of electronic signatures there. Mason reports two cases in which advanced signatures were considered in Finland. In the first case, in 2004, the Market Court held that an administrative appeal in a public procurement matter sent as an attachment to an email required an advanced electronic signature.[1019] The requirement for an advanced electronic signature was derived from chapter 5 section 24 of the Administrative Judicial Procedure Act (586/1996, 26.7.1996 Hallintolainkäyttölaki) requiring a signature, which could be fulfilled by using an advanced electronic signature in terms of section 9 of the Act on Electronic Services and Communication in the Public Sector (13/2003, 24.1.2003 Lakisähköisestäasioinnistaviranomaistoiminnassa), which in turn refers to section 18 of the Act on Electronic Signatures (14/2003, 24.2.2003 Lakisähköisistäallekirjoituksista).[1020] The Market

1013 Art 6(1)(a)
1014 Art 6(1)(b)
1015 Art 6(1)(c)
1016 Art 6(1) last sentence
1017 Art 6(1) and (2)
1018 ICRI *The Legal and Market Aspects of Electronic Signatures* 70
1019 Combined cases 106/04/JH (140/04/JH and 147/04/JH, judgment MAO: 161/04, 162/04, 163/04 of 27.8.2004) available in Finnish at www.finlex.fi (reported by Mason *Electronic Signatures in Law* (2012) 113)
1020 Mason *Electronic Signatures in Law* (2012) 113

Court ruled that the appeal was not delivered as there were no court facilities for lodging appeals by email, and the email did not include an advanced electronic signature.[1021]

The second case mentioned by Mason was heard in the Insurance Court, and it dealt with a matter relating to an administrative appeal claim in which the claimant appealed a decision of the social security authority to the unemployment benefits board by sending the appeal by email.[1022] The claim was dismissed because the claimant did not provide a manuscript signature on paper after submission of an unsigned electronic version of the document.[1023] Under chapter 5 section 24 of the Administrative Judicial Procedure Act an appeal was required to be signed. Section 9 of the Act on Electronic Services and Communication in the Public Sector (13/2003), however, provides, with regard to electronic delivery of documents to authorities, that the document does not need to be signed provided that the document includes sender information and there is no uncertainty about the originality or integrity of the document.[1024] The Insurance Court reversed the board's ruling and referred the matter back, holding that it is not necessary to supplement the application by providing a manuscript signature where the electronic message contains sufficient information regarding the sender such that there is no reason to doubt the authenticity or integrity of the document.[1025]

From the discussion on the eSignature Directive above one can conclude that the legal framework provided by this instrument facilitates the use of electronic signatures and contributes to their legal recognition within the Internal Market. This regional effort by the EU is in line with the global effort by the UN previously discussed. Efforts by both organisations constitute the international initiatives vis-à-vis electronic signatures discussed in the framework of this research. Apart from these international initiatives, national measures have been taken in relation to electronic signatures and constitute national initiatives which are discussed below.

1021 Mason *Electronic Signatures in Law* (2012) 113

1022 Case 1486: 2006 judgment 19.10.2006, available online in Finnish at www.finlex.fi (reported by Mason *Electronic Signatures in Law* (2012) 113)

1023 Mason *Electronic Signatures in Law* (2012) 113

1024 Mason *Electronic Signatures in Law* (2012) 114

1025 Mason *Electronic Signatures in Law* (2012) 114

4.3.2 National initiatives

Three jurisdictions are examined under this heading, namely England, Singapore, and South Africa.

4.3.2.1 England

As all European Union countries, England has transposed the eSignature Directive in its national law in the form of the Electronic Communications Act 2000. This piece of legislation is discussed below followed by the Electronic Signatures Regulations 2002.

4.3.2.1.1 The Electronic Communications Act 2000

The purpose of this Act is *inter alia* to facilitate the use of electronic communications and electronic data storage. It deals, amongst other matters, with the legal recognition and admissibility of electronic signatures. In respect of electronic signatures, the central provision is section 7 which provides as follows:

> (1) In any legal proceedings—
>
> (a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
>
> (b) the certification by any person of such a signature,
>
> shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.
>
> (2) For the purposes of this section an electronic signature is so much of anything in electronic form as—
>
> (a) is incorporated into or otherwise logically associated with any electronic communication or electronic data; and
>
> (b) purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of the communication or data, the integrity of the communication or data, or both.
>
> (3) For the purposes of this section an electronic signature incorporated into or associated with a particular electronic communication or particular electronic data is certified by any person if that

person (whether before or after the making of the communication) has made a statement confirming that—

(a) the signature,

(b) a means of producing, communicating or verifying the signature, or

(c) a procedure applied to the signature,

is (either alone or in combination with other factors) a valid means of establishing the authenticity of the communication or data, the integrity of the communication or data, or both.

This section can be divided into three parts. The first part deals with the admissibility in evidence of electronic signatures and the certification of a signature. The second part defines electronic signature, and the third part explains the modalities of certifying an electronic signature.

As the first part cannot be properly comprehended without understanding both the second and the third parts, it is suggested that one deals with these first.

A. Definition and certification of an electronic signature

Definition

From the definition of electronic signature set out in subsection 7(2) above, three elements can be highlighted, namely "so much of anything in electronic form", "incorporation or logical association", and "authenticity or integrity purpose".

So much of anything in electronic form

This element is widely formulated to make sure that it covers not only current technology but also future technology.

Incorporation or logical association

The second element requires that "such thing" in electronic form be incorporated into or logically associated with electronic communication or electronic data. "Electronic communication" is defined as meaning "a communication transmitted (whether from one person to another, from one device to another, or from a person to a device or *vice versa*) – (a) by means

of an electronic communications network; or (b) by other means but while in an electronic form.[1026] "Electronic data" on the hand, is not defined; presumably the lawmaker did not deem it necessary as the expression is self-explanatory.[1027] The terms "incorporation" or "logical association" are interconnected and refer simply to the link that must exist between the electronic signature and the electronic communication or data, either in the form of inclusion as part of a whole or as an external logical link. For example, in the case of digital signature, the incorporation can be realised by taking part of the plaintext and encrypting it; this creates a message authentication code that allows the recipient to check whether the message has been altered. The message authentication code is, in effect, a separate part of the message; it is, however, also incorporated into the message as it takes the message and encodes it.[1028]

Authenticity or integrity purpose

According to the third element, the "thing in electronic form" which is incorporated into or logically associated with electronic communication or electronic data must serve to authenticate or to establish the integrity of the communication or data, or both. Under this Act, authenticity of communication or data refers to three points: (i) whether the communication or data comes from a particular person or other source; (ii) whether it is accurately timed and dated; (iii) whether it is intended to have legal effect.[1029] The integrity of communication or data, on the other hand, refers to whether there has been any tampering with, or other modification of, the communication or data.[1030] In the light of the above, where an electronic signature is in issue, the person bearing the burden of proof must submit evidence to satisfy the requirements set out in section 15(2).[1031]

The concept of "advanced electronic signature" is not dealt with in the Electronic Communications Act. It is, however, provided for by the Electronic Signatures Regulations 2002 which is discussed below.

1026 S 15(1)

1027 Note that the expression or even "data" is not defined under the Model Laws on E-commerce, or Electronic signatures, or the eSignatures Directive. South Africa, however, defines data as meaning "representation of information in electronic form."

1028 Mason *Electronic Signatures in Law* (2012) 143

1029 S 15(2)(a)

1030 S 15(2)(b)

1031 Mason *Electronic Signatures in Law* (2012) 144

Certification

Certification is the process by which a person certifies an electronic signature, or, in other words, confirms by means of a statement that the signature, or a method or procedure applied to it, is a valid means to establish the authenticity or integrity of the communication or data. The certificate will often be provided by an entity such as a trusted third party, although this is not an obligation.[1032] The certification may be done before or after making the communication. Mason remarks that, from a practical perspective, certification will occur most of the time before the sending of the communication and will need to be substantiated by suitable evidence.[1033] Although a certificate alone might be sufficient in some instances, it should, however, be noted that, most of the time where a party produces a certificate to establish the authenticity or integrity of a message, additional evidence will be necessary.[1034]

B. Admissibility of electronic signatures

An electronic signature is admissible in evidence in relation to the authenticity or integrity of communication or data. In addition, a certification of such electronic signature is also admissible to prove the authenticity or integrity of the communication or data concerned. The evidential weight of the above, however, will be a matter for the courts to decide upon.

It should be highlighted that, although section 7 deals with admissibility, it does not indicate whether an electronic signature will satisfy a statutory signature requirement. Hence, it does not help in determining the extent to which existing statutory signature requirements are capable of being satisfied electronically.[1035] To address this, the English Law Commission suggests the following approach: to demonstrate that the signatory had an authenticating intention. This can be done by applying a purely objective test, such as to ask whether the conduct of a signatory would indicate an authenticating intention to a reasonable person. This approach, as correctly submitted by the Law Commission, is consistent with the authorities, it is flexible, and would,

1032 Mason *Electronic Signatures in Law* (2012) 145
1033 Mason *Electronic Signatures in Law* (2012) 145
1034 Mason *Electronic Signatures in Law* (2012) 146
1035 English Law Commission *Electronic Commerce: Formal Requirements in Commercial Transactions, Advice from the Law Commission* 2001 (hereafter referred to as English Law Commission *Electronic Commerce*) 13

over time, produce the greatest certainty.[1036] The approach is applied below to four methods of electronic signatures to determine whether these will pass the authenticating intention test, namely digital signatures, scanned manuscript signatures, the typing of a name and the clicking on a website button.

Digital Signatures

A digital signature uses cryptography. Within a Public Key Infrastructure, using asymmetric keys, the signing party uses a key pair (private and public key). The sender affixes the signature using his private key, and the recipient checks the signature with the public key. Such digital signature can give high assurance that the electronic communication originated from the person possessing the private key and that it was not changed *en route*. The Law Commission notes that this method of signature indicates to the recipient the authenticating intention of the signatory and, therefore, satisfies a statutory signature requirement.[1037]

Scanned manuscript signatures

A scanned manuscript signature incorporated in a document is capable of indicating to the recipient that the signatory had the necessary authenticating intention, in the same way that an original manuscript signature would do so.[1038] This view was supported by Laddie J in *Re a Debtor* (No2021 of 1995) who considered that a scanned manuscript signature incorporated in a document and then faxed to the recipient and held that such document was signed by the author.

The typing of a name

The typing of the signatory's name or initials onto an email or a document either manually or automatically is capable of indicating to the recipient that the signatory had the necessary authenticating intention and is, therefore, capable of satisfying a statutory signature requirement. This is consistent with case law according to which a signature may be stamped, printed, or typewritten.[1039]

1036 English Law Commission *Electronic Commerce* 13
1037 English Law Commission *Electronic Commerce* 14
1038 English Law Commission *Electronic Commerce* 14
1039 English Law Commission *Electronic Commerce* 14-15

Clicking on a website button

The Law Commission believes there is no doubt that clicking on a website button to confirm an order demonstrates the intent to enter into a contract and satisfies the principal function of a signature, namely the authenticating intention. In addition, it suggests that the click be regarded as the technological equivalent of a manuscript 'X' signature. An "X" clicking, therefore, is capable of satisfying a statutory signature requirement (in those rare cases in which such a requirement is imposed in the contract formation context).[1040]

A click may be challenged on the grounds that it does not produce a visible signature, unlike other forms of signature. In response, the Law Commission notes the following seven points. Firstly, it points out that the criterion for the validity of a signature in English law is function based and not form based, in other words a signature will be valid if it fulfils the function of a signature, irrespective of its form. Secondly, in combination with the information which will be available, such as the email address of the "clicker", a click is capable of satisfying functions such as provide certainty about the personal involvement of the signatory in the act of signing or associate that person with the content of a document. This combination is similar to a stamp signature. Thirdly, regarding the requirement in terms of old authorities that a signature must be a mark and, therefore, visible, the Law Commission believes it is unlikely that the courts would regard such authorities as binding in modern conditions. Fourthly, on most websites the purchaser's details will appear on screen. These details, together with any password and the click, could be regarded as a manuscript signature or a typed signature. Fifthly, the vendor's system may display or record the click in a visible form. Sixthly, the click may generate a writing, the record of the transaction in the vendor's system, and any confirmatory response to the purchaser. Finally, even if a click is less secure than a manuscript signature, the Law Commission notes that reliability is not essential to validity.[1041]

In concluding, it should be pointed out that, in terms of section 8(1), the appropriate Minister has been granted power to modify legislation for the purpose of authorising or facilitating the use of electronic communications or electronic storage.

1040 English Law Commission *Electronic Commerce* 15

1041 English Law Commission *Electronic Commerce* 15-16

The discussion on the Electronic Communications Act 2000 reveals a few missing elements in this statute, for example the absence of provisions on advanced electronic signatures or the failure to indicate whether an electronic signature will satisfy a statutory signature requirement although for this second aspect, it can be argued that the function played by the electronic signature should suffice to determine whether such an electronic signature satisfies a statutory signature requirement. In respect of the first aspect, this is included in the Electronic Signatures Regulations 2002 discussed below.

4.3.2.1.2 Electronic Signatures Regulations 2002

These regulations implement certain aspects of the eSignature Directive, in particular provisions relating to the supervision and liability of certification service providers. "Advanced electronic signature" is defined in the regulations exactly as it is in the eSignature Directive.[1042] In addition, in terms of Regulation 3 the Secretary of State has a duty to keep under review the carrying out of activities of certain certification service providers, to establish, maintain, and publish a register of these certification service providers, and to have regard to any evidence of their conduct which is detrimental to users of qualified certificates with a view to publication of any of this evidence.

Finally, Regulation 4 imposes liability on the certification service providers in certain circumstances even though there is no proof of negligence unless the certification service provider in question proves that he was not negligent. Mason notes here the shift in the burden of proof which lies in this instance with the service provider while normally the person suffering loss bears the burden of proving negligence. This might result in a situation where qualified certificate issuers may seek an indemnity from the subscribing party against claims by a receiving party, Mason remarks.[1043]

The section on England has discussed the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. The 2000 Act transposes the eSignature Directive into England's national law while the 2002 Regulations deal with certain aspects of this Directive, for example advanced electronic signatures. Both texts constitute the legal framework for electronic signatures in England, complemented by case law. They contribute to the legal recognition and

1042 Regulation 2; see also Ch 4 par 4.3.1.2.2

1043 Mason *Electronic Signatures in Law* (2012) 146

admissibility of electronic signatures. After completing the discussion on England, one may move to the next national initiative provided by the jurisdiction of Singapore.

4.3.2.2 Singapore

The discussion under the jurisdiction of Singapore will focus mostly on the Electronic Transactions Act 2010 although some references will be made to its predecessor, the Electronic Transactions Act 1998.

4.3.2.2.1 The Electronic Transactions Act 2010

The purpose of this Act, and the Electronic Transactions Act 1998 which it repeals, is, amongst other things, to facilitate electronic commerce, eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce.[1044] To address the uncertainty surrounding the signature requirement, section 8 provides as follows:

> Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if —
>
> (a) a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and
>
> (b) the method used is either —
>
> (i) as reliable as appropriate for the purpose for which the electronic record 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 paragraph (a) by itself or together with further evidence.

Before amendment, section 8 read as follows:

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

[1044] S 3(b)

(2) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a party, 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 such party.[1045]

Save for subsection (b)(ii), the provisions of the amended section 8 closely follow article 7 of the Model Law on E-commerce discussed above. Indeed, like the Model Law, the signature requirement in respect of electronic documents will be satisfied by the use of a method able to identify the signatory and to determine his intention, and that method must be appropriately reliable. Contrary to the Model Law, however, the new section 8 includes the possibility of adducing evidence to prove that the method used has actually fulfilled the functions of identification and determination of the signatory's intention notwithstanding the reliability of that method in terms of section 8(b)(i).[1046]

Electronic signature was defined in the 1998 Electronic Transactions Act as including any letters, characters, numbers, or other symbols in digital form attached to, or logically associated with, an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record.[1047] The definition was clearly in harmony with definitions of this concept encountered above. Indeed, it included the existence of an electronic element which had to be attached or logically associated with an electronic record for the purpose of authentication or approval of the record. The noticeable difference is that this definition refers to electronic record rather than data message. A closer look at the definition of "electronic record", however, reveals that the difference is merely semantic. Indeed "electronic record" is defined under both Electronic Transactions Acts as a record generated, communicated, received, or stored by electronic, magnetic, optical, or other means in an information system or for transmission from one information system to another.[1048] In other words, the definition is formulated in similar terms, for example, to the definition of data message under the Model Laws examined above.[1049] The term "electronic signature" has been removed not only from section 8 as illustrated above but also from the list of terms defined under the amendment Act. Hence, the use of the terms

1045 S 8 of the Electronic Transactions Act 1998
1046 S 8(b)(ii)
1047 S 2 of the Electronic Transactions Act 1998
1048 S 2 of both Electronic Transactions Acts
1049 Ch 4 pars. 4.3.1.1.1 and 4.3.1.1.2

"signed" or "signature" is preferred. These terms and their grammatical variations are defined as meaning a method (electronic or otherwise) used to identify a person and to indicate the intention of that person in respect of the information contained in a record.[1050] In *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*,[1051] a name forming part of an e-mail address was held to constitute an electronic signature. It should be noted that, although the Electronic Transactions Act was not applicable in that case because of the exclusion under section 4(1) of the Act to any contract for the sale or other disposition of immovable property, or any interest in such property, the subject matter of this case, the court was satisfied that the common law does not require handwritten signatures for the purpose of satisfying the signature requirements of the relevant statute. A typewritten or printed form is sufficient. The court further stressed that no real distinction can be drawn between a typewritten form and a signature that has been typed onto an e-mail and forwarded with the e-mail to the intended recipient of that message.[1052] Similarly, in *Kim Eng Securities Pte Ltd v Tan Suan Khee*,[1053] the court accepted, on the authority of the previous case, that the defendant's e-mail satisfied the requirements of signature in terms of the Act under examination. The e-mail originated from the defendant and the inclusion of his name "SuanKhee" at the end of the e-mail affirmed his act of signing off.[1054]

The phrase "secure electronic signature" is, however, retained, and it means an electronic signature that is treated as a secure electronic signature by virtue of section 18 or any other provision of this Act. With regard to this type of signature, section 18 states that:

> (1) If, through the application of a specified security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made —
>
> (a) unique to the person using it;
>
> (b) capable of identifying such person;
>
> (c) created in a manner or using a means under the sole control of the person using it; and

1050 S 2(1)
1051 [2005] SGHC 58
1052 *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd*[2005] SGHC 58 at par 91
1053 [2007] 3 SLR 195
1054 *Kim Eng Securities Pte Ltd v Tan SuanKhee* [2007] 3 SLR 195 at par 52

(d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,

such signature shall be treated as a secure electronic signature.

(2) Whether a security procedure is commercially reasonable shall be determined in accordance with section 17(2).[1055]

The definition of "secure electronic signature" is similar to the definition of "advanced electronic signature" provided by both the English Electronic Signatures Regulations and the eSignature Directive discussed above.[1056] Such a type of signature enjoys a presumption which is set out by section 19(2) as follows:

In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that —

(a) the secure electronic signature is the signature of the person to whom it correlates; and

(b) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

In the absence of a secure electronic signature, however, the Act stresses that nothing in Part III[1057] shall create any presumption relating to the authenticity and integrity of the electronic signature.[1058]

An example of a secure electronic signature under the Act is digital signature. The latter is recognised under the Act as a specified security procedure capable of fulfilling the requirements set out in section 18(1).[1059] Digital signature is defined as an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function

1055 S 17(2) provides that whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including — (a) the nature of the transaction;(b) the sophistication of the parties; (c) the volume of similar transactions engaged in by either or all parties;(d) the availability of alternatives offered to but rejected by any party; (e) the cost of alternative procedures; and (f) the procedures in general use for similar types of transactions

1056 Ch 4 par 4.3.2.1.2.and par 4.3.1.2.2 respectively

1057 Part dealing with secure electronic records and signatures

1058 S 19(3)

1059 Second Schedule

such that a person having the initial untransformed electronic record and the signer's public key can accurately determine (a) whether the transformation was created using the private key that corresponds to the signer's public key, and (b) whether the initial electronic record has been altered since the transformation was made.[1060] The asymmetric cryptosystem referred to above is a system capable of generating a secure key pair, consisting of a private key for creating a digital signature and a public key to verify the digital signature, while the hash function mentioned above means an algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that (a) a record yields the same hash result every time the algorithm is executed using the same record as input, (b) it is computationally infeasible that a record can be derived or reconstituted from the hash result produced by the algorithm, and (c) it is computationally infeasible that two records can be found that produce the same hash result using the algorithm.[1061]

A digital signature used to sign a portion of an electronic record shall be treated as a secure electronic signature in respect of such portion provided, on the one hand, that the digital signature was created during the period of validity of the certificate supporting it and can be verified by reference to the public key listed in such certificate, and, on the other hand, the certificate is considered trustworthy, in that it is an accurate binding of a public key to a person's identity.[1062] Information contained in a certificate issued by an accredited certification authority or a recognised certification authority, or in a recognised certificate, is presumed correct if the certificate was accepted by the subscriber. A person who unreasonably relies on a digital signature, however, will bear the risk of such unreasonable behaviour.[1063] Certification authorities, on the other hand, are exempted from liability in respect of false or forged digital signatures if they have complied with the requirements of the Act with regard to these.[1064]

This concludes the discussion on electronic signatures in Singapore which has focused on the Electronic Transactions Act 2010 with a few references to the Electronic Transactions Act 1998. The legal framework in this jurisdiction, which is in harmony with the international initiatives

1060 Par 1(1) of the Third Schedule
1061 Par 1(1) of the Third Schedule
1062 Par 3 of the Third Schedule
1063 Par 5 of the Third Schedule
1064 Par 11(a) of the Third Schedule

above, promotes the use of electronic signatures in Singapore.[1065] Having completed international initiatives as well as national initiatives from two jurisdictions, namely England and Singapore, one may now discuss the last national initiative, which is provided by South Africa and discussed below.

4.3.2.3 South Africa

The discussion on the legal framework for electronic signatures in South Africa will focus mostly on the ECT Act. During the discussion on this statute, however a few references will be made to the Accreditation Regulations.

4.3.2.3.1 The Electronic Communications and Transactions Act 25 of 2002

As its title indicates, the ECT Act provides for the facilitation and regulation of electronic communications and transactions in South Africa. The key provision with regard to electronic signature is section 13. This section adopts the so-called two-tier approach promoted by the Model Laws on Electronic Commerce and Electronic Signatures and followed by a great number of jurisdictions around the world.[1066] It provides for two types of electronic signature, namely an electronic signature and an advanced electronic signature and the effect of both. Before dealing with section 13 *per se*, it seems appropriate to review a couple of definitions such as electronic signature and advanced electronic signature.

A. Definitions

Electronic Signature

"Electronic signature" means, in terms of the ECT Act, any data attached to, incorporated in, or logically associated with other data which is intended by the user to serve as signature.[1067] This definition clearly demonstrates that South Africa has embraced the functional equivalence approach promoted by the Model Laws from which the ECT Act originates. It should, however, be noted that, in contrast to the Model Laws and other definitions discussed above and focusing almost exclusively on the functions of authentication and approval that an electronic signature

1065 Ch 4 par 4.3.1

1066 Such as EU countries implementing the eSignature Directive, including England, or Singapore; for a list of jurisdictions which follow a two-tier approach, see Mason *Electronic Signatures in Law* (2012) 161-164

1067 S1

must fulfil,[1068] South Africa takes a much wider approach as it goes beyond these functions and defines "electronic signature" broadly so that, without any doubt, it can apply easily to any imaginable function of a handwritten signature if this was the user's intention; hence the use of the phrase "serve as signature".

Advanced Electronic Signature

"Advanced electronic signature" is defined as an electronic signature which results from a process which has been accredited by the Accreditation Authority as provided for in section 37 of the ECT Act.[1069] Under section 37, the Accreditation Authority is granted power to accredit authentication products and services in support of advanced electronic signatures, in other words products and services designed to identify the holder of an electronic signature to other persons.[1070] The accreditation can, however, be done only if a certain number of requirements are met, such as those contained in section 38(1):

> 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 the user;
> (c) is created using means that can be maintained under the sole control of that user;
> (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; and
> (e) is based on the face-to-face identification of the user.

Five requirements that an electronic signature must satisfy to qualify as an advanced electronic signature can be highlighted from this provision, namely: unique linkage with the user; capacity to identify the user; creation by means maintainable under the sole control of the user; strong linkage with data allowing the detection of any subsequent change; and face-to-face identification of the user. The first four requirements are identical to those provided by the

---

1068 For example, definitions by the eSignature Directive Ch 4 par 4.3.1.2.2, the English Electronic Communications Act 2000 Ch 4 par 4.3.2.1.1, and the Singapore Electronic Transactions Act 2010 Ch 4 par 4.3.2.2.1

1069 S 1

1070 S 37(1)read with S 1

eSignature Directive and have been extensively analysed earlier.[1071] Requirement (e), however, is an addition to the above Directive and, therefore, deserves a closer look.

Face-to-face identification of the user

It is unclear what this requirement entails as one would assume that requirements (a) and (b) would suffice to identify the user unambiguously. Perhaps the Legislature was simply being extra cautious to ensure the highest level of security in the production of an advanced electronic signature. This requirement, nevertheless, remains a bit confusing; it possibly refers to the issuance of digital certificates in support of advanced electronic signatures. As part of the requirements for issuing certificates, the certification service provider is required to establish the identity of a person or entity applying for the certificate which shall include face-to-face identification of the user or authorised key holder.[1072]

It is submitted that this requirement was not initially included in section 38 (1) of the ECT Act.[1073] Its inclusion came only after a recommendation to Parliament by the South African Post Office (SAPO). It seems, however, that SAPO was acting out of self-interest, as it knew that with its greater footprint it would be best able to carry out the authentication of the identity of applicants and link the applicants to digital certificates.[1074] Unfortunately, over a decade after the promulgation of the ECT Act, SAPO has failed in the face-to-face identification of users and in issuing advanced electronic signatures.[1075]

Other factors

In addition to the above requirements, the Accreditation Authority must consider other factors prior to accrediting authentication products or services, such as, but not limited to: the financial and human resources of the authentication service provider, including its assets; the quality of its

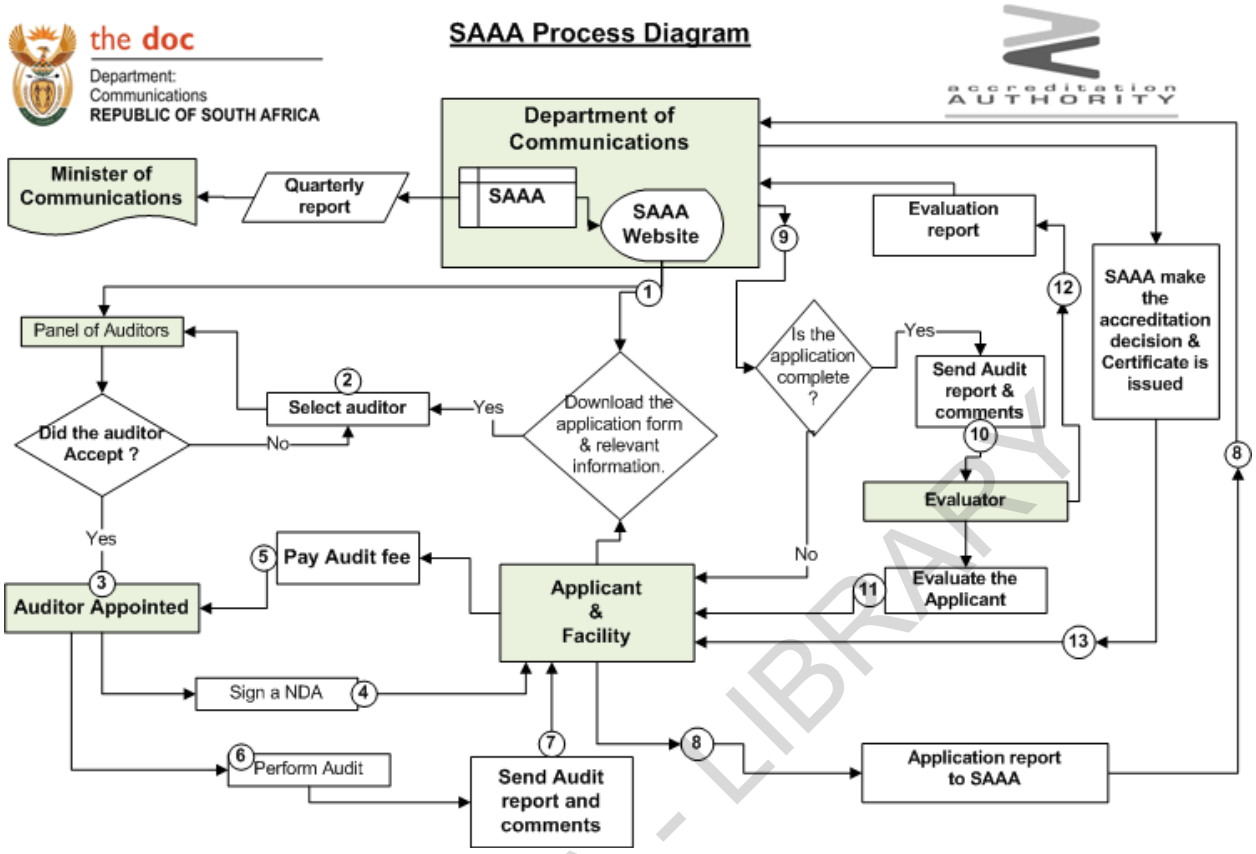
1071 Ch 4 par 4.3.1.2.2
1072 Regulation 14(1)
1073 Heyink *Electronic signatures for South African Law firms* (Guidelines: Oct 2014) (Hereafter referred to as Heyink *Electronic Signatures Guidelines*) 27
1074 Heyink *Electronic Signatures Guidelines* 27
1075 Heyink *Electronic Signatures Guidelines* 27

hardware and software systems; its procedures for processing products or services; or the regularity and extent of audits by an independent body.[1076]

Application for accreditation

The application must be made to the Accreditation Authority in the prescribed manner supported by the prescribed information and accompanied by the prescribed fee.[1077] The application form is available on the South African Accreditation Authority's website www.saaa.gov.za, and the prescribed information is provided in regulation 7 of the Accreditation Regulations.[1078] It includes *inter alia*: the constitutive documents of the applicant; a declaration detailing, amongst other things, the authentication products and services resulting in, and used to, support an electronic signature in respect of which accreditation is sought; procedures in respect of the identification and authentication of subscribers to those products or services, including face-to-face identification; or the manner in which the authentication products or services comply with the requirements of section 38(1) of the ECT Act. If the applicant is a certification service provider, that is, a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in, or logically associated with a data message,[1079] it must provide a copy of its certification practice statement and certification policy drafted in accordance with the Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, as well as a written undertaking that it can and will comply with the requirements of its certification practice statement and certificate policy.[1080] The prescribed fee is R20,000.00 for each authentication product or service resulting in or used in support of an electronic signature.[1081] Below is the journey the application will go through before accreditation.[1082]

1076 S 38(2)
1077 S 37(2)
1078 Regulation 6(1) of the Accreditation Regulations
1079 S 1 ECT Act
1080 Regulation 7(b)
1081 Regulation 29(1)
1082 Flow diagram available on www.saaa.gov.za (accessed on 22/07/2014)



To date, authentication products or services of two companies have been accredited in South Africa: AeSign provided by the company LAWTRUST, an advanced electronic signature solution based on high assurance digital certificate and compatible with any product or service supporting X.509 digital certificate usage;[1083] and the SAPO Trust Centre Advanced Electronic Signature (SAPO Class 4 Certificate) and related digital certificates that are compatible with all applications that support the use of X509 digital certificates.[1084]

A look at the certificates of accreditation issued by the Accreditation Authority, however, reveals some confusion. Indeed the following is stated in the certificates:

> The authentication product/service used in support of an electronic signature is hereby accredited as an advanced electronic signature

This provision is followed directly underneath by the phrase:

1083 www.saaa.gov.za (accessed on 23/07/2014)
1084 www.saaa.gov.za (accessed on 23/07/2014)

(Description of an Authenticated Product / Service)

In respect of the first provision, the wording is clearly confusing as it is appears that authentication products and services are accredited as advanced electronic signatures; whereas the ECT Act provides for the accreditation of authentication products and services capable of producing advanced electronic signatures which meet a set of requirements.[1085] In other words, it is the process of producing advanced electronic signatures which is accredited.[1086] Mark Heyink submits that the wording relating to accreditation is confusing as only authentication products and services in support of advanced electronic signatures are accredited and not the signatures themselves nor the parties who use the products and services to issue advanced electronic signatures.[1087]

Regarding the second provision dealing with the description of the authenticated product or service, it is unfortunate that the certificates issued to date by the Authentication Authority do not contain such a description.[1088] Hence it is not possible to know from the certificate what products and services have been accredited and whether they are, indeed, the products and services on which the authentication service provider relied to provide advanced electronic signatures.[1089]

B. Section 13

This section, dealing with signature requirements, provides as follows:

> (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.

1085 S 37 (1) and 38 (1) of the ECT Act
1086 S 1 of the ECT Act
1087 Heyink *Electronic Signatures Guidelines* 23
1088 Accreditation certificates of both LAWTRUST and SAPO are available respectively at https://www.lawtrust.co.za/documents/DOCCertificate.pdf and https://www.trustcentre.co.za/docs/Accreditation_Award_Certificate.pdf (both accessed on 12 October 2015)
1089 Heyink *Electronic Signatures Guidelines* 23

(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.

With regard to the provision of section 13, the first point to note is that an electronic signature cannot be denied legal force and effect only because it is in electronic form; there must be a substantive reason for any denial, such as lack of technological reliability. As a general rule, however, a requirement for a signature in law will be satisfied electronically only by the use of an advanced electronic signature and such a signature will be presumed to be a valid electronic signature and properly applied. In contrast, when a signature is required by parties transacting electronically without prior consent on the type of the signature, this requirement will be satisfied by the use of a method capable of identifying the signatory and indicating his approval of the electronic communication. In addition, the method must, under the circumstances, be as reliable as appropriate for the purpose of the electronic communication. In conclusion, both types of electronic signatures are admissible in evidence and must be given due evidential weight.[1090]

[1090] S 15 ECT Act

The validity of an electronic signature under the above section was considered in *Spring Forest Trading v Wilberry*.[1091] The court had to decide whether the use of the parties' names at the bottom of their emails constituted signatures in terms of subsections 13 (1) and 13 (3) of the ECT Act.[1092] In respect of subsection 13 (1), the respondent contended that the sentence "where the signature of a person is required by law" should be interpreted widely enough to include the formalities required by both statutes and parties in a contract. Since the parties required their signatures to cancel the contracts binding them, therefore, the use of an advanced electronic signature was necessary.[1093] Cachalia JA rejected such interpretation for two reasons. Firstly, the requirement for signature was agreed by the parties and not imposed upon them by any law, such as under section 6 (12) of the Companies Act 71 of 2008. Secondly, Cachalia JA submitted that the purpose for which an advanced electronic signature is used excludes its application to private agreements between the parties in this case.[1094]

In respect of the first reason, it may be argued that, even if the use of a signature was the result of an agreement between parties, it can still be considered as required by the law if it is accepted that such agreement is law in the eyes of the signatories. Such an argument, however, cannot resist the juxtaposition of subsection 13 (1) with subsection 13 (3). Reading both sections together one comes to the conclusion that section 13 of the ECT Act distinguishes between the case where a signature is required by law in the strict sense (subsection 13 (1)) and where a signature is agreed by parties (subsection 13 (3)). Cachalia JA is, therefore, right.[1095]

As to the second reason provided by Cachalia JA, it should not have been necessary as it is correctly submitted that subsection 13 (1) does not apply in this case because the signature is required not by law as envisaged in the subsection but by virtue of the agreement of the parties.[1096] Since, however, Cachalia JA suggests that the purpose of an advanced electronic signature is the reason that prevents it from being used between private parties, it is appropriate to assess the validity of such submission.

1091 (725/13) [2014] ZASCA 178

1092 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [17]

1093 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [19]

1094 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [20]

1095 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [18]

1096 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [20]

It is not very clear what Cachalia JA considers to be the purpose of an advanced electronic signature. Apparently, he seems to suggest that such purpose is to be "used for accredited 'authentication products and services' which are designed to identify the holder of the electronic signature to other persons."[1097] If this is the case, then Cachalia JA must have misread the definition of "advanced electronic signature" in terms of section 1 read with section 37 (1) of the ECT Act. Indeed, it is clear from the definition that an advanced electronic signature is the product of authentication products and services which have been accredited by the Accreditation Authority, and its purpose is not to be used for these authentication products and services but rather to be used for any transaction for which parties decide to use it. The erroneous interpretation of the purpose of an advanced electronic signature by Cachalia JA led him to believe that parties must be involved in the business of providing authentication products and services to require advanced electronic signatures for their contracts.[1098] This is not correct, as nothing in the ECT Act prevents parties from agreeing to the use of an advanced electronic signature for any type of transaction.[1099]

As far as subsection 13 (3) is concerned, the respondent submitted that, even if that subsection was applicable, it could not assist the appellant for three reasons. Firstly, the emails did not, and could not, constitute a separate electronic transaction as they related to the oral negotiations about the written agreements. Secondly, even if they were considered as separate electronic transactions, an electronic signature as contemplated in the section was not required by parties. Finally, there was no reliable method used to identify parties and indicate their approval of the information contained in the emails.[1100]

In response, Cachalia JA held, regarding the first ground, that the emails constituted a separate transaction consisting of the reduction in writing of the oral negotiations between parties and, therefore, constituted an agreement to cancel their written agreements.[1101] To back his submission further, Cachalia JA relied on section 22 (1) of the ECT Act in terms of which an

1097 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [21]
1098 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [22]
1099 S 13(3) of the ECT Act suggests that parties are free to agree on any type of electronic signature they want to use for their electronic transaction.
1100 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [23]
1101 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [24]

agreement should not be denied legal force and effect solely on the ground that it was concluded in part or in whole by means of data messages.[1102]

On the second ground relating to the requirement of an electronic signature, Cachalia JA started by discussing the approach of courts towards signatures in general and he held, as already noted in this thesis, that such an approach is pragmatic and not formalistic. That means that one needs to examine the method of signature used and determine whether it fulfils the function of a signature of authenticating the identity of the signatory rather than focusing on the form.[1103] Applying this approach to the facts in the case, Cachalia JA held that the parties' names at the bottom of their emails constituted valid signatures as they were put there by the users to serve as signatures, they were logically connected with other data in the emails, and they, therefore, complied with the definition of electronic signature.[1104]

On the third and last ground relating to the absence of a reliable method to identify parties and indicate their approval of the information contained in the emails, Cachalia JA found no merit in such an argument as there was no dispute on the reliability of the emails, on the accuracy of the information contained in the emails, or on the identities of the persons whose names appeared at the foot of the emails.[1105]

Another piece of legislation providing for the requirement of signature is the Wills Act 7 of 1953.[1106] Although this Act is excluded from the application of the ECT Act,[1107] it deserves some attention as it was the subject matter of a case involving the application of a signature in the electronic environment. The relevant case is *Macdonald v The Master*.[1108] This case dealt with an application for an electronic document to be accepted as the will of the deceased under the Wills Act. In the hypothesis that the ECT Act was applicable, it means that the use of an advanced electronic signature would have been necessary to comply with the signature requirement in accordance with section 13(1) of the ECT Act. This requirement was not complied with. It must be stressed, however, that the applicant relied on section 2(3) of the Wills

1102 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [24]
1103 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [25] & [26]
1104 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [27] & [28]
1105 *Spring Forest Trading v Wilberry* (725/13) [2014] ZASCA 178 at [29]
1106 S 2(1)(a)
1107 S 4 read with Schedule 2
1108 2002 (5) SA 64

Act which permits, under certain circumstances, the acceptance of a will that does not comply with the signature requirement or other formalities. The facts in this case are as follows; the deceased committed suicide and left some notes on the bedside table next to the bed on which he was lying. One note read:

> I, Malcom Scott MacDonald, ID 5609065240106, do hereby declare that my last will and testament can be found on my PC at IBM under directory:/WINDOWS/MYSTUFF/MYWILL/PERSONAL.[1109]

The deceased was a senior IT specialist in the employ of IBM. He had a personal computer at his office and was the only one to have access to it as the computer was protected by a password that was known only to him. As part of the company's policy, each employee had to submit his password in a sealed envelope to the designated employee to be kept safely. After his suicide, therefore, access to his PC was gained and the file referred to in the above note was found and printed. The printed document was entitled:

> LAST WILL AND TESTAMENT FROM MALCOM SCOTT MACDONALD

The first paragraph read:

> I, the undersigned, Malcom Scott MacDonald (ID 5609065240106), divorced, do hereby revoke all wills, codicils and other testamentary acts heretofore made by me and declare the following to be my last will and testament.

The document also contained provisions relating to the executor and the disposition of the deceased's property. The document was, however, not signed.[1110] The Master, consequently, refused to accept the will as it did not comply with the formalities imposed by section 2(1)(a) of the Wills Act, such as to be signed, attested by two competent witnesses, and initialled by the testator on each page.[1111] With regard to the signature of the testator, Mason notes that, although the latter did not sign his name in the document, it can be argued that the use of a password served a similar function.[1112]

1109 *Macdonald v The Master* 2002 (5) SA 64 at p 65
1110 *Macdonald v The Master* 2002 (5) SA 64 at p 68
1111 Mason *Electronic Signatures in Law* (2012) 206
1112 Mason *Electronic Signatures in Law* (2012) 208

Under section 2(3) of the Wills Act, to be successful in their application, the applicants had, on balance of probabilities, to establish that:

(a) The documents, annexures A and F were drafted by the deceased;
(b) That the deceased has died since the drafting of the documents; and
(c) The documents were intended by the deceased to be his will.[1113]

The court was satisfied that all these requirements had been established by the applicant.[1114]

C. Section 18 Notarisation, acknowledgment, and certification

Section 18 deals with instances where the law provides for more stringent requirements, such as the notarisation, the acknowledgment, or the certification of signatures. It reads as follows:

> (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.

The effect of this provision is that the electronic notarisation of documents in general, and of signatures in particular, is now a reality in South Africa, especially with the accreditation of authentication products and services in support of advanced electronic signatures of two companies. It is, further, interesting to note that it is now possible to certify a paper document electronically. This can be done by scanning the document and certifying the electronic copy

1113 *Macdonald v The Master* 2002 (5) SA 64 at p 72

1114 See also Snail and Hall "Electronic Wills in South Africa" in 2010 *Digital Evidence and Electronic Signature Law Review* 7 (hereafter referred to as Snail and Hall "Electronic Wills in South Africa") 67-70

using an advanced electronic signature.[1115] In the same vein, a document may be sealed by electronic means. Indeed a requirement for a seal in law will be 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.[1116]

D. Liability of certification service providers

Apportionment of liability must be determined in a certification service provider's certification practice statement in accordance with SANS 21188. The certification service provider cannot, however, exclude liability resulting from its own gross negligence.[1117]

This discussion on South Africa concludes the section on national initiatives relating to electronic signatures after England and Singapore. Electronic signatures are governed in South Africa by the ECT Act. This Act adopts the so-called two-tier approach promoted by the Model Laws on Electronic Commerce and Electronic Signatures by providing for two types of electronic signature, namely an electronic signature and an advanced electronic signature and the effect of both. The Act was analysed and similarities with the Model Laws and the eSignature Directive highlighted. For example the definition of advanced electronic signature is almost identical in the ECT Act and the eSignature Directive meaning that comments which were made for the latter were relevant for the former.[1118] The discussion extended to the application procedure for advanced electronic signatures, in other words the accreditation and to circumstances where the law requires a signature and how an electronic signature can satisfy such requirement. Attention was also given to more stringent conditions regarding signatures, for example the electronic notarisation. Finally regard was made to case law with a couple of cases which have considered the use of an electronic signature and its legal effect. Now that the legal framework of electronic signatures has been explored through international and national initiatives, one may look at a certain forms of electronic signatures.

4.3.3 Forms of electronic signatures

1115 S 18(3)
1116 S 19(3)
1117 Regulation 19 of Accreditation Regulations
1118 Ch 4 par 4.3.1.2.2 A & par 4.3.2.3.1

Seven examples of electronic signatures are discussed below. They include typing a name, clicking, browse wrap, personal identification number and password, e-mail address, scanned manuscript signature and digital signature.

4.3.3.1 Typing a name

Typing a name in an electronic document is widely accepted as a form of electronic signature. Mason reports that this method was accepted in the UK even before the passing of the Electronic Communications Act 2000, as illustrated by the case of *Hall v Cognos Limited*,[1119] in which a series of emails between Mr Hall and his line manager (containing at the bottom the names "Sarah" and "Keith") were held to be signed when printed and to vary the terms of the written contract of employment. Similarly to the UK, this form of electronic signature has been accepted in various other jurisdictions. In the Australian case of *Faulks v Cameron*,[1120] the court was satisfied that the printed signature on the defendant's emails constituted a valid signature. The Missouri Court of Appeals reached the same conclusion in an exchange of e-mail communications relating to the termination of a lease in *Crestwood Shops, LLC v Hilkene*.[1121] In addition, in *Haywood Securities, Inc v Ehrlich*,[1122] the Supreme Court of Arizona held that the name of a judge typed in a judgment constitutes a signature. The same decision was reached with regard to the names of attorneys typed at the bottom of e-mails in the case of *Kloian, d/b/a Arbor Management Company v Domino's Pizza, LLC*.[1123]

4.3.3.2 Clicking

Clicking an "I accept" or "I agree" icon is an act that satisfies the function of a signature. Indeed it is capable of providing evidence of the process that is executed or adopted by the person

1119 Industrial Tribunal Case No 1803325/97; Mason *Electronic Commerce* (2010) 331
1120 [2004] 32 Fam LR 417;[2004] NTSC 61; cited by Mason *Electronic Signatures in Law* (2012)194
1121 197 S W 3d 641 (Mo App WD 2006); cited by Mason *Electronic Signatures in Law* (2012) 194
1122 149 P3d 738 (Ariz 2007); cited by Mason *Electronic Signatures in Law* (2012) 202
1123 733 N W 2d 766 (Mich App 2006); cited by Mason *Electronic Signatures in Law* (2012) 202

clicking on the icon.[1124] This method of expressing intent has been widely accepted in the USA.[1125] With regard to the English jurisdiction the method is discussed elsewhere.[1126]

4.3.3.3 Browse wrap

This method of indicating knowledge is mainly present in the USA where it is commonly referred to as "browse wrap" agreements. Under these agreements, one party imposes its terms of use or sale on another party who is bound by using the website. Thus, by browsing the website, the visitor indicates knowledge of the relevant terms which must, however, be conspicuous.[1127]

4.3.3.4 Personal Identification Number and password

A PIN is a numeric password shared between a user and a system that can be used to authenticate the user to the system.[1128] Arguably the oldest form of electronic signature, a PIN is widely used to access a bank account through an ATM or to confirm a transaction with a credit or debit card.[1129] Its origin can be traced back to the introduction of ATMs in 1967.[1130]

The use of PINs has given rise to numerous claims. The main concern in these claims is to determine whether it was the account holder or somebody else who was responsible for withdrawals made from the account using the correct PIN or password. The oldest cases in this regard can be found in the USA. In the 1980 American case of *Judd v Citibank*,[1131] the plaintiff discovered two withdrawals made from her account using a cash card and PIN while she was at work. The issue was to believe the plaintiff or the printout of the transactions from the machine. The court was satisfied that the plaintiff proved her case "by a preponderance of credible evidence".[1132] In contrast, in the 1981 cases of *Feldman v Citibank, N.A.; Pickmanv Citibank,*

1124 Mason *Electronic Signatures in Law* (2012) 215

1125 Mason lists various cases, including *CompuServe, Incorporated v Patterson*, 89 F 3d 1257 (6th Cir 1996); *M A Mortenson Company, Inc v Timberline Software Corporation*, 998 P 2d 305 (Wash 2000); *Person v Google Inc* , 456 F Supp 2d 488 (S D N Y 2006); Mason *Electronic Signatures in Law* (2012) 216-219

1126 Ch 4 par 4.3.2.1.1.B

1127 Mason *Electronic Signatures in Law* (2012) 220

1128 http://www.businessdictionary.com/definition/personal-identification-number-PIN.html (accessed on 28/08/2014)

1129 Mason *Electronic Signatures in Law* (2012) 221

1130 http://www.history.com/topics/inventions/automated-teller-machines(accessed on 29/08/2014)

1131 N Y City Civ Ct, 435 N Y S 2d 210

1132 Mason *Electronic Signatures in Law* (2012) 222

N.A,[1133] the plaintiffs in both cases were held liable for withdrawals from their accounts. Mr Feldman was victim of a deceiving scheme leading him to cooperate unwittingly with the thief. The court held that Mr Feldman was liable for the unauthorised ATM transaction because he had unwittingly allowed a thief to withdraw money from his account.[1134] Ms Pickman, on the other hand, discovered that six withdrawals had been made from her account during a period of three months. As she did not alert the bank after noticing the first unauthorised transaction, the court followed a recommendation by the National Commission on Electronic Fund Transfers in terms of which, if a customer fails to notify the bank of a disputed transaction, the customer will be liable for any subsequent use that could have been prevented if the customer had notified the bank in a timely manner. Thus, Ms Pickman could recover for only the first unauthorised withdrawal.[1135]

In England, PC John Munden was charged and convicted for attempting to obtain money by deception after he had complained of six unauthorised transactions on his account from ATMs. His conviction was, however, set aside in appeal because the defence was denied information about the computer systems, records, and operational procedures of the bank.[1136]

In South Africa, the use of a PIN was considered in *Diners Club SA (Pty) Ltd v Singh and another*.[1137] In this case, the plaintiff, a credit card business operator, sued the defendants (a husband and wife) and alleged that the first defendant's credit card and PIN had been used to make ATM withdrawals in London. The defendants claimed, on the other hand, that the first defendant had not gone to London that weekend, that his card was at all times in his possession, that his PIN had not been given to anyone, and that some unknown person or persons had made the withdrawals.[1138] In addition, the defendants alleged that they were not aware of the latest amendments to the terms and conditions of issue of a card, in terms of which a cardholder would

1133 N Y City Civ Ct, 443 N Y S 2d 43;(two cases brought into one hearing)
1134 Mason *Electronic Signatures in Law* (2012) 223
1135 Mason *Electronic Signatures in Law* (2012) 222
1136 Mason *Electronic Signatures in Law* (2012) 224
1137 2004 (3) SA 568 (D)
1138 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 568 e

be liable if his PIN was used by any person whatsoever.[1139] They further argued that such a clause was *contra bonos mores*.

Various expert witnesses testified on behalf of the defendants on the operation of PINs and ATMs. One witness testified that, before an ATM is activated, two things must coincide, the magnetic strip on the card and the PIN. In addition, he pointed out that a PIN performs an authentication function; when it is inserted, the ATM ties the account number and the PIN together and permits the transaction.[1140]

Another witness described the operation of ATMs of different generations. According to him, the first generation was somewhat primitive and vulnerable to attack by fraudsters.[1141] The second generation of ATMs used enciphered PINs. Each ATM had its own small computer, and it would perform an encryption function. The particular ATM would have a particular link to the bank's mainframe computer. There were two methods of authenticating the customer, namely the PIN and the magnetic strip.[1142] The concern with second generation ATMs occurred when the bank's mainframe was offline in that a customer entering his card and PIN in an ATM not communicating with the bank's mainframe would be allowed to take a certain amount of money even if he could not do a balance enquiry. This concern led to the design of a new system whereby the card's magnetic strip would obtain encrypted information with regard to the PIN. When the card was inserted into the ATM, the encryption key which would be known to the ATM would be a means of verifying the PIN offline.[1143] This system was still unsatisfactory according to the witness since it did not protect against dishonest insiders because, as he observed, if you have a PIN master key sitting around in the ATM there is a risk that ATM repairmen might access it and so be in a position to forge cards. Similarly, if the PIN master key is sitting around in the software of the bank's mainframe, there is a risk that programmers will eventually find its value.[1144]

1139 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 568 g
1140 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 573 f and h
1141 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 574 b
1142 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 574 d
1143 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 574 e-f
1144 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 574 h

The witness then testified that the next generation of ATMs was linked to a network such as SASWITCH in South Africa. This involved doing the encryption by means of tamper-resistant processers which prevent programmers, repairmen, and the like from getting hold of the PIN. These processers are known as hardware security modules (HSMs) or black boxes. They serve to keep the PIN master key and all other information on which the authentication of customers depends safe. The HSMs are kept in a locked room to prevent people from obtaining physical access to them, and they have a printer attached to them so that it is possible to print out PINs in a secure environment.[1145] With the development of network systems the encryption process becomes more and more complex.[1146] The witness later revealed that research showed that HSMs did not give as much protection against insiders as had previously been believed.[1147]

In this case, the expert witness was of the view that the most likely culprit was an insider at Diners Club International server centre in the United Kingdom, who probably ran software to interrogate the security module to get information. He was also of the view that, in order to access the 199 transactions in this case, it was likely that the PIN and a card were used; the card was probably forged in the UK by someone who had access to PAN details and someone with access to PINs.[1148]

With regard to this expert evidence suggesting the possibility that the withdrawals were made by a third party, the court held that it was irrelevant who had accessed the PIN and fraudulently withdrawn the money, because, under the agreements, defendants were nonetheless liable. The court, however, considered the evidence as to who had withdrawn the funds and was satisfied that there was a strong preponderance of probability that the withdrawals had been made by associates of the first defendant in complicity with the latter.[1149]

As to the *contra bonos mores* argument, the court dismissed it, holding that the plaintiff is entitled to protect itself by placing the risk of wrongful use of the card on the customer. The

1145 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 574 i-j
1146 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 575 c
1147 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 576 e
1148 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 577 a and g
1149 *Diners Club SA (Pty) Ltd v Singh and another* 2004 (3) SA 568 (D) at 569 a-b

ruling on this point seems to be harsh considering the relative ease by which a PIN can be obtained without the consent of the cardholder.[1150]

4.3.3.5 E-mail address

In the analysis of an e-mail address as a form of an electronic signature, it is submitted that the purpose of the e-mail address is of the utmost importance.[1151] According to Mason, an e-mail address ensures that the electronic communication reaches the person it is addressed to, and, if it is accepted that the "From" line of an email acts to designate the sender, then the act of signature is the irrevocable despatch of the e-mail.[1152] Mason links this submission to the view of the English Law Commission indicating that clicking constitutes the technological equivalent of signing with a mark, and is, therefore, a signature. Similarly, the action of clicking the "send" icon of an e-mail page is an act of authentication and constitutes a signature.[1153]

An e-mail address has been held as a form of electronic signature in a number of jurisdictions. A Singapore case discussed above illustrates this.[1154]

Similarly, in the Australian case of *McGuren v Simpson*,[1155] the court held that an e-mail address was a signature for the purpose of a section that required an acknowledgment to be in writing and signed by the maker.

In the USA, the same decision was reached in *JSO Associates, Inc. v Price*.[1156] The source and authenticity of the e-mail were not in issue in this case, and it was, therefore, determined that the e-mail had been signed.[1157]

In England and South Africa, electronic signature is defined under section 7(2) of the Electronic Communications Act 2000 and section 1 of the ECT Act respectively.[1158] The question that arises is whether an e-mail address can be considered to be an electronic signature in terms of

1150 This is the view taken by Mason *Electronic Signatures in Law* (2012) 225
1151 Mason *Electronic Signatures in Law* (2012) 239
1152 Mason *Electronic Signatures in Law* (2012) 239
1153 Mason *Electronic Signatures in Law* (2012) 241
1154 *SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd* [2005] SGHC 58;Ch 4 par 4.3.2.2.1
1155 [2004] NSWSC 35;cited by Mason *Electronic Signatures in Law* (2012) 227-229
1156 2008 WL 904703 (N Y Sup), 239 N Y L J 72, 2008 N Y Slip Op 30862 (U)
1157 Mason *Electronic Signatures in Law* (2012) 242
1158 See Ch 4 par 4.3.2.1.1.par 4.3.2.3.1 respectively

these statutes. To answer this question, it is necessary to consider the elements of an electronic signature under these statutes.

The first element is "anything in electronic form" for England and "data or electronic representation of information in any form" for South Africa. There is no doubt that an e-mail address complies with this element as it represents information in electronic format.

The second element refers to the incorporation of, or the logical association between, the information in the first element and any other data. The link between the e-mail address and the electronic mail cannot be disputed, as the electronic mail will not arrive at its destination without a correct e-mail address; a slight difference in the e-mail address even by one letter, number, or dot will have devastating consequences as the electronic mail will not reach its destination.

The third element, finally, requires the information "to be incorporated into or logically associated with other data with the purpose of being used to establish authenticity or integrity" in England or "to be intended by the user to serve as a signature" in South Africa.

The third requirement looks more problematic. In the case of England, to qualify as an electronic signature an e-mail address must be incorporated or logically associated with an e-mail with the purpose of being used to establish the authenticity or integrity of the e-mail. While accepting the logical association that exists between an e-mail address and an e-mail as explained above, and the fact that an e-mail address can serve as a means of establishing authenticity, it is debatable whether the purpose of putting an e-mail address is to authenticate the e-mail, at least not from a sender point of view, where an e-mail address serves only to indicate the addressee of the e-mail and has no other purpose. An e-mail address is not different from a postal or physical address on an envelope which is not put for the purpose of establishing the authenticity of the content but simply to indicate the recipient of the mail. The situation might be different if considered from the recipient's point of view. The sender's e-mail address contained in the e-mail received by the recipient can clearly be used to authenticate the e-mail; it can, however, be debated whether it was included by the sender for that specific purpose, as, generally, the sender's e-mail address will be included automatically in the e-mail without the sender's knowledge. It is my submission there is uncertainty about whether an e-mail address falls within the definition of electronic signature under section 7(2) of the Electronic Communications Act 2000. This submission is,

unfortunately, not shared by Mason who strongly believes that an e-mail address comes under the provisions of this section as it is in electronic form, and the name included in the e-mail address is included with the purpose of establishing the authenticity of the content.[1159] He insists that, even if the name included is a nickname or pseudonym, the same conclusion would apply.[1160]

In the South African scenario, it is even more doubtful that an e-mail address will fall within the definition of electronic signature in terms of the ECT Act. Indeed, to be considered to be an electronic signature under this Act, the e-mail address must be included in the e-mail by the user with the intention that it serves as a signature. As explained above, the reason why the user or the sender includes the recipient's e-mail address in an e-mail is only to indicate the destination of the e-mail. As to the inclusion of the sender's e-mail, this process will normally be done automatically, and, thus, there is no intention by the sender to include it, let alone for it to serve as a signature. It can, therefore, be concluded without doubt that an e-mail address is not an electronic signature in terms of the ECT Act.

In contrast, there is no uncertainty that an e-mail address will qualify as an electronic signature in terms of the eSignature Directive.[1161]

4.3.3.6 Scanned manuscript signature

As noted above, a scanned manuscript signature incorporated into a document is capable of indicating to the recipient that the signatory had the necessary authenticating intention, in the same way as an original manuscript signature would.[1162] This view was supported by Laddie J in *Re a Debtor* (No2021 of 1995) who considered a scanned manuscript signature incorporated in a document and then faxed to the recipient and held that such document was signed by the author. Mason concurred with this view while stressing that the sending party must have

1159 Mason *Electronic Signatures in Law* (2012) 243

1160 Mason *Electronic Signatures in Law* (2012) 243

1161 The eSignature Directive defines electronic signature as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.

1162 English Law Commission *Electronic Commerce* 14; see also Ch 4 par 4.3.2.1.1 B

intended the recipient to accept such a signature as a method of authentication and to act upon the content of the document transmitted.[1163]

It should be stressed, however, that scanned manuscript signatures have faced challenges in various jurisdictions. In France it was held that a manuscript signature did not fall within the definition of an electronic signature under article 1316-4 of the French Civil Code. Surprisingly, however, the dismissal letter on which the scanned signature was affixed was held to be signed.[1164]

In Denmark, scanned signatures affixed to the cancellation endorsement of a mortgage were held to be invalid.[1165]

Closely connected to a scanned manuscript signature is a biodynamic version of a manuscript signature (biodynamic signature). This form of electronic signature relies on authentication through a biometric device based on manuscript signatures. It is produced by signing manually on a computer screen or digital pad by means of a special pen. The manuscript signature is then analysed by the computer and stored as a set of numerical values which can be appended to a data message and displayed by the relying party for authentication purposes. These numerical values, representing the behaviour of the signer during the signing process, include the speed, rhythm, pattern, habit, stroke sequence, and dynamics unique to the individual at the time of signing. Such an authentication system would presuppose that samples of the manuscript signature have been previously analysed and stored by the biometric device.[1166] According to Mason, although this concept might be usefully applied in an electronic environment, it does, nevertheless, present drawbacks as with any other form of generating electronic signatures, such as, for example, the difficulty of linking the evidence in a coherent manner to prove that a

1163 Mason *Electronic Signatures in Law* (2012) 254

1164 Case of the Cour de Cassation, soc 17 May 2006, 04-46706; it should be noted that this ruling was made at the Court of Appeal in this unfair dismissal case. A second appeal was lodged to the Cour de Cassation, the highest French civil court, which did not specifically address this point; it held, however, that there were substantive justifiable grounds for the dismissal.

1165 Mason *Electronic Signatures in Law* (2012) 255; read also Christianson & Mostert "Digital signatures" May 2000 *De Rebus* 26 (hereafter referred to as Christianson & Mostert "Digital signatures")

1166 Par 33 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

particular person signed the particular document, or problems relating to the protection of personal data.[1167]

In Australia, the biodynamic signature of a voter was refused by the Electoral Commissioner in the case of *Getup Ltd v Electoral Commissioner*.[1168]

4.3.3.7 Digital signature

Digital signatures will be discussed by referring firstly to the description of the functioning of a digital signature system and secondly, to the public-key infrastructure and certification service providers.

4.3.3.7.1 Description of the functioning of a digital signature system

Digital signatures are created and verified by cryptography.[1169] They rely on public-key cryptography which employs an algorithm using two different, but mathematically related, keys; one key serves to create a digital signature or transform data into a seemingly unintelligible form, and another key serves to verify a digital signature or return the message to its original form.[1170] The key used to create a digital signature is termed "private key" and is known only to the signer while the corresponding key, termed "public key", is ordinarily more widely known and used by the relying party to verify the signer's digital signature. Computer equipment and software that use two such keys are often collectively referred to as an "asymmetric cryptosystem".[1171] It is suggested that, if the asymmetric cryptosystem is designed and implemented securely, although the keys are mathematically related, it is computationally infeasible to derive the private key from knowledge of the public key.[1172] The fact that the public key of a given signer used to verify the signer's signature is, therefore, known by many people does not mean that these

1167 Mason *Electronic Signatures in Law* (2012) 256

1168 [2010] FCA 869 (13 August 2010)

1169 Cryptography is the branch of applied mathematics dealing with the transformation of messages into seemingly unintelligible forms and back again

1170 American Bar Association (ABA) *Digital Signatures Guidelines* 1996 (hereafter referred to as ABA *Digital Signatures Guidelines*) 9

1171 ABA *Digital Signatures Guidelines* 9

1172 ABA *Digital Signatures Guidelines* 9

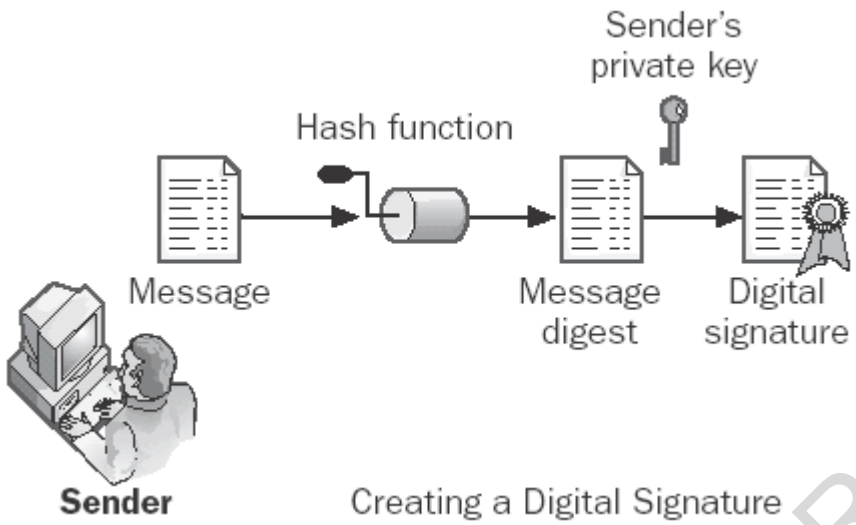
people can discover the signer's private key and use it to forge digital signatures; in fact, they cannot. This is why this process is sometimes referred to as the principle of irreversibility.[1173]

In addition to the existence of the above two keys, another fundamental process, known as "hash function", plays a critical role in the creation and verification of a digital signature. A hash function is an algorithm which creates a digital representation or compressed form of a message, often referred to as a "message digest" or a "fingerprint" in the form of a hash value or hash result of a standard length which is usually much smaller than the message but, nevertheless, substantially unique to it. Any change to the message invariably produces a different hash result when the same hash function is used.[1174] The hash function enables the software used to create digital signatures to operate on smaller and predictable amounts of data while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.[1175]

The creation of a digital signature involves the use of a hash result derived from and unique to both the signed message and a given private key. The hash result will be considered secure only if the possibility that the same digital signature could be created by the combination of any other message or private key is negligible. The digital signature creation process, as illustrated in Figure 1 below, operates as follows. Firstly, the signer needs to delimit precisely the limits of what is to be signed. Secondly, a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. Thirdly, the signer's software transforms the hash result into a digital signature using the signer's private key. The resulting digital signature is, thus, unique to both the message and the private key used to create it.[1176]

1173 ABA *Digital Signatures Guidelines* 10
1174 ABA *Digital Signatures Guidelines* 10-11
1175 ABA *Digital Signatures Guidelines* 11
1176 ABA *Digital Signatures Guidelines* 11

Figure 1 Digital signature creation[1177]



Digital signature verification, on the other hand, is the process of checking the digital signature by reference to the original message and a given public key thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.[1178] This process is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the recipient will check two things: firstly, whether the digital signature was created with the corresponding private key; and, secondly, whether the newly-computed hash result matches the original hash result which was transformed into the digital signature during the signing process.[1179] If the response to these two questions is positive, in other words if it is established that the signer's private key was used to digitally sign the message and that the message has remained unaltered, the verification software will confirm the digital signature as verified.[1180] Figure 2 below illustrates this process.

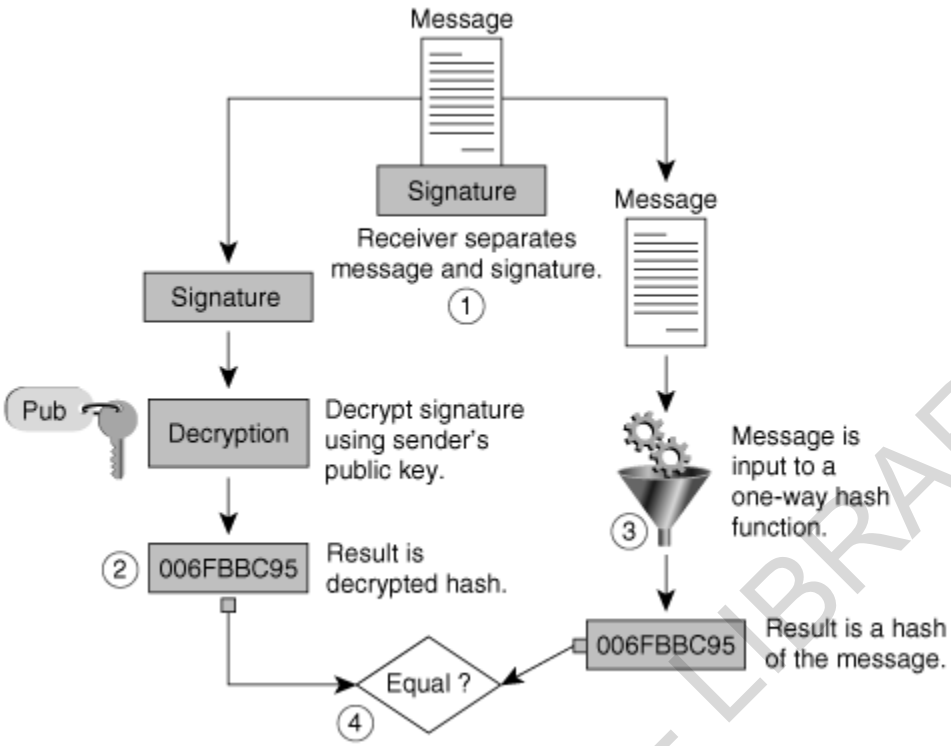
1177 Available at http://www.exploit-db.com/wp-content/themes/exploit/docs/14963.pdf (accessed on 06/08/2014)

1178 ABA *Digital Signatures Guidelines* 11

1179 ABA *Digital Signatures Guidelines* 11

1180 ABA *Digital Signatures Guidelines* 11

Figure 2 Digital signature verification process[1181]



A digital signature can accomplish the essential effects desired of a signature from a legal point of view, such as the authenticity of the identity of the signer or the integrity and the non-repudiation of the message. It ensures the authenticity of the identity of the signer by the use of a public and private key pair associated with an identified signer which makes it possible to attribute the message to the signer. This is even reinforced by the fact that the digital signature cannot be forged unless the signer loses control of the private key.[1182] The integrity of the

1181 Available at http://etutorials.org/Networking/Wireless+lan+security/Chapter+2.+Basic+Security+Mechanics+and+Mechanisms/Security+Mechanics/ (accessed on 06/08/2014)

1182 ABA *Digital Signatures Guidelines* 13; to avoid the risk of forgery, it is recommended that: (1) the subscriber, who holds the private key, should use a degree of care in its safekeeping; and (2) the subscriber must be able to disassociate himself from the key by temporarily suspending or permanently revoking his certificate and publishing these actions in a "certificate revocation list", or "CRL". In addition, it is important to use safe storage methods, for example to store the private key in a "cryptographic token" (such as a smart card), "which executes the signature program within an internal microprocessing chip, so that the private key is never divulged outside the token and does not pass into the main memory or processor of the signer's computer. The signer must typically present to the token some authenticating information, such as a password, pass phrase, or personal identification number, for the token to run a process requiring access to the private key. In addition, this token must be physically produced, and biometric authentication such

message can also be accomplished by the use of a digital signature with greater certainty and precision than the use of a manuscript signature. Indeed, as described above, the verification process can reveal any tampering with the message. Finally, the evidence of both the identity of the signer of a message and of message integrity will prevent the repudiation of the message by the parties. The signer will not be able to deny the signing of the message, on the one hand, while the recipient will be precluded from denying the origin, submission or delivery of the message, and the integrity of its content, on the other hand.[1183]

It has been stressed above that in order to verify a digital signature, the verifier must have access to the signer's public key. In addition, he must have the assurance that the public key corresponds to the signer's private key. How does the verifier acquire access to the signer's public key and obtain certainty that such public key corresponds to the signer's private key? He can do so by approaching a trusted third party to associate an identified signer with a specific public key.[1184] That third party is generally referred to as a "certification authority", "certification service provider", or "supplier of certification services" in most technical standards and guidelines. In a number of countries, such certification authorities are being organised hierarchically into what is often referred to as a "public-key infrastructure" (PKI).[1185]

4.3.3.7.2 Public-key infrastructure and certification service providers

The following lines give an overview in two points (A and B) of the PKI and the certification services providers.

A. Public-key infrastructure

A PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. Such digital certificates are used to verify that a particular public key belongs to a certain entity.[1186]

---

as fingerprints or retinal scan can assure the physical presence of the token's authorized holder." ABA *Digital Signatures Guidelines* footnote 20.

1183 ABA *Digital Signatures Guidelines* 54

1184 ABA *Digital Signatures Guidelines* 16

1185 Par 49 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

1186 Oei "Digital Signatures" 52

The whole PKI system provides confidence, on the one hand, that the user's public key has not been tampered with and, in fact, corresponds to that user's private key, and, on the other hand, that the cryptographic techniques being used are sound. To ensure such confidence, a PKI may provide various services, such as:"(a) managing cryptographic keys used for digital signatures; (b) certifying that a public key corresponds to a private key; (c) providing keys to end users; (d) publishing a secure directory of public keys or certificates; (e) managing personal tokens (e.g. smart cards) that can identify the user with unique personal identification information or can generate and store an individual's private keys; (f) checking the identification of end users, and providing them with services; (g) providing time-stamping services; and (h) managing cryptographic keys used for confidentiality encryption where the use of such a technique is authorized."[1187]

In broad terms, there are two categories of PKI, namely a closed environment, and an open environment. The first category uses only one domain for all communications. The domain is located either in a single place for a single enterprise, or consists of a set of enterprises, each of which operates under the same set of technical and operational procedures. For example, a multinational company operating in several jurisdictions may maintain an intra-company domain across the world; or a group of end users consisting of both sending and receiving parties may enter a network with one or more certification authorities under which liability is determined according to agreed contractual terms between the parties, as with IdenTrust or Bolero.[1188]

An open environment relies on the existence of certification service providers which act to certify the link between a person and their public key. These organisations are discussed below.

B. Certification service providers

The principal function of a certification service provider is to issue a certificate, an electronic record, which binds a public key with a particular signer. The certificate shall contain, amongst other things, the following: the identity of the certification service provider; the identity of the subscriber; the subscriber's public key; the confirmation that the subscriber holds the corresponding private key; and the period of validity of the certificate. In addition, the certificate

1187 Par 50 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001)

1188 Mason *Electronic Signatures in Law* (2012) 274

must be signed using the certification service provider's private key to ensure the authenticity of the certificate with respect to both its contents and its source.[1189]

A person desiring to rely on a digital signature created by the person identified in the certificate can use the public key listed in the certificate to verify that the digital signature was created with the corresponding private key. If such verification is successful, it can be assured that the digital signature was created by that person.[1190] This principle is applicable to a digital signature created either by the subscriber, or by the certification service provider itself whose digital signature on the certificate can be verified by using the public key of the certification service provider listed in another certificate by another certification service provider.[1191]

There might be issues regarding the reliability of the certificate. Indeed, a certificate may be proved unreliable at the issuance, for example in the situation where the subscriber misrepresents his identity to the certification service provider, or the unreliability might arise sometime thereafter, for example where there is a compromise of the private key, or, in other words, the loss of control of the private key by the subscriber. In such situations, the certification service provider may, at the request of the subscriber or not depending on the circumstances, suspend (temporarily invalidate) or revoke (permanently invalidate) the certificate and publish notice of suspension or revocation or inform interested parties.[1192]

To sum up, a digital signature, whether created by the subscriber or by the certification service provider should generally be reliably time-stamped to determine reliably that it was created during the operational period stated in the certificate, a condition for the verifiability of the digital signature.[1193]

In the preceding lines, a technical description of digital signatures has been provided. It covered the PKI system which is made of all the hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.[1194] In addition the

1189 ABA *Digital Signatures Guidelines* 17
1190 ABA *Digital Signatures Guidelines* 17
1191 ABA *Digital Signatures Guidelines* 17
1192 ABA *Digital Signatures Guidelines* 18-19
1193 ABA *Digital Signatures Guidelines* 18
1194 Ch 4 par 4.3.3.7.2 A

role of certification service providers has been addressed.[1195] Since insight has been gained on the operation of digital signatures from a technical point of view, it is appropriate to deal now with digital signatures from a legal point of view by looking at case law. This exercise is undertaken below.

4.3.3.7.3 Digital signatures and the law

Digital signatures are recognised as valid signatures by most of statutes or legal instruments dealing with electronic signatures explored above.[1196] They may also be held valid under common law.[1197]

In addition, the use of digital signatures has also been considered by courts in some jurisdictions. In the German case of FG Münster 11 K 990/05 F, the court considered the validity of a statement of claim filed by e-mail signed with a qualified electronic signature whose corresponding signature certificate contained a monetary limitation of €100. The court dismissed the case, holding that an electronic signature containing a monetary limitation was not a qualified electronic signature capable of replacing a manuscript signature on a written statement of claim. The decision was reversed in appeal where it was held that the monetary restriction clause does not affect the validity of the signature for the purpose of legal appeals.[1198]

In the Colombian case of *Juan Carlos Samper Posada v Jaime Tapias, Hector Cediel and others*,[1199] the defendant argued that documents sent by the court required a digital signature. This argument was dismissed; it was held that the law only requires the use of digital signatures in certain instances. In the absence of a digital signature, the law required the assurance that the content of the message was original; this was apparently the case in this instance. In any event, the court could not affix a digital signature to an e-mail as it did not have the facilities.[1200]

1195 Ch 4 par 4.3.3.7.2 B

1196 Art 5 of the eSignature Directive; Art 6 of the Model Law on Electronic Signatures; S 13(1) of the ECT Act;S 18 of the Electronic Transactions Act 2010

1197 English Law Commission *Electronic Commerce* 14

1198 Mason *Electronic Signatures in Law* 3 295-296

1199 Decision 73-624-40-89-002-2003-053-00

1200 Mason *Electronic Signatures in Law* 3 297-298

In contrast, in the case number IV.ÚS 319/05 (issued on 24 April 2006) from Czech Republic the Constitutional Court upheld the possibility of using a digital signature for the purposes of signing applications sent to courts.[1201]

In the Russian case of N КГ-А 40/8531-03-П, the plaintiff initiated legal action to recover money from its bank following a debit on its account, arguing that it did not issue instructions to the bank to make such transfer. The appeal court rejected the claim and, relying on expert evidence, upheld conclusions by lower courts that the evidence showed that there were signs of an electronic payment order transfer and use of the plaintiff's vice general director's private key. In addition, evidence indicated that the system used did not permit the starting of the communication session without producing the client's main key, or the sending of documents from the client's computer on behalf of another client, or the processing of documents not signed with a duly registered signature.[1202]

These few cases from a variety of jurisdictions provide an overview of the different approaches taken by courts vis-à-vis digital signatures. In some instances such signatures were held a requirement to perform a certain action, in other instances not. The legal perspective through these cases completes the technical perspective on digital signatures.

4.4 Conclusion

This chapter was introduced by a reminder of the challenges identified in the previous chapter in respect of electronic evidence. It was noted that these challenges, which referred to the notions of authenticity, integrity, and non-repudiation of electronic evidence, were addressed for traditional documents by the adoption of rules imposing specific requirements including the necessity of a writing, an original, and a signature. A brief overview of the first two requirements was provided before dealing in more detail with the requirement of signature. With regard to writing the discussion focused on the law of contract and dealt with various statutes providing for the requirement of writing for certain categories of contract. As a general rule, however, writing is not a condition for the validity of a contract, but it offers a lot of advantages that makes it an

1201 Mason *Electronic Signatures in Law* (2012) 298-299
1202 Mason *Electronic Signatures in Law* (2012) 294

important element.[1203] In respect of original, the general rule that no evidence is ordinarily admissible to prove the contents of a document except the original document itself was highlighted.[1204] The reader was then referred to sections which dealt with that requirement previously. [1205] In addition it was pointed out that generally what makes a document to be seen as an original is the affixing of a signature on it. This led to the discussion on signature, addressed firstly from a traditional perspective and then from an electronic point of view. From a traditional perspective the discussion contained three parts. The first part dealt with definitions. With regard to that, it was pointed out that although signature is often understood as a handwritten or manuscript signature, the discussion under the first part revealed a virtually limitless number of possible ways of signing, including various symbols, devices and procedures which have been accepted as valid signatures by many courts in various common law countries such as England and South Africa.[1206] The second part discussed the form of a signature versus its function. It stressed that the function played by the signature is the main criterion used to determine the validity of a signature irrespective of the form it takes; and the major function played by a signature is evidential.[1207] Lastly, the third part dealt with signatures under analogue technologies which included signatures under facsimile technology, typed signatures and signatures contained in telegrams. This discussion showed that, despite a few challenges here and there, signatures under analogue technologies are accepted as valid signatures in many instances in various jurisdictions, including England and South Africa.[1208]

From an electronic point of view, it was assumed that an electronic signature could guarantee the authenticity, integrity, and non-repudiation of electronic evidence. Thus, electronic signatures were discussed in great detail. The analysis included international initiatives, relating to the UN and EU, on the one hand; and on the other hand national initiatives with reference to the jurisdictions of England, Singapore, and South Africa.

In respect of international initiatives, the first part dealt with UN documents and discussed the UNCITRAL Model Laws on Electronic Commerce and Electronic Signatures respectively, as

1203 Ch 4 par 4.2.1
1204 *Standard Merchant Bank Ltd v Creaser* 1982 4 SA 671 (W) at 674B
1205 Ch 2 par 2.2.4.3.1 and Ch 3 par 3.4.2.1.1 A and par 3.4.2.1.3 B 2 (d)
1206 Ch 4 par 4.3.2.1
1207 Ch 4 par 4.2.3.2.2
1208 See in general Ch 4 par 4.2.3.2.3

well as the 2005 UN Convention on the Use of Electronic Communications in International Contracts. The second part, relating to the EU, included a discussion on the E-commerce Directive and the eSignature Directive.

With reference to the UN, all instruments discussed under the first part recognise electronic signatures. The Model Law on Electronic Signatures, however, deals with the subject in more detail and was therefore given more attention. Indeed it offers practical standards against which the technical reliability of electronic signatures may be measured. It further provides a link between such technical reliability and the legal effectiveness that might be expected from a given electronic signature.[1209] It is an interesting initiative in that it contributes to enabling or facilitating the use of electronic signatures and provides equal treatment to both users of paper-based documentation and users of computer-based information.[1210]

Regarding the EU, the second part briefly discussed the E-commerce Directive more as an introduction to the discussion on the eSignature Directive which followed. From that discussion it was concluded that the legal framework provided by the eSignature Directive facilitates the use of electronic signatures and contributes to their legal recognition within the Internal Market. It was submitted that this effort by the EU was in line with the global effort by the UN above.[1211]

Under national initiatives, the section on England discussed the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. The 2000 Act transposes the eSignature Directive into England's national law while the 2002 Regulations deal with certain aspects of this Directive, for example advanced electronic signatures. Both texts constitute the legal framework for electronic signatures in England, complemented by case law. They contribute to the legal recognition and admissibility of electronic signatures in England.[1212]

In Singapore the discussion on electronic signatures focused on the Electronic Transactions Act 2010 with a few references to the Electronic Transactions Act 1998. The legal framework in this

1209 Par 4 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001); Ch 4 par 4.3.1.1.2 above

1210 Ch 4 par 4.3.1.1.2

1211 Ch 4 par 4.3.1.2.2 B

1212 Ch 4 par 4.3.2.1

jurisdiction, which is in harmony with the international initiatives above, promotes the use of electronic signatures in Singapore.[1213]

Lastly, in South Africa, electronic signatures are governed by the ECT Act. This Act adopts the so-called two-tier approach promoted by the Model Laws on Electronic Commerce and Electronic Signatures by providing for two types of electronic signature, namely an electronic signature and an advanced electronic signature and the effect of both. The Act was analysed and similarities with the Model Laws and the eSignature Directive highlighted. For example the definition of advanced electronic signature under the ECT Act is almost identical to that of the eSignature Directive.[1214] The discussion extended to the application procedure for advanced electronic signatures, in other words the accreditation and to circumstances where the law requires a signature and how an electronic signature can satisfy such requirement. Attention was also given to more stringent conditions regarding signatures, for example the electronic notarisation. Finally regard was made to case law with a couple of cases which have considered the use of an electronic signature and its legal effect.[1215]

Chapter four was concluded by a review of different forms of electronic signatures. It included typing a name, clicking, browse wrap, personal identification number and password, e-mail address, scanned manuscript signature and digital signature.[1216] The latter enjoyed more attention and was discussed from both technical and legal perspective, with a review of case law.[1217] With this background set one can move to the next stage of the thesis relating to electronic justice from both technical and procedural point of view under chapter five below.

[1213] Ch 4 par 4.3.1
[1214] Ch 4 par 4.3.1.2.2 A & par 4.3.2.3.1
[1215] Ch 4 par 4.3.2.3.1
[1216] Ch 4 par 4.3.3
[1217] Ch 4 par 4.3.7

CHAPTER 5 ELECTRONIC JUSTICE

5.1 Introduction

After analysing electronic evidence in great detail in the previous two chapters and since one has now a full understanding of the nature and the operation of electronic evidence as well as the challenges posed by such evidence and how an electronic signature can overcome these, the time has come to deal with electronic justice which is the framework within which this thesis envisages electronic evidence to operate. Indeed, this thesis argues that there is a need for having a safe and efficient e-justice system in order to deal effectively with electronic evidence. The question that arises, however, is whether rules of procedure designed to cater for exchange of information in physical world can be applied successfully to electronic procedure. After outlining the history of e-justice from a general point of view in the first part, this question is analysed comparatively in the second part.

5.2 General overview of e-justice

5.2.1 Definition

As defined in chapter 2 above, e-justice refers to the use of information and communication technologies in the administration of justice.[1218] It is a specific field under the broad concept of e-Government which refers to the use of ICTs for administrative procedures. ICTs cover all the technologies which are able to store, retrieve, manipulate, transmit or receive digital data. These technologies have revolutionised the way human beings communicate, the way business is conducted, and, ultimately, the way law is practised. This revolution on a massive scale leaves no sector of the legal industry untouched as most of the information handled by this industry have derived from such electronic revolution. Indeed it is as difficult to find a business transaction that is not produced by electronic means as it is difficult to find legal documents that are not created by electronic means. The result of this revolution is the existence of a mountain of electronic information that needs to be identified, collected, searched, reviewed and produced in case of civil litigation. In addition, this information plays an important role in the event of a criminal case as it constitutes either the instrumentality of the crime or the main source of

[1218] Ch 2 par 2.4.2

evidence in case of a more traditional crime. ICTs are at the upstream of the creation of information and should play a role downstream in the adjudication of cases relying on this information. It is at this point that e-justice comes in to play. The use of ICTs in the justice system, however, serves not only that single goal, but rather constitutes a means to improve the functioning of the courts by ensuring, amongst other things, a more efficient and effective judicial system, a better citizens' access to justice, and the speed of procedures. E-justice involves different technologies and applications which are discussed below.

5.2.2 Main applications

ICT applications in the judicial system can be divided into three broad categories. The first category comprises applications used to support court administrative staff and judges. The second category involves applications allowing the exchange of information between courts, parties and the general public. And, finally, the third category consists of applications that facilitate the presentation of electronic evidence in court.

5.2.2.1 Applications in support of administrative staff and judges

Before dealing with specific applications supporting each category, one needs to look first at the basic technologies used by both administrative staff and judges.

5.2.2.1.1 Office applications

Office applications are the least sophisticated technologies, and they are easily available on the market as standard products. They include technologies such as desktop computers, word processing, spreadsheets and internal and external e-mail.[1219] In other words, it is all the hardware and software used to create, collect, store, manipulate and exchange electronic information in the performance of basic administrative tasks.[1220]

Velicogna reports that the diffusion of basic technologies in Europe, including England, dates back to the 1980s. It is only in the 1990s, however, that many governments in Europe started to invest more in technology as a support of the judiciary with the supply to the courts of equipment

[1219] Velicogna "Justice systems and ICT: What can be learned from Europe" 2007 *Utrecht Law Review* 3(1*)* 129 (hereafter referred to as Velicogna "Justice systems and ICT: What can be learned from Europe") 131 available at http://www.utrechlawreview.org (accessed on 7/11/2014)

[1220] Velicogna "Justice systems and ICT: What can be learned from Europe" 131

and office applications in large quantities and in a systematic way.[1221] Currently, such basic technologies are widespread in European courts.[1222] In England, for example, 100% of the courts have basic applications, such as Word processing, Internet connection, E-mail, and so on.[1223]

In Singapore, the electronic revolution started in 1989 with the decision by the government to embrace Information Technology aggressively in order to make the country more competitive and to nurture its growth and participation in the new global economy. To achieve this purpose, a system, known as TradeNet, was established. That system relies on the Electronic Data Interchange.[1224] This aggressive approach was extended to the legal industry with a vision clearly going beyond the simple use of basic technology with the launch, as early as 7 July 1990, of an ambitious strategic national information network within the legal sector, known as LawNet and forming part of the information technology infrastructure of Singapore.[1225] LawNet is discussed later.[1226] It can, however, be stressed already that technology is ubiquitous in Singapore courts.

South Africa embarked in a process to promote the use of technology in the judicial sector around 1996 with the launch of the Integrated Justice System initiative. This initiative comprised various components of which only the Digital Nervous System or DNS is relevant at this stage as its objective was to provide justice officials with the necessary basic technology. The technology provided by the DNS included, amongst other things, Word Processing and Spreadsheet capabilities on the network, e-mail facilities, access to electronic databases, online applications, and Internet access for specified users.[1227] DNS was expected to remedy the situation that was prevalent up to April 2000 where fewer than 10% of departmental officials had access to

1221 Velicogna "Justice systems and ICT: What can be learned from Europe" 131

1222 Velicogna "ICT within the court in the e-justice era" 2 available at http://effectius.com/yahoo_site_admin/assets/docs/ICT_within_the_court_in_the_e-Justice_Era_by_Marco_Velicogna.207234735.pdf (accessed on 23/10/2015) (hereafter referred to as Velicogna "ICT within the court in the e-justice era"); Velicogna relays quantitative data from the CEPEJ Report "European judicial systems – Edition 2008 (2006 data): Efficiency and quality of justice"

1223 CEPEJ Report "European judicial systems – Edition 2014 (2012 data): Efficiency and quality of justice" 125

1224 Kim "Electronic Evidence, Singapore's Approach" 3

1225 Sze "Chapter 3: Singapore" 64

1226 Ch 5 par 5.2.2.2 B

1227 Department of Justice and Constitutional Development "E-justice, Piecing IT Together" 3-4

computers albeit they were outdated and equipped only with Word processing and some rudimentary financial administration capabilities.[1228]

In July 2002, the situation of the DNS project was as follows:

- 10,595 out of 13,000 network points were in place;
- the network was operational in 80 sites in Johannesburg, Cape Town, Pretoria and Durban, representing 80% of the computer users;
- project support teams were set up in each area;
- 56 of 80 servers required were in place;
- 28 sites had been approved for installation;
- PC and printer deployment was on track and 1600 PCs were in place; and
- 11 training venues had been established.[1229]

The existence of basic technology is of paramount importance as it paves the way to the use of more sophisticated technologies. It must be accompanied, however, by supporting actions, such as training or new work practices, or it will not be able to bring about the efficiency that it is expected to achieve.[1230]

5.2.2.1.2 Applications specific to administrative staff

The administrative staff plays a critical role in the judicial setting. They are not only the interface of the court but also the intermediary between the presiding officer and all the stakeholders involved in the judicial process.[1231] They constitute the entry point of a case in the justice system as they receive the action, cause, or matter when it is filed, they record it in the relevant register, they issue the necessary receipt, and they keep registers and documents. Administrative staff members are, therefore, present from the start to the end of the case, and technology can definitely help them in the performance of these tasks. Organisational tools, such as a computerised case management system, are very useful and can significantly assist administrative staff in their daily activities. The case management system is described below.

1228 Department of Justice and Constitutional Development "E-justice, Piecing IT Together" 3

1229 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 15-16

1230 Velicogna "ICT within the court in the e-justice era" 3

1231 Velicogna "Justice systems and ICT: What can be learned from Europe" 132

Computerised case management system

Case management is the process by which court cases are monitored and managed throughout their life cycle.[1232] Traditionally this process was conducted manually with a case history recorded in paper court docket books or other court registers, that is, huge books required by law to be kept or are kept as a means to achieve the functions that such tools are supposed to perform.[1233] All these traditional registers may have benefits in theory, such as the ability to determine the status of a case or documents filed with the court without the need of the physical access of the case file, the possibility of comparing it with the case file to determine its completeness, and the guarantee that the formal procedure has been complied with, for example the calculation of prescribed periods of time. In practice, however, the difficulty in accessing these books makes these benefits more of a longing than a reality. Indeed, often these registers are located in one place, the clerk's offices for instance, and access to them requires going personally to that office to go through piles of books, which is time-consuming and tedious. In addition, only one office worker can work with the book at a specific time.[1234] To overcome these difficulties, the computerisation of the case management system was thus necessary. The importance of such a case management system goes beyond the mere management of a court case. It serves various other functions, such as the planning and organisation of court activities, the allocation of resources, the monitoring of the output and performance of courts. In addition, it can provide a summary of the court day, week and month work flow and present such information in graphs.[1235] It is such a useful tool in the management of court cases and courts in general that many countries have felt the need to introduce it into their judicial system. The following countries, England, Singapore, and South Africa, have followed that path with different successes. The extent to which the case management system is developed in each jurisdiction is discussed below.

A. England

England is not among the top 12 European countries with the most effective and complete level of computerisation of the management and administration of courts. Neither is it among the

[1232] Sze "Chapter 3: Singapore" 48
[1233] Velicogna "Justice systems and ICT: What can be learned from Europe" 132
[1234] Velicogna "Justice systems and ICT: What can be learned from Europe" 132; Sze "Chapter 3: Singapore" 48
[1235] Velicogna "Justice systems and ICT: What can be learned from Europe" 135

bottom four of the countries with the lowest rate of computerisation of courts.[1236] It is not, however, a jurisdiction that can serve as an example as far as computer case management system is concerned. It probably needs itself to learn, as does its South African counterpart, from most advanced countries from a technological point of view, and Singapore is undoubtedly one of the world top leaders in that regard.[1237]

B. Singapore

To understand how technology was introduced in Singapore courts, one needs to go back to the end of the 1980s. At that time the judiciary was in a chaotic state with thousands of cases clogged up in the court system, some having been there for ten years or more; a breach and total disregard for the Rules of Court by lawyers; and indifference from the Bench and the Bar. All these factors contributed to an inefficient judiciary.[1238] In addition, access to information on the cases was also a challenge. In response, various actions were taken, such as the reform of outdated procedural rules and the extension of the court hearing hours, but the most important measure taken was case management.[1239] Given the limitations of the paper case management pointed out above, it was necessary to develop a computerised case management system. The Civil System responded to that need. There is almost no detail on a case that cannot be found on the Civil System, be it the parties' particulars, the nature and quantum of the claim, the documents filed or the outcome of hearings. This system allows the tracking of a case from its inception to its finalisation with mechanisms to detect any problem with such a case, including any form of inactivity or any breach by the parties of a court order. The Civil System has been such a considerable success that there are no more backlogs in the Singapore court system, with the majority of cases finalised within six months and virtually no case not disposed with within a year.[1240]

1236 CEPEJ Report "European judicial systems – Edition 2014 (2012 data): Efficiency and quality of justice" 126
1237 Sze "Chapter 3: Singapore" 45
1238 Sze "Chapter 3: Singapore" 47
1239 Sze "Chapter 3: Singapore" 48
1240 Sze "Chapter 3: Singapore" 49

C. South Africa

As in Singapore, a computer case management system was envisaged in South Africa as a solution to deal effectively with unacceptably high case backlogs. The system, known as the Court Process Project (CPP) and regarded as the flagship project of the Integrated Justice System, was introduced with the aim of providing a single point within the court from which to manage the entire court process. It was designed in such a way as to be able to automate case management by routing workflow, managing work load, notifying events, generating and managing forms and documents, and scheduling resources, such as court rooms and judges.[1241] In civil matters, on the one hand, automation would involve various tasks, including managing interaction between courts and private attorneys and sheriffs, registering and managing case documentation, scheduling hearings, recording the outcome of hearings, and issuing notification of such outcomes. In criminal cases, on the other hand, automation should make easier the interaction between various stakeholders of the criminal process as well as the management of court cases from commencement to adjudication.[1242] The stakeholders, including the Director of Public Prosecutions, the South Africa Police Service, the Department of Correction Services and the Department of Social Development, were expected to be linked to the Department of Justice.[1243]

The main objective of the CPP was the reduction of the average case cycle time.[1244] Additional objectives of the CPP included:

- The reduction of processing time;
- The elimination of fraud and corruption;
- The electronic tracking of cases;
- The automation of the scheduling of resources;
- The provision of electronic real-time communication;

1241 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 30

1242 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 31

1243 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 30

1244 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 29

- The provision of accurate and current management information;
- The improvement of the efficiency of court management;
- The conversion of the paper systems into electronic systems;
- The reduction of trial delays;
- The improvement of access to information;
- The reduction of duplication of data entry;
- The reduction of the incidence of lost dockets and case files; and
- The improvement of the administration of prisoners.[1245]

The CCP relied on a user-friendly and simple computer programme which allowed the capture and management of information related to a case contained in a docket or charge sheet. Such information which was available in real time electronically included the name, the address and the ID of the accused or the parties, the date of arrest, the case number, to name but a few .The above computer programme was first used at the Middleburg's Magistrate Court in the Eastern Cape Province from December 2001 with the intention of extending its use to 26 other sites throughout the country by the end of July 2002. After four months of operation of the computer programme at the Middleburg's Magistrate Court, very interesting statistics were observed, such as:

- The increase of the court's average usage time from 3 hours 45 minutes to 5 hours;
- The increase of the number of cases finalised per month from 101 to 206; and
- The decrease of the number of cases withdrawn because dockets were not at court from 20 to nil.[1246]

Over 10 years after the launch of CCP it seems that case management systems are available only in certain courts in South Africa.[1247] This situation is unfortunate as it implies that a certain number of courts are still facing some of the challenges identified above, such as an unacceptable high case backlog. Efforts must, thus, be intensified to extend such systems to all courts to

---

1245 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 29

1246 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 31

1247 Van Rijswijck "South Africa justice system goes hi-tech" online publication 9 Nov 2011 available at http://www.southafrica.info (accessed on 25/11/2014) (hereafter referred to as van Rijswijck "South Africa justice system goes hi-tech")

ensure that the above benefits are experienced throughout the country. The positive effect of this system has been pointed out earlier with regard to Singapore; it is interesting to note that, not far from South Africa, another country is reaping the dividends of investing in such a system, and that is Botswana. In this neighbouring country to South Africa, an electronic court records management system has been introduced since 2005 to modernise and make court operations more efficient. The result of the introduction of this system is that access to case information is easier, so is the determination of the exact status of a case during the judicial process.[1248]

5.2.2.1.3 Applications specific to judges[1249]

Applications for supporting judges include all the individual tools designed to help judges in their daily activities. These tools can broadly be divided into three categories, office tools, legal research tools, and judgment and sentencing tools. Firstly, office tools, which have been described above, can be used by judges to draft judgments or prepare court cases electronically. Secondly, legal research tools are very important tools used in support of an activity of the judge considered to be the most affected by ICT, namely legal research. These tools and applications include CD-ROMs, Intranet, and Internet software to access legal materials, including statutory law, common law, case law, rules, court working methods, electronic databases, and so on.[1250] The Internet is a particularly useful tool for legal research as it allows judges to conduct more qualitative and efficient legal research by surfing through various websites, using search engines or text mining techniques.[1251] Finally, judgment and sentencing tools consist of those applications developed to assist judges in drafting judgments or sentences. They are often pre-programmed standard-decision templates linked to automated registers or case management systems from which data relating to litigation can be retrieved automatically to help judges to make their decisions.[1252] These tools are expected to improve the quality of judgment and timeliness and bring about more consistency in sentences imposed over the time. In addition they should be capable, in theory at least, of giving judges quick and easy access to relevant information relating to previous sentences passed by that specific court in cases of a similar

1248 Van Rijswijck "South Africa justice system goes hi-tech"
1249 Or magistrates as the case may be
1250 CEPEJ Report "European judicial systems – Edition 2014 (2012 data): Efficiency and quality of justice" 124
1251 Velicogna "Justice systems and ICT: What can be learned from Europe" 136
1252 Velicogna "ICT within the court in the e-justice era" 8

nature without restricting the exercise of judicial discretion.[1253] It is submitted, however, that the development of an application with such a capability is very difficult because of the complex nature of tasks involved in the judicial decision-making process which includes virtually endless variations of the sentencing exercise.[1254] Indeed, it is not easy to design computer automated systems with the characteristics of judicial decisions such as complexity, variability, flexibility and discretion. In spite of this situation, there is reason to keep hope for the future with improvements in semantic technologies and data mining.[1255]

After a general introduction to the applications for supporting judges, the time has come to analyse the existence and the use of these applications within the jurisdictions of England, Singapore and South Africa.

A. England

During the nineties, a project known as JUDITH started to provide judges in England with computers for their daily activities.[1256] The project was seen to be a success and, as a result, it created more appetite for technology from judges who started to demand to be linked to various databases, such as the prison records, and so create an intranet.[1257] Judges started typing notes during case hearings instead of handwriting them. In one instance, reported by Philip Leith, a judge was able to hand over an approximately 7-page typed judgment 16 minutes after the final speech on behalf of the complainant. This decision was unsuccessfully challenged on appeal on the basis, it was argued, that the judge was not listening to the submissions as he was making notes on his laptop at the same time. The appeal court dismissed the appeal as it found no discrepancy between the facts of the case and the records of the judge.[1258]

1253 Velicogna "ICT within the court in the e-justice era" 9

1254 Velicogna "ICT within the court in the e-justice era" 9

1255 Velicogna "ICT within the court in the e-justice era" 9

1256 Around 330 judges were supplied with personal computers around the third quarter of 1996, according to Woolf *1996 Final Report on Access to Civil Justice* Ch 21.5

1257 Lodder, Oskamp and Schmidt (ed) *IT Support of the Judiciary in Europe* 2001 (hereafter referred to as Lodder *et al IT Support of the Judiciary in Europe*) 66

1258 Lodder *et al IT Support of the Judiciary in Europe* 67

Woolf stressed the importance of IT in the judiciary in both his interim and final reports on access to civil justice.[1259] He was convinced that IT will play a key role not only in streamlining and improving existing systems and processes, but it will also serve as a catalyst for radical change.[1260] He, therefore, recommended judges be equipped with usable and well-supported technology which, in his view, needed to include powerful and portable computers. In addition, it was important for the computers to be equipped with communication facilities, hardware and software, allowing access by judges to information and files from anywhere, as well as communication with other judges and legal advisers.[1261]

The latest development, as far as the use of IT in the judiciary is concerned, vindicates Woolf, as, almost 10 years after his final report, 100% of judges in England are equipped with the technologies he recommended. [1262]

B. Singapore

Following the great success of the computerised case management system in Singapore, the vision of introducing a paperless courtroom emerged as a means of building a world-class judiciary. To achieve this, the use of technology was central and every court process needed to be computerised, whether it was the filing of court documents, the preparation of the trial or the trial itself.[1263] And obviously judges had a critical role to play in the materialisation of this vision.

The man behind the introduction of technology into the Singapore justice system is Chief Justice Yong Pung How[1264] who proposed a framework for the application of technology in the judiciary which resulted in the implementation of multiple projects promoting the use of technology to

1259 Woolf *1995 Interim Report on Access to Civil Justice* Ch 13.1.; Woolf 1996 *Final Report on Access to Civil Justice* Ch 21.1

1260 Woolf *1996 Final Report on Access to Civil Justice* Ch 21.1

1261 Woolf *1995 Interim Report on Access to Civil Justice* Ch 13.8

1262 CEPEJ Report "European judicial systems – Edition 2014 (2012 data): Efficiency and quality of justice" 125

1263 Sze "Chapter 3: Singapore" 50

1264 Chief Justice Yong Pung How was appointed head of the Judiciary in September 1990 with a main priority to reform the Judiciary

improve the service of the courts and the legal profession in Singapore.[1265] Most of these projects promoted applications much more sophisticated than the technologies specific to judges discussed in this section. For example, a technology court was inaugurated in July 1995. Such a futuristic court consisted of a network of computers allowing for the sharing of online information, video conferencing, and other visual facilities as well as a digital recording system.[1266] Another example is the Electronic Filing System allowing for the electronic filing of court documents.[1267] These technological innovations and others are discussed later in this thesis as they clearly exceed the scope of this section.[1268] It goes without saying, however, that such innovations could not have been successfully implemented without the basic technologies and applications specific to judges dealt with in this section which constitute the basis upon which these advanced technological innovations could be introduced. It is, thus, obvious that judges in Singapore have been accustomed to using basic technologies for ages. As an illustration, legal research was identified as one of the six key drivers in the implementation of the Electronic Litigation System project[1269] and it required adequate online legal research facilities. This tool is very useful for judges as, without it, they would have to spend a great amount of time going through thick volumes of law reports and other legal sources in the library in the preparation of cases or drafting of judgments.[1270] Judges may also access the Supreme Court LAN to do online legal research, data retrieval, and e-mail. Equipped with a laptop since July 2001, they can access the network from their homes via the Citrix server and prepare their hearings by reading electronic cases or carrying out the necessary legal research in that respect. The installation of the wireless LAN infrastructure has made things even easier for judges who can access several applications available on the LAN while in meetings or discussions in conference rooms.[1271]

1265 Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals" Sept 2000 *Pacific Rim Law & Policy Journal* 9 (hereafter referred to as Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals") 3

1266 Sze "Chapter 3: Singapore" 50; Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals" 3

1267 Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals" 3

1268 Ch 5 par 5.2.2.2 B

1269 Other key drivers in this project discussed later include: conduct of trials and hearings; filing of court documents; access to court information; service of court documents and internal court processes; Sze "Chapter 3: Singapore" 51

1270 Sze "Chapter 3: Singapore" 51

1271 Sze "Chapter 3: Singapore" 51

C. South Africa

Technologies specific to judges were part of the above-mentioned DNS project whose objective was to provide 80% of justice officials with the appropriate infrastructure, Internet connection and research facilities by the end of 2002.[1272] The vision of the DNS was to bring the South African justice system into the modern information age by the provision of state-of-the-art technology. Although the DNS project was not designed specifically for judges, it contained applications relevant for judges, such as the Internet, e-mail, online applications, or electronic databases. Under the DNS, judges could, for instance, have access to electronic databases such as Jutastat or Butterworths from their own desk, which was not possible before that as these databases were accessible only from a stand-alone computer located in the library in several courts.[1273] The picture of the DNS project at mid-2002 as pointed out above showed a project well on track.[1274]

With regard to judges, there is no clear indication of whether IT projects focusing only on them have been introduced in South Africa. It will be interesting to find out whether there are any, and what, applications specific to judges are in use in South African courts.

5.2.2.2 Applications for information exchange between courts, parties and the general public

As the title suggests, this section deals with technologies and applications specifically designed for the electronic communication and exchange of information between the courts and other stakeholders of the justice system, such as attorneys, parties, prosecutors, and so on, or other third parties, including the general public. These applications include, among other things, a court website where information regarding the court's organisation and activities can be found; downloadable forms might also be available on the website to permit for the electronic submission of claims. Other important tools for the electronic communication and information exchange between the courts and their environment include electronic registers, business or land registers, for example, or text-messaging application allowing parties to be informed of the status

1272 Department of Justice and Constitutional Development "E-justice, Piecing IT together" 3
1273 Department of Justice and Constitutional Development "E-justice, Piecing IT together" 4
1274 See Ch 5 par 5.2.2.1.1 above

of their cases on the court list.[1275] As has been the general trend in this chapter so far, an overview of these technologies in the selected jurisdictions is provided as follows.

A. England

1. General information provision

In England, as in many other jurisdictions, the main platform nowadays for the provision of information regarding the courts is websites. Velicogna affirms that three approaches are followed in Europe in respect of the organisation of websites providing information on courts. The centralised approach leaves a prominent role to the highest courts, ministries of justice, or the judicial council in the organisation of websites. The second approach restricts web information provision within common frameworks. The third and final approach promotes complete freedom and local initiative in the development of the courts' websites.[1276] England follows the centralised approach with court information now provided on the Ministry of Justice website www.justice.gov.uk, but currently in the process of moving to www.gov.uk. The move is motivated by the desire to make information simpler, clearer and faster to find and use.[1277] This new website will be a true goldmine once all the content from the websites of other government departments, bodies, and agencies is moved there, and it will make access to such government services and information easier, including information relating to legal processes, courts and the police under the hyperlink "Crime, justice and the law". In the meantime, the website www.justice.org.uk provides a variety of information on courts, including information on the addresses, opening hours, daily court lists, court fees, procedure rules, and so on of courts. In addition, the British and Irish Legal Information Institute (BAILII) provides access to British and Irish case law and legislation free of charge.

Besides the Internet, information kiosks are used in England as a means of providing court information. A pilot project for the development of an information kiosk by the HM Courts and Tribunal Service (HMCTS) in partnership with other partners was launched in 2000. The information kiosk is a touch-screen facility used to extract information about the HMCTS or the

1275 CEPEJ Report "European judicial systems –Edition 2014 (2012 data): Efficiency and quality of justice" 125

1276 Velicogna "Justice systems and ICT: What can be learned from Europe" 138

1277 https://www.justice.gov.uk/news/features/moving-to-gov.uk(accessed on 21/01/2015)

local authority. It also provides electronic versions of civil forms and leaflets which can be printed if necessary.[1278]

2. Electronic exchange of court documents

Traditionally in judicial matters, official communication is done in paper form with a myriad of formal rules with which to comply. But, with the advent of technology, judicial administrations around the world have been considering the possibility of providing court services electronically, and England is not an exception to this trend. Money Claim Online (MCOL) is a good example of this paradigm shift in England. MCOL is a HMCTS Interned-based service for claimants and defendants to make, or to respond to, a money claim on the Internet in a convenient and secure way.[1279] The procedure to make a money claim online through the MCOL is simple. Firstly, you need to register to receive a Government Gateway ID. Once registered, you can submit a money claim for a fixed amount not exceeding £100.000 against no more than two people or organisations; you must be over 18 and reside in the UK. You can, however, only claim against a person with an address in England and Wales; to complete the submission process you need to pay a court fee with a debit or credit card.[1280] To respond to a money claim using MCOL the respondent needs also to register. He may, however, decide to respond in the same way as he was notified of the claim, that is, by post, and, in that case, he does not need to register.[1281]

B. Singapore

The vision of a paperless court system in Singapore led to the development of the Electronic Litigation System. This project covered all the technological initiatives that were necessary to make the vision of a paperless courtroom a reality in Singapore. It relied on the following six areas of the litigation process:

- conduct of trials and hearings;
- filing of court documents;
- access to court information;

1278 Velicogna "Justice systems and ICT: What can be learned from Europe" 140-141
1279 https://www.moneyclaim.gov.uk/web/mcol/welcome (accessed on 22/01/2015)
1280 https://www.gov.uk/make-money-claim-online (accessed on 22/01/2015)
1281 Velicogna "Justice systems and ICT: What can be learned from Europe" 142

- service of court documents;
- legal research; and
- internal court processes.[1282]

This section deals primarily with items 2 to 4 as the last two items have already been addressed,[1283] and the first item will be discussed later.[1284] Items 2 to 4 fall under the subject matter of this section dealing with applications relating to the electronic communication and information exchange between courts and other relevant actors.

1. Legal Information

Under this heading are discussed issues relating to legal information in the broadest sense, including court information and information relevant for legal research accessible from LawNet.

a. Court information

A technological initiative worth mentioning in respect of court information is the Supreme Court Mobile Information Service. This service allows any person with a mobile phone to request information on a pending case, such as the name of the judge presiding over the case, the time and venue of the hearing. The response to the request is made by means of a free short message to the requestor. Another communication channel with the Supreme Court consists of its website which contains a variety of information relevant for both the public and legal researchers, such as the history of the judiciary, hearing lists, policies, procedures and practice directions, and so on.[1285] In addition, the Supreme Court also provides within its premises interactive information kiosks, known as "infokiosks", where visitors can obtain useful information to guide them around the courts.[1286]

b. LawNet

As a strategic national information network within the legal sector, LawNet forms part of the information technology infrastructure of Singapore. It is based on a number of computerisation

1282 Sze "Chapter 3: Singapore" 51
1283 Ch 5 par 5.2.2.1.3 B
1284 Ch 5 par 5.2.2.3 B
1285 Sze "Chapter 3: Singapore" 66
1286 Sze "Chapter 3: Singapore" 66

projects initiated by the government for the legal sector, and it coordinates and integrates all endeavours towards the creation of a national legal information database. As such, it operates as a one-stop centre providing access to various databases, such as those of the Supreme Court, case law or parliamentary debates, or the Registry of Companies. Launched on 7 July 1990, LawNet is chaired by a council comprising high-profile people representing the main structures of the legal profession.[1287] LawNet has made legal research an enjoyable experience.

2. Filing and service of court documents

At the centre of the electronic filing and service of court documents in Singapore courts lies the Electronic Filing System, a massive technological initiative which has completely transformed the nature of the whole litigation process, by moving it from paper to electronic form and changing the way not only court documents are filed or served, but also the way they are processed, stored, retrieved or managed. This prompted an expert to say that the Electronic Filing System has changed the litigation landscape from a "paper mountain" to an "electronic super-highway".[1288] The metaphor used is very illustrative of the extent of the transformation brought about by the introduction of technology in the litigation system; it is not merely a fashion exercise to conform to new hi-tech trends just for the sake of it, but rather it means a substantial transformation that brings more efficiency and effectiveness to the litigation system which is no longer climbing a mountain of paper but rather using a very rapid electronic highway with reduced movement of people and paper documents. The Electronic Filing System is critical to the above-mentioned Electronic Litigation System with all its six components that it supports through these following services:

- Electronic Filing Service;
- Electronic Extracts Service;
- Electronic Service of Documents Facility; and
- Electronic Information Service.

1287 Sze "Chapter 3: Singapore" 64
1288 Sze "Chapter 3: Singapore" 55

a. Electronic Filing Service

Contrary to the traditional manual filing of documents in court, since July 2001 the Electronic Filing Service allows lawyers in Singapore to file documents electronically via the web-based front-end system. The Web-based Law Firm Front-End System, which is one of the six main components[1289] of the Electronic Filing System, is used by lawyers not only to file documents electronically but also to receive information regarding the outcome of their submissions, extract copies of cause papers, or to serve court documents on other law firms.[1290]

Fewer than two years after the launch of the Electronic Filing System, figures indicated that over 80% of documents had been filed electronically in court.[1291] In addition, two Service Bureaux had been established to accommodate lawyers not registered on the Electronic Filing System or litigants acting in person with the electronic filing of documents. The procedure was to submit paper documents to the Service Bureau and pay the manual handling fee. The Bureau would then type in the relevant information, scan the documents, and transmit them electronically to court.[1292]

b. Electronic Extracts Service

Through this service, a lawyer can, from his office or a Service Bureau, seek approval and the extraction of copies of cause papers from the court. This service allows a lawyer to make an online search on the index of documents filed for a specific case and have electronic copies of documents sent to him by e-mail.[1293]

c. Electronic Service of Documents Facility

This service facilitates the electronic service of court documents among law firms which is done by way of e-mail. Documents served under such Electronic Service of Documents Facility are deemed to be served in accordance with the Rules of Court with a certificate of service

1289 Other components include: the VAN Operator Filing Processing System;the Service Bureau System;the Courts Workflow System;the Key Management System;and the Commissioner for Oaths System.
1290 Sze "Chapter 3: Singapore" 57
1291 Sze "Chapter 3: Singapore" 56
1292 Sze "Chapter 3: Singapore" 56 & 58
1293 Sze "Chapter 3: Singapore" 56

automatically generated by the system. The certificate can be used as a substitute to the affidavit of service and filed in court to serve as evidence of service.[1294]

d. Electronic Information Service

The last service of the Electronic Filing System allows lawyers to search the databases of courts electronically. It includes all the search services of LawNet.[1295]

e. Other components of the Electronic Filing System

In addition to the two components of the Electronic Filing System presented under point a. above, four more components are described below briefly. They include: the VAN Operator Filing Processing System; the Courts Workflow System; the Key Management System; and the Commissioner of Oaths Systems.

The VAN Operator Filing Processing System routes documents received from law firms to the appropriate court or other recipients. In addition, it is used to determine the charges related to a specific transmission or transaction, including court fees, processing fees and hearing fees. Finally, the system is also used to collect money from law firms on behalf of the judiciary.[1296]

The Courts Workflow System enables the tracking and management of cases and documents received by the courts. Once approved, all received documents are indexed and stored in the system. Electronic case files stored on such system can be accessed during hearings or for any other good reason. In addition, any relevant information from the documents is automatically extracted and used in the updating of the computer databases of the courts.[1297]

The Key Management System is responsible for the issuance and management of smart cards and digital certificates. The role played by such system is important as the Electronic Filing System as a whole relies on the Public Key Infrastructure to guarantee the security of the Electronic Filing System proprietary network; hence, there is the necessity to have a system such

1294 Sze "Chapter 3: Singapore" 56
1295 Sze "Chapter 3: Singapore" 57
1296 Sze "Chapter 3: Singapore" 57-58
1297 Sze "Chapter 3: Singapore" 58

as the Key Management System to serve as a certification service provider.[1298] Upon registration on the Electronic Filing System, a lawyer is issued with a smart card and the related unique identity code and password. He needs this to access the four services of the Electronic Filing System via the Web-based Front-End System.[1299]

Finally, under the Commissioner for Oaths System, affidavits can be sworn or affirmed before both judiciary and non-judiciary Commissioners for Oaths electronically.[1300]

C. South Africa

1. General information provision

The main access point to court information in South Africa is the website of the Department of Justice and Constitutional Development www.justice.gov.za. This website provides a list of all courts making up the judicial system in South Africa, their location and links to websites of certain courts, such as the Constitutional Court www.constitutionalcourt.org.za, or the Supreme Court of Appeal www.supremecourtofappeal.org.za, as well as the website of the South African judiciary www.judiciary.org.za.

2. Electronic exchange of information

In South Africa, the CPP, already mentioned above, envisaged electronic communication and exchange of information within the court and among the courts and other stakeholders of the justice system through its objectives relating to the provision of electronic real-time communication and the improvement of access to information. A pilot project, in both the civil system and the criminal system, was initiated as a first step in the implementation of the CCP. Its operation is described below.

a. Criminal system

Although the thesis deals mostly with the use of technology in civil cases, consideration of technology in the criminal law system shows that technology can benefit the whole justice system. It is thus included in this discussion for completeness sake. Under the automated

1298 For more on public-key infrastructure and certification service providers, read Ch 4 par 4.3.3.7.2
1299 Sze "Chapter 3: Singapore" 58
1300 Sze "Chapter 3: Singapore" 59

criminal system, a data management programme registers cases, and it captures and manages case data contained in the docket or charge sheet, including, but not limited to, the name, address, and ID of the accused, or the date of arrest.[1301] The system actually converts the docket into a virtual docket where information can be added as the case progresses. It provides for an electronic charge sheet (form J15) which is the exact copy of the paper version, and it also generates other e-forms which it authorises after performing a certain number of security checks, including checking the signature on the smart card.[1302] In addition, the system allows magistrates and court officials to view case records through a Case Properties screen. To access this feature, however, they need to identify and authenticate themselves by means of a smart card. Such smart card includes a user ID, finger prints, and a digital signature.[1303]

b. Civil system

The management of a civil case is very complex because of the nature of civil cases which are subjected to complex procedures and processes, including the possibility of having multiple defendants, a case consisting of many different claims, a case where a claimant becomes a defendant. The design of an automated civil system, therefore, proved to be much more difficult than that of the criminal system. In spite of this difficulty, the following system was designed. Under this system a case is initiated by completing forms; these forms are checked for authenticity or completeness. A validation process determines whether it is a new case, and, if the answer is in the affirmative, a case number is allocated. If it is not, the case is linked to the case record of the existing case to which it relates.[1304] The system enables summonses and warrants to be submitted online or as e-mail attachments. It, further, comprises a database of the case details which is updated as the case proceeds. The information in the database is used to populate forms generated by the system. The relevant form can be called up by typing in the case

1301 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 33

1302 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 33

1303 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 33

1304 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 34

number in the list of forms provided by the menus. It is possible to attach documents to any form so that they form part of the virtual case folder. Forms are in PDF format.[1305]

As an illustration, under the civil system a typical civil case procedure will follow the path below:

1. A Summons Commencing Action (Ordinary) screen is called up and completed by an attorney with the details of the parties and the nature and particulars of the claim.
2. Initial costs are then calculated by the system and fees are collected.
3. Civil claims are allocated by the system depending on whether the clerk or the magistrate will deal with them.
4. After the successful submission of a summons, it receives a case number and an internally generated check number, and a signature is applied electronically. It is then possible to view the summons on the screen with the Justice logo and date and time stamp.
5. An instruction is then sent to the sheriff to serve the document on the defendant. The document can be downloaded directly from the system by the sheriff or received by mail sent by the attorney. The confirmation of service can be done electronically by the sheriff. The defendant will need to respond within the applicable time, and failure to do so will result in the plaintiff's asking for default judgment.
6. A Request for Default Judgment form is available. If the default judgment is granted, a warrant can be generated automatically by the system upon request and sent to the attorney. The attorney will check and sign the warrant and send it back to the Clerk of the Court to be executed by the sheriff. This process was expected to be able to be completed in four days compared to the 40 days necessary for the existing manual system.
7. In addition, the system can assist in the control of case flow, compilation of management statistics, and so on.[1306]

1305 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 34

1306 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 35

c. Law Society of South Africa's initiatives

In addition to the CPP, the Law Society of South Africa (LSSA) is also investigating the possibility of establishing a public-key infrastructure to allow attorneys to use advanced electronic signatures and to be able validly to exchange information electronically.[1307] Such advanced electronic signatures will be necessary not only for electronic communication with courts but also in dealing with the prospective eCadastre electronic registration systems which are being investigated by the Department of Land Affairs, or in the interaction with the Master of the High Court once the right electronic infrastructures and interfaces are in place.[1308] The successful use of advanced electronic signatures by attorneys in electronic communication and information systems which are currently available, however, requires pilot projects to identify the advantages and challenges.[1309] The pilot projects are planned.[1310]

5.2.2.3 Applications used in the courtroom

Courtroom technologies include a wide range of hardware and software designed to help parties in the presentation of their case in court, such as computers and multimedia screens, video conferencing, electronic evidence presentation software, overhead projectors, scanning and bar coded devices, digital audio technology and real-time transcription of audio and video recordings with possibly the feature to create an index of the contents. In addition, Internet and intranet infrastructures are also available in the courtroom.[1311]

The display and presentation of evidence in court can be done, using either standard software packages or dedicated software packages. PowerPoint, part of the Microsoft Office package, falls into the first category, so are word processors used to display text documents, image manipulation or image-viewing software allowing the display of digital pictures or other imagery, and Web browsers used to display Internet content. The second category consists of all software products specifically designed for the presentation of evidence in court and includes the

1307 Heyink *Electronic Signatures Guidelines* 28
1308 Heyink *Electronic Signatures Guidelines* 28
1309 Heyink *Electronic Signatures Guidelines* 29; read also Heyink *Information Security Guidelines for Law firms* (2001)
1310 Heyink *Electronic Signatures Guidelines* 29
1311 Velicogna "ICT within the court in the e-justice era" 9

following products, Trial Director, Sanction, Summation, Trialbook 32, TrialPro and Visionary.[1312]

The use of visual evidence is particularly interesting in the case of the presentation of complex technical evidence arising from the advent of new digital technology. It helps to construe and convey such evidence in a way that can, for instance, assist the jury to retain the evidence presented, maintain interest throughout the proceedings, and better understand the nature of the case.[1313] These advantages also benefit judges and other triers of fact.

Most of these technologies are available in the three jurisdictions under review in this chapter, and they are highlighted below with regard to each jurisdiction.

A. England

In 2001, the HMCTS launched a modernisation programme aiming at improving the provision of technology in the Crown Courts in England. At the heart of this project lay the Kingston-upon-Thames state-of-the-art high-technology court. A national pilot programme was initiated to develop mechanisms for the Electronic Presentation of Evidence (EPE) in such courts. The EPE is a tool allowing electronic evidence to be presented in court in electronic format using installed technology. In addition, it allows witnesses to give evidence through Video Conferencing.[1314] In 2012, the UK counted 12 specifically equipped EPE courtrooms.[1315] The EPE presents a number of advantages, including: an estimated one-third reduction in trial length; an estimated one-third cost saving; saving in court space; increased retention rate by judges and jury; record of displayed documents by exhibit log and hyperlinking from transcript.[1316]

Even before the above modernisation programme had been initiated, however, information technology was used in courts, albeit sporadically. This was the case in the civil case of *Pelopidas (owners) v TRSL Concord (owners)*.[1317] This collision case between two vessels (the

1312 Mason *Electronic Evidence* (2010) 138
1313 Mason *Electronic Evidence* (2010)139
1314 *SFO Operational Handbook* 2012 1;available at http://www.sfo.gov.uk/media/106019/electronic_presentation_of_evidence_sfo_operational_handbook_topic.pdf (accessed on 27/01/15) (hereafter referred to as *SFO Operational Handbook*)
1315 *SFO Operational Handbook* 1
1316 *SFO Operational Handbook* 1
1317 [1999] 2 Lloyd's Rep 675, 2 All ER (Comm) 737

Pelopidas and TRSL Concord) relied on computer-generated evidence consisting of two-dimensional computer-generated simulations of both vessels' trajectories to determine the liability for the collision and the apportionment thereof. The court found such computer-generated reconstruction evidence useful.[1318]

In criminal cases, in contrast, given their sensitive nature, it is suggested that computer-generated evidence should be thoroughly examined by assessing its prejudicial effect, accuracy and relevance carefully before its admission. These concerns were expressed in *R v Ore*.[1319] Tucker J understood the concern raised by the defence that the jury may place more weight on the graphic animation than its value in the case. In spite of this, however, he was satisfied that such electronic evidence should be admitted, provided that proper directions were given to the jury. The computer-generated animation in this case was a reconstruction of a collision between two vehicles at a junction, and it constituted one of the first experiences of forensic computer-generated animations in an English criminal case.[1320]

An EPE courtroom is equipped with the following technology installed: monitors distributed between all parties; active and backup servers; all necessary cabling and power sockets as per health and safety standards. In addition, some courtrooms will have a scanner, a printer, microphones and Web cameras.[1321] To use an EPE courtroom one needs to apply, and, after permission has been granted, a case can be prepared for an EPE trial. This will require going through a three-phase process. Firstly, electronic evidence must be dealt with by preparing all the exhibits to use in court. Secondly, the courtroom must be prepared by selecting the appropriate EPE package, and, if necessary, Real-Time Transcription and Video Conferencing. Five lots of EPE are available for selection:

- Lot 1: Document Scanning Services;
- Lot 2: a combination of Lot 1 and Lot 3 (presentation package) and Lot 4 (Hardware support);
- Lot 3: Build EPE presentation package but can scan documents (Lot 2) and provide Hardware (Lot 4);

1318 Mason *Electronic Evidence* (2012) 147
1319 [1998, unreported], Birmingham Crown Court; Mason *Electronic Evidence* (2012)148
1320 Mason *Electronic Evidence* (2012) 148
1321 *SFO Operational Handbook* 2-3

- Lot 4: Hardware Provision combined with Lots 2-3; and
- Lot 5: Lots 1-4 in Counter Terrorism Division cases.[1322]

As far as Real-Time Transcription is concerned, it is performed by using a computer programme called "Transend" to record word by word, and in real time, legal proceedings on a laptop. Words will be displayed on the laptop roughly three seconds after their utterance. Transend also provides counsel with the possibility to customise annotations and reports on issues pertaining to the case. Transcripts will include references to documents, exhibits and graphics with hyperlinks for easy access.[1323]

Video Conferencing provides witnesses with the opportunity to give evidence from a remote location and offers many advantages, such as: cost-effectiveness, in that it saves money on air transport and hotel accommodation for witnesses who do not need to travel; it removes any intimidation to which witnesses may be subjected in a courtroom; and it saves time in a situation where a witness is required urgently but cannot travel to court.[1324]

Thirdly, and finally, the graphical support must be prepared by approaching the Graphics and EPE Unit which provides support to cases from start to finish. Such support will include the drafting, the rendering, the amendment, and the animation of graphics. This process can take up to three months.[1325]

The next step in this review of courtroom technologies is Singapore.

B. Singapore

The extent to which Singapore has embraced technology in the judicial system has been already documented in this thesis.[1326] The first technology court was introduced 20 years ago and offered advanced technologies such as a digital recording system, audio-visual facilities and video conferencing. It was such a success that it led, after feedback from judges and practitioners, to a newer improved version in terms of quality in the presentation of cases and effectiveness in the

1322 *SFO Operational Handbook* 5
1323 *SFO Operational Handbook* 8-9
1324 *SFO Operational Handbook* 10
1325 *SFO Operational Handbook* 4
1326 Read Ch 5 par 5.2.2 in general

taking of evidence from witnesses. The Technology Court 2 has indeed had a positive impact on the following functions of the court: control of court proceedings; recording of proceedings; and the taking of evidence by means of video conferencing and the presentation of evidence. A colour touch-screen panel allows the court officer to control various functions in the courtroom. In addition, he can control sound and light in the courtroom as well as the eight cameras installed in the room and their movement in the courtroom, including the zooming in on a particular corner.[1327]

The touch-screen panel is also used to activate recording systems, telephone and video conferencing facilities.[1328]

Regarding the presentation of evidence, the Technology Court makes it easier and more effective. With the audio-visual system for instance, evidence stored in various media, such as DVDs or VCDs, can be presented in court and viewed from a 100-inch projection screen. This screen is capable of displaying images from different sources, including cameras within the courtroom, the video conferencing system and the lawyers' laptops. The presentation of evidence incorporating video content and computer animation can also be accommodated in the Technology Court. Such evidence, as discussed above in the English jurisdiction, is useful in technically complex cases, such as ship collisions or patent cases.[1329]

As with the presentation of evidence, the taking of evidence from witnesses is made easier and more effective by the use of technology, and specifically video conferencing. This tool allows a witness who is unable to be physically present in court to give evidence from anywhere in the world. It also has the benefits of saving in time and costs.[1330]

The above description shows how advanced Singapore is in the use of technology in the courtroom. This is the end result of a long process towards a paperless court system which is now a reality thanks to a certain number of technological initiatives which are part and parcel of

1327 Sze "Chapter 3: Singapore" 52

1328 Sze "Chapter 3: Singapore" 52

1329 Sze "Chapter 3: Singapore" 52

1330 Witnesses from various countries around the world have given evidence through the video conferencing system, including the USA, the UK, Switzerland, the Netherlands, Austria, Belgium, Italy and Japan; Sze "Chapter 3: Singapore" 53

the Electronic Litigation System,[1331] including the initiative on the conduct of trials and hearings. The goal of this initiative was to transform the environment in which trials and hearings were conducted, from paper to electronic, allowing the use of electronic documents.

From 1998, the use of electronic documents became compulsory in all appeals before the Court of Appeal and magistrate's appeals in criminal matters before the Chief Justice.[1332] The rationale for introducing such an initiative at the highest level was to show to the rest of the legal profession the importance and seriousness that the judiciary placed on technology as a means to improve the litigation process.[1333]

To make the use of electronic documents possible, some renovations had to take place in the relevant courts, such as putting in the necessary cables and wires, installing computer terminals connected to flat screen monitors and video switching devices to allow communication between the judge and the counsel. To familiarise itself with this new setting the legal profession was offered demonstrations and presentations, as well as hands-on training in handling electronic documents. They could also benefit from the assistance of specially trained court officers both during practice sessions and hearings.[1334]

From the above, it can be clearly seen that Singapore constitutes a true model in the use of technology in the court system in general and in the courtroom in particular. The journey which started with the development of a case management system, passing through the Electronic Filing System, has now reached a point where the virtual courtroom is a reality. A futuristic Supreme Court Complex with state-of-the-art technology was planned to be completed in 2005. And, as a result, all trials, court processes and transactions were expected to be carried out in that court electronically from that year onwards. Technology available in the New Supreme Court includes: extensive wireless facilities; a multi-media digital recording facility able to produce an audio, visual and textual record of proceedings as well as real time transcription of notes of evidence; an intranet system facilitating the usability of all knowledge management tools and applications available; a high bandwidth network for better access to links for broadband and video-streaming applications; video conferencing facilities, including being available from the

1331 Discussed above Ch 5 par 5.5.5.2 B
1332 Sze "Chapter 3: Singapore" 54
1333 Sze "Chapter 3: Singapore" 54
1334 Sze "Chapter 3: Singapore" 54

desktop; a mobile commerce infrastructure to cater for mobile information services and transactions; a centralised computerised resource management system to manage the use of court resources, such as courtrooms, chambers and meeting rooms; an Info-communications Resource Centre; Electronic signages; fully interactive information kiosks; and a digital video wall-display in public areas providing access to general information on the Supreme Court.[1335]

After dealing with courtroom technologies in both England and Singapore, the time has come to shift our attention to South Africa.

C. South Africa

Among the technologies used in the courtroom in South Africa, video conferencing occupies a very special place. Such technology was at the centre of an investigation by the SALRC on the use of electronic equipment in court proceedings.[1336] Although video conferencing was envisaged, in this investigation, as a tool to be used for postponement purposes only in criminal cases against accused persons in custody awaiting trial, it is worthwhile to mention it in this discussion as it illustrates the use of technology in the justice system and by analogy it can apply to civil court proceedings. In order to be able to make postponements using video conferencing possible the so-called "video-conference courts" had to be set up. Such "video-conference courts" were supposed to link courts and the Department of Correctional Services. Both points in each location had to be equipped with the following equipment:

(1) a video link consisting of a video camera and two visual display devices (television monitors, plasma displays);
(2) an audio link consisting of an audio conferencing facility, which is interfaced with the video-conferencing unit;
(3) a telephone linking the court and the prison for a secure conference between the prisoner and the defence team;
(4) a fax machine connecting the court and the prison; and

1335 Sze "Chapter 3: Singapore" 69

1336 SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings (Postponement of Criminal Cases via Audiovisual Link)* 2003 (hereafter referred to as SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings*)

(5) in certain cases, a confidential interview booth allowing the defence team to confer with the prisoner in the prison via another video link in private.[1337]

The subject matter of the investigation by the SALRC was to determine whether existing legislation and constitutional principles could accommodate such a video-conferencing procedure. The SARLC identified two constitutional principles relevant in this case, namely the right of the accused person to be brought before the court,[1338] and the right of the accused person to a fair trial, including the right to a public trial before an ordinary court and the right to be present when being tried.[1339] In addition, the SALRC suggested taking into account the limitation clause in terms of section 36 of the Constitution.[1340]

Regarding the first-mentioned right, it is important to note that the use of technology takes place only after the first appearance and for postponement reasons only. This right is, thus, not upset in any way as the accused person will be brought before the court in accordance with section 35(1)(d) of the Constitution. One interesting question that might arise, however, is whether an accused person can be considered to be "brought" before the court if he remains in prison while his first appearance takes place by means of video conferencing. One must assume that it would have created great constitutional challenges, and it was probably a wise decision by the SALRC to recommend the use of video conferencing only after the first appearance.[1341] Nevertheless it is foreseeable that some time in future we will reach a point where first appearances could be made using video conferencing; it is only at that time, arguably, that certainty will be established as to the possibility of a very wide interpretation of "brought" as to include situations where accused persons will make their first appearance in court from prisons using video conferencing.

The second-mentioned right raises the same kind of concerns. It must be stressed that concerns pointed out here are hypothetical, as the use of video conferencing as envisaged in the SALRC investigation is limited to postponement and is, thus, not relevant in cases of trials. In a hypothetical scenario, however, where video conferencing were to be used in a trial, would the right of an accused person to be present when being tried be infringed if such person is not

1337 SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings* 6-7
1338 S 35(1)(d) of the Constitution
1339 S 35(3)(c) & (e)of the Constitution
1340 SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings* 7-8
1341 SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings* 33

physically present in court but can follow proceedings only through the video-conferencing system? The general rule is that the accused person must be present during criminal proceedings; this constitutional principle is reiterated by section 158(1) of the CPA.[1342] If one considers that the heading of section 158 is "criminal proceedings to take place in presence of accused" and that it provides for the possibility of evidence by the accused being given by means of closed circuit television or similar electronic media, one may conclude that an accused person may be considered to be present although he is participating only by means of some technology. This submission is further supported by the fact that section 159 of the CPA, dealing with the exceptions to the general rule requiring the presence of the accused in criminal proceedings, does not include the case of an accused interacting with the court by means of technology among the circumstances of absence. It remains, however, to be seen whether such an interpretation will pass constitutional test.

The SALRC points out that a number of Acts in South Africa provide for video conferencing. They include section 4 of the International Co-operation in Criminal Matters Act, 75 of 1996, section 25(2)A of the Competition Act, Act 89 of 1998, the Schedule to The Implementation of the Rome Statute of the International Criminal Court Act, Act 27 of 2002, and section 158(2) of the CPA.[1343] In addition, the investigation of SALRC led to the enactment of the Criminal Procedure Amendment Act 65 0f 2008. This Act amends the CPA by adding 4 sections, namely sections 159A, 159B, 159C and 159D. Section 159A defines a certain number of terms used in Act 65 of 2008; it, furthermore, provides that the accused is not required to appear or physically be brought before the court. Section 159B provides the requirements for the audio-visual appearance by the accused person. Section 159C provides for the technical requirements for the use of an audio-visual link. Finally, section 159D provides for the protection of communication between the accused person and his legal representative.

Section 158 (2) of the CPA was discussed in *S v De Grandhomme and Another*,[1344] case in which the advantages of leading evidence via electronic media were realised for the first time in South African legal history. In that case, a successful application by the prosecution in terms of that

1342 Except as otherwise expressly provided by this Act or any other law, all criminal proceedings in any court shall take place in the presence of the accused

1343 SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings* 14

1344 (C) 4-12-97 (case SS18/97 unreported)

section resulted in the court's convening at Telkom offices in Cape Town where a video conference facility was set up between Telkom and the geographical locations of the state witnesses, namely Moscow (Russia), Rancho Mirage (Florida, USA) and Boca Raton (California, USA). The advantages of using this method were seen in a trial without unreasonable delay compared to the situation of evidence on commission which requires many formalities to be complied with. Testimony via a video-conference facility was also the most cost-effective means of obtaining evidence from the witnesses. It cost the State about R40 000, while it was estimated that evidence on commission for the three witnesses would have cost around R185 000 had it been used.[1345]

The discussion on the courtroom technologies available in South Africa concludes the section on ICT applications used in the judicial system. The section has discussed three broad categories of applications, namely applications used to support court administrative staff and judges; applications allowing the exchange of information between courts, parties and the general public; and, applications that facilitate the presentation of electronic evidence in court. All these applications have been discussed with reference to England, Singapore and South Africa.

The discussion on the first category included firstly a point on basic technologies used by both administrative staff and judges and consisting of Office applications before dealing with specific applications supporting each category. An overview of the selected jurisdictions showed that Office applications are available in all courts in England and Singapore. In South Africa, however, because of difficulty to get recent data, there is uncertainty regarding the current situation. Based on figures from 2002, the availability is limited.[1346]

In respect of applications specific to administrative staff the focus was on the computerised case management, an organisational tool used by administrative staff members in managing cases from the entry point to the end of the case. The situation in the three jurisdictions covered showed that England is not among the top 12 European countries with the most effective and complete level of computerisation of the management and administration of courts.[1347] In South

1345 Howie "Evidence led via electronic media" Nov 1998 *De Rebus* 49 (hereafter referred to as Howie "Evidence led via electronic media")

1346 Ch 5 par 5.2.2.1.1

1347 Ch 5 par 5.2.2.1.2 A

Africa, it seems that case management systems are available only in certain courts in spite of the CPP project.[1348] The reference in that regard remains Singapore which has developed a very effective computerised case management system known as the Civil System. There is almost no detail on a case that cannot be found on the Civil System. It allows the tracking of a case from its inception to its finalisation with mechanisms to detect any problem with such case, including any form of inactivity or any breach by the parties of a court order.[1349]

Regarding applications for supporting judges, the discussion dealt with individual tools designed to help judges in their daily activities and included office tools, legal research tools, and judgment and sentencing tools. In England a project known as JUDITH contributed to the use of computers by judges for their daily activities.[1350] In Singapore judges are equipped with laptops since July 2001 and can access the Supreme Court's network from their homes via the Citrix server and prepare their hearings by reading electronic cases or carrying out the necessary legal research in that respect.[1351] In South Africa, the Digital Nervous System or DNS project, although not designed specifically for judges, contained applications relevant for judges, such as the Internet, the e-mail, online applications, or electronic databases.[1352] The picture of the DNS project at mid-2002 showed a project well on track.[1353] There is, however, no clear indication of whether IT projects focusing only on judges have been introduced in South Africa. In addition no information was found on the applications specific to judges that are currently in use in South African courts.[1354]

The second category of ICT applications used in the judicial system that was discussed consists of applications allowing the exchange of information between courts, parties and the general public. These applications include, among other things, a court website where information regarding the court's organisation and activities can be found; downloadable forms might also be available on the website to permit for the electronic submission of claims. Other important tools for the electronic communication and information exchange between the courts and their

1348 Ch 5 par 5.2.2.1.2 C
1349 Ch 5 par 5.2.2.1.2 B
1350 Ch 5 par 5.2.2.1.3 A
1351 Ch 5 par 5.2.2.1.3 B
1352 Ch 5 par 5.2.2.1.3 C
1353 See Ch 5 par 5.2.2.1.1 above
1354 Ch 5 par 5.2.2.1.3 C

environment include electronic registers, business or land registers, for example, or text-messaging application allowing parties to be informed of the status of their case on the court list.[1355] The situation of these applications in the selected jurisdictions is a follows. England follows a centralised approach for the provision of information regarding the courts with court information now provided on the Ministry of Justice website www.justice.gov.uk, but currently in the process of moving to www.gov.uk. In addition for the electronic exchange of court documents there is the Money Claim Online (MCOL) which is a HMCTS Interned-based service for claimants and defendants to make, or to respond to, a money claim on the Internet in a convenient and secure way.[1356] In Singapore court information can be obtained from the Supreme Court's website, the Mobile Information Service or via the infokiosks available within the premises of the Supreme Court. In addition the filing and service of court documents can easily be done through the Electronic Filing System. The vision of a paperless courtroom is a reality in Singapore.[1357] In contrast, South Africa is lagging behind despite the fact that general court information is available from the website of the Department of Justice and Constitutional Development www.justice.gov.za. In respect of the electronic exchange of information there is a big gap with Singapore. Apparently South Africa is still at a theoretical level with the CPP although a pilot project was initiated. There is no indication that electronic exchange of information is taking place at this stage in South Africa.[1358]

The last category of ICT applications used in the judicial system comprises applications used in the courtroom. They include hardware and software designed to help parties in the presentation of their case in court, such as computers and multimedia screens, video conferencing, electronic evidence presentation software, and so on. In 2012, the UK counted 12 specifically equipped EPE courtrooms, in other words courtrooms equipped with Electronic Presentation of Evidence facilities.[1359] In Singapore, the first technology court was introduced 20 years ago and offered advanced technologies such as a digital recording system, audio-visual facilities and video conferencing. Since then there has been even more advances with The Technology Court 2.[1360]

1355 Ch 5 par 5.2.2.2
1356 Ch 5 par 5.2.2.2 A 2
1357 Ch 5 par 5.2.2.2 B
1358 Ch 5 par 5.2.2.2 C
1359 Ch 5 par 5.2.2.3 A
1360 Ch 5 par 5.2.2.3 B

In South Africa an important technology used in the courtroom is video conferencing. It was for instance used with success in *S v De Grandhomme and Another*,[1361] case during which witnesses scattered around the world were able to give evidence through video conferencing.[1362]

This section has been useful in identifying and understanding ICT applications used in the judicial system. In addition, it has provided information regarding the availability of these applications in the jurisdictions under consideration. With such knowledge in place, one can look at the legal challenges that the implementation of some of these applications may raise. The discussion that follows focuses on challenges from a civil procedure point of view and is entitled rules of civil procedure and electronic justice.

5.3 Rules of civil procedure and electronic justice

The second part of this chapter analyses rules of civil procedure and their effectiveness in dealing with electronic justice, in other words the use of ICTs in the administration of justice. Rules examined in this part include all those rules applicable to both application and action proceedings from the initiation of the litigation up to its conclusion and relevant to the exchange of documents or information. Given the amount of exchange of information occurring among parties and the courts during such procedure, the idea is to examine the challenges that may appear if such a procedure had to be done electronically. The procedure in application proceedings will normally be introduced by means of a notice of motion accompanied by a founding affidavit. Such proceedings are decided on the papers placed before the court. It appears easy to file such application papers electronically to the court. What are the legal consequences in doing so? In contrast, in action proceedings the procedure is more complex; it is initiated by a summons which is followed by four stages, the pleading stage, the pre-trial stage, the trial and the judgment stage. Technology may be used at each stage, and this raises as a concern the extent to which such use may challenge the relevant rules of procedure. The rules of interest to be examined include those relating to the service of documents which start legal proceedings, also known as process of the court (summons, notice of motion…) and go on to include the delivery of documents and notices, to pleadings, to discovery, inspection and production of documents, pre-trial conference, and trial. For the sake of order and convenience,

[1361] (C) 4-12-97 (case SS18/97 unreported)

[1362] Ch 5 par 5.2.2.3 B

the rules are discussed below according to a three-pronged division consisting of rules for the service of documents in the first group, rules for discovery in the second, and rules for documents to be used at the court's hearings in the third and final group.

5.3.1 Service of documents

The service of two categories of documents, namely court process on the one hand and other documents such as notices and pleadings on the other hand, falls under this heading.

5.3.1.1 Court Process

The first documents to be served in a civil case are court process, namely summons or notice of motion, which start legal proceedings. The normal procedure will be for an attorney to draw such documents and lodge them with the registrar or clerk of the court who registers them, assigns them a case number, and opens a court file in which to put them. Then the summons or notice of motion is transmitted to the sheriff to be served on the defendant or respondent. After successful service, the sheriff brings back the return of service which constitutes proof of service, and this document is placed in the court file with a copy sent to the attorney who requested such a service.[1363] In an era where technology is ubiquitous, it will be appropriate to reflect on the possible computerisation of the above procedure and its legal implications. This is the reflection carried out in the following lines in respect, firstly, of application proceedings before dealing with action proceedings.

5.3.1.1.1 Application proceedings

The introduction of technology in application proceedings will result in a notice of motion and the supporting affidavit being filed electronically to the registrar or clerk of the court and, if applicable, served electronically to the party against whom relief is claimed.[1364] At this stage the first legal question which arises is whether a notice of motion or an affidavit in electronic form is valid in terms of the Uniform Rules of Court or Magistrates' court rules; secondly, are there any

---

1363 *Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa* 27; Peté, Hulme, Du Plessis, Palmer and Sibanda *Civil Procedure a Practical Guide* (2nd ed) 2013 (hereafter referred to as Peté *et al Civil Procedure, a Practical Guide*) 101-102

1364 The application procedure is provided for by rule 6 and rule 55 of the Uniform Rules of Court and Rules Regulating the Conduct of Proceedings of Magistrates' Courts of SA (Magistrates' court rules) respectively. - As the procedure is similar in both sets of rules, the discussion will rely on the Uniform Rules of Court.

legal obstacles preventing the electronic filing or service of these documents? Finally, from a technical point of view, what technologies are required to be in place for such a procedure to be feasible?

A notice of motion and its affidavit would need to be in electronic form for an electronic application procedure to take place. This, in turn, raises the issue of the validity of such documents. To determine such validity, one needs to look at existing legal provisions. Both the Uniform Rules of Court and the Magistrates' court rules do not contemplate the possibility of the existence of a notice of motion and its supporting affidavit in electronic form as implied by their rules dealing with the service of process of court.[1365] From the manners of service under these rules, it is clear that the process of court and its supporting affidavit must be in paper form. In addition, in terms of the Magistrates' court rules, there is an explicit requirement for a process of court to be on a paper known as A4 standard paper of a size of approximately 210mm by 297mm.[1366] Thus, as a consequence a notice of motion and its supporting affidavit in electronic form is not currently valid in South Africa. A precondition for these documents to become valid is to include electronic service in the existing manners of service for a process of court and to amend the above requirement of A4 paper.

In the hypothesis that a notice of motion and its affidavit in electronic form were valid, the logical consequence would be for such notice of motion and affidavit to be able to be filed or served electronically. Would such electronic filing or service be valid in terms of existing rules? In accordance with the relevant rules of procedure it is not possible to file a notice of motion and its supporting affidavit electronically with the registrar.[1367] This is normal, as this possibility was clearly not envisaged when adopting these rules. To remedy to this situation and embrace the digital era, one needs to adopt rules of procedure that take electronic documents into account.

From a technical point of view, the implementation of such a system will require technologies facilitating the exchange of information among all actors, namely the applicant, the registrar, the sheriff, and the respondent. Such technologies must also be able to respond to the needs for a revenue stamp to be affixed to the electronic notice of motion and for an advanced electronic

1365 Rule 4 and rule 9 respectively
1366 Rule 1(4)(c)
1367 Rule 4(1)(a) of the Uniform Rules of Court

signature to be used for the electronic affidavit. As has already been noted above, Singapore can serve as a good model in the design and implementation of such technologies. Singapore has implemented a very successful litigation system, known as the Electronic Filing System. Under this system there is a service called Electronic Filing Service containing a web-based front-end system allowing lawyers to file documents electronically to courts and to serve court documents to other law firms. In addition, another important component of the Electronic Filing System is the VAN Operator Filing Processing System. This system is used to determine transactions charges such as court fees, processing fees and hearing fees; it also allows for the collection of money from law firms on behalf of the judiciary. [1368] Thus, such an application, if used in South Africa, could easily manage the payment of revenue stamps. Finally, to deal with electronic affidavits, a component called the Commissioner for Oaths System allows for affidavits before Commissioners for Oaths to be made electronically. South Africa can also learn from this experience.

The Singapore Electronic Filing Service is governed by Order[1369] 63A. In accordance with rule 2 of this Order, an electronic filing service may be established by the Registrar with the approval of the Chief Justice. In addition, the Registrar must determine the category of documents that may be filed, served, delivered or conveyed by means of that service. In compliance with such powers, the Registrar has established an electronic filing service, known as the Integrated Electronic Litigation System or eLitigation and accessible at www.elitigation.sg, and has appointed, in terms of rule 3 of the Order, CrimsonLogic Pte Ltd as the electronic filing service provider for this service and the Electronic Litigation Systems Committee of the Singapore Academy of Law as its superintendent.[1370] As far as documents are concerned, it must be stated that most documents required to be filed with, served on, delivered or otherwise conveyed to the Registrar, must be done using the Electronic Filing Service.[1371] Documents for which the use of the Electronic Filing Service is not required include almost exclusively documents relating to various proceedings commenced before 2003.[1372] It is important to note that the Electronic Filing

1368 Ch 5 par 5.2.2.2 B

1369 An Order is a division used in the Rules of Court of Singapore to separate between topics. Each Order is divided into rules.

1370 Direction 101 of the Supreme Court Practice Directions (hereafter referred to as e-Practice Directions)

1371 Direction 104(1) of the e-Practice Directions

1372 Direction 104(2) of the e-Practice Directions

Service can be used not only online but also through a service bureau which the Registrar can establish directly or through agents to assist in the filing, service, delivery or conveyance of documents using the Electronic Filing Service.[1373] The service bureau is particularly relevant for litigants in person as, in most cases, they will not be registered on the Electronic Filing Service. The registration on the Electronic Filing Service is open to any entity by application to the Registrar to become a registered user.[1374] Once granted such status, the entity may designate any of its partners, directors, officers or employees to be an authorised user.[1375] For the purpose of this Order, an entity includes a law firm, the Attorney-General's Chambers, a government department, a public authority, or a company or other body corporate.[1376]

Order 63A deals with other important issues such as the signature of electronic documents, the date of filing, the time when service begins to run, and affidavits in electronic form, to name but a few.

The requirement of a signature for a document filed, served, delivered or conveyed using the Electronic Filing Service is satisfied by the use of the identification code of the authorised user or registered user.[1377] Regarding the date of filing, depending on different circumstances, it will be the date and the time that the first part of the transmission is received in the computer system of the electronic filing service provider or of the Registrar.[1378] The time when service begins to run is the time when the Registrar's notification of acceptance of documents filed is received in the computer system of the registered user or by the service bureau.[1379] Lastly, for affidavits in electronic form, it is provided that they may be filed in Court using the Electronic Filing Service under the following conditions:

a) Be sworn in the normal way that the original paper affidavit is signed;
b) It is created as a true and complete electronic image of the original paper affidavit; and

[1373] Rule 4(1) or Order 63A
[1374] Rule 5(1) of Order 63A
[1375] Rule 5(2) of Order 63A
[1376] Rule 1 of Order 63A
[1377] Rule 9(1) of Order 63A
[1378] Rule 10(1) of Order 63A
[1379] Rule 11(1)&(2) of Order 63A

c) The original paper affidavit is retained for 7 years by the party who filed it.[1380]

In England, it is also possible to file documents to courts by electronic means. Indeed specified documents may be filed by parties to specified courts by e-mail or via an online forms service.[1381] A specified document is a document listed on Her Majesty's Courts and Tribunals Service website as a document that can be filed by e-mail or is available for completion on the online forms service accessible on the website.[1382] Similarly, a specified court is a court that either is listed on Her Majesty's Courts and Tribunals Service website as able to receive documents filed via the online forms service or has published an e-mail address for the filing of documents on that website.[1383] To summarise, Practice Direction 5B is divided in three sections. Section 1deals with the communication and filing of documents by e-mail. It is important to note under this section that it is not possible to file a document by e-mail if a fee is required for such filing.[1384] The only exception is an application to the Preston Combined Court using the PREMA (Preston E-mail Application Service) User Guide and Protocols.[1385] The section also provides the technical specifications for e-mails.[1386] Section 2 deals with the online forms service. In contrast to the filing by e-mail, a document can be filed using the online forms service for a claim requiring the payment of a fee. The payment must be made using the facilities available on the online forms service before filing the document to the specified court.[1387] Lastly, section 3 deals with general provisions, such as the fact that a document is not filed until the transmission is received by the court,[1388] or, if the transmission is received after 4pm, it will be considered received the next court day.[1389] In addition, the party filing is responsible to ensure that the transmission is done within the relevant time limits.[1390]

1380 Rule 15(2) of Order 63A
1381 Par 1.1 & par 1.2 of Practice Direction 5B- Electronic Communication and Filing of Documents (hereafter referred to as Practice Direction 5B)
1382 Par 2.1(2) & par 5.2(2) of Practice Direction 5B
1383 Par 5.2(1) & par 2.1(1) of Practice Direction 5B
1384 Par 3.2 of Practice Direction 5B
1385 Par 3.2A of Practice Direction 5B
1386 Par 4.1-4.8 of Practice Direction 5B
1387 Par 6.2 of Practice Direction 5B
1388 Par 8.2 of Practice Direction 5B
1389 Par 8.4 of Practice Direction 5B
1390 Par 8.5 of Practice Direction 5B

The situation in England concludes the discussion on the legal issues raised by the introduction of technology in application proceedings, in other words the legal validity of a notice of motion in electronic form and of the electronic service of such a notice of motion. The discussion which follows focuses on the same aspects but with reference to a summons in action proceedings.

5.3.1.1.2 Action proceedings

The action procedure begins with the issue of a summons. Every person making a claim may approach the office of the registrar or clerk of the court to issue a summons addressed to the sheriff directing him to inform the defendant of the claim and the steps he needs to take to defend such a claim.[1391] The summons must be signed by the plaintiff if he is unrepresented or by his attorney in the contrary; in addition it must contain the plaintiff's *domicilium citandi address* or the attorney's physical address and, where available, the plaintiff's or the attorney's e-mail address.[1392] The summons is then signed and issued by the registrar or clerk of the court.

The analysis of the above procedure in an e-justice context shall be conducted following a five-stage approach: the first stage concerns the exchange taking place between the plaintiff/attorney and the registrar or the clerk of the court; the second stage links the latter to the sheriff; the third stage brings together the sheriff and the defendant; the fourth stage concerns the feedback from the sheriff to the plaintiff via the registrar or clerk of the court; and, finally, the fifth stage sees the interaction between the defendant and the registrar or clerk of the court. The exercise at this point seeks to assess the legal impact if such a procedure were to be conducted totally electronically.

Since such electronic procedure is possible only if the summons is in electronic form, it becomes imperative to deal first of all with the legal validity of an electronic summons. Although there seems to be no specific provision preventing such court process to be in electronic form, the intention of the drafters of both the Uniform and Magistrates' courts rules drawn from the mode of service of the summons appears to exclude such an eventuality. The rules distinguish between the service of a document initiating proceedings, such as a summons, and the service of subsequent documents and notices in the suit. Contrary to the freedom for parties to determine

1391 Rule 17 of the Uniform Rules of Court
1392 Rule 17 (3) (a) & (b) of the Uniform Rules of Court

the mode of service of the latter, the former will be, as a general rule, restricted to personal service or service through physical address or postal address.[1393] Exceptionally, service of a summons can be effected differently from the above as provided by rule 4(2) of the Uniform Rules of Court, such as by way of publication in a newspaper or other publication. It appears, however, that the electronic service of a summons is not possible at this stage in South Africa. This can possibly be attributed to a lack of confidence by the courts in technology, even though technology is arguably the most effective notification channel currently. It should, therefore, be right to put electronic service on a par with other modes of service listed under rule 4(1)(a) of the Uniform Rules of Court and its equivalent in Magistrates' courts as there seems to be no substantial reason to exclude the electronic service of a summons in the digital age while it is accepted for subsequent documents and notices in the suit. Indeed, if such service is not reliable for a summons, then it should not be accepted for other documents and notices either. On the argument that the necessity for a summons to be signed by the plaintiff or his attorney and by the registrar or clerk of the court constitutes an impediment to the existence of an electronic summons, one can dismiss such argument by saying that the use of an electronic signature can satisfy such requirement as observed above in Singapore where the requirement of a signature is satisfied by the use of the identification code of the authorised user or registered user in the framework of the Electronic Filing Service.

On the issue of the existence of a summons in electronic form, the examples of Singapore and England, explored above, show that technically this is not a difficult task; one needs simply to develop a software programme that will make it possible to fill and complete the summons online. Another possible option, albeit less satisfactory, is to scan the paper summons to create an electronic copy. Considering the fact that nowadays in most cases summonses will be produced by means of a computer, it will be right to favour the first scenario.

Now that the issue of legal validity of an electronic summons has been discussed, it is appropriate to deal with the five-stage approach pointed out above.

Traditionally, a summons is filed in court manually in paper form. In an e-justice context this step, which constitutes stage 1 of the above division, can be done electronically. In other words,

[1393] Rule 17(3)(d) & (e) of the Uniform Rules of Court

the plaintiff, or better his attorney, would not need to go physically to the registrar or clerk of the court to file the summons in paper form, but would rather be able to file it electronically from the convenience of his home, office or anywhere else. In addition, computer facilities may be set up in courts to assist in the electronic filing of summonses and other documents in general. The Singapore Electronic Filing Service discussed above can also be a good model to follow for this stage.[1394] What are the legal issues raised by such interaction between the plaintiff or his attorney and the office of the registrar or clerk of the court if such a procedure had to be done electronically? A close look at rule 17(1) of the Uniform Rules of Court reveals nothing, suggesting that such interaction cannot be done electronically. Indeed, the provision stipulates only that a claim must be done through the office of the registrar without specifying the manner. Supposing the necessary technical infrastructure was in place, would it be necessary to amend the above rule to facilitate the making of an electronic claim through the office of the registrar? The answer is in the negative as there is no specific reference to the manner in which the claim must be made; thus, an electronic claim is not excluded although in practice it is done in paper form. To remove any doubt regarding the possibility of making a claim through the office of the registrar by electronic means, however, a practice directive must be adopted to clarify that point.

Stage 2, linking the registrar or clerk of the court with the sheriff, is the phase where technology should be the easiest to introduce as it does not cause any major legal challenges; rather the communication taking place at that stage accelerates the procedure.

The exchange of information between the sheriff and the defendant in stage 3 is very important as it is crucial to be sure that the defendant has been informed of a claim against him in accordance with the legal maxim *audi alteram partem*. How can one ensure this if the communication is done electronically? Before answering this question, it is important to deal firstly with the traditional service. Traditionally, service by the sheriff on the defendants will take the following forms: delivering a copy on the defendant personally; leaving or delivering a copy at the place of residence, business or employment of the defendant; or leaving or delivering a copy at the *domicilium citandi* address, and so on. To ensure that the service was successfully effected, there must be a form of proof such as a return of service by the sheriff. Likewise, if service is effected electronically, there must be a means to prove such electronic service, for

[1394] Ch 5 par 5.3.1.1.1

example a functional equivalent of the traditional return of service or any other appropriate electronic proof of service. A good example of an electronic proof of service is the Google's read receipt, an email notification sent to the sender of an email when the recipient opens the email. The receipt confirms not only that the recipient has seen the message but also gives the time the message was seen.[1395] The Singapore Electronic Filing Service has also developed an appropriate response to that concern as it automatically generates a Certificate of Service and stores it in the electronic case file when documents are served using such system. These two illustrations show that technology has the potential to ensure an even more efficient service as the sender is informed not only of the receipt but also of the receipt time by the recipient. Except when service is done by delivering a copy to the person personally, usual modes of service will normally not offer the same level of guarantee of receipt by the intended recipient as the electronic service. Hence, the electronic service of a summons should be accommodated as other modes of service as long as the necessary precautionary measures are in place.

The fourth stage consists of the communication of the return of service or proof of service by the sheriff to the plaintiff via the registrar or clerk of the court. What would be the legal issues raised if such communication had to be performed electronically? Rule 4(13) of the Uniform Rules of Court requires that, after service, a copy of the summons together with a proof of service, for example a certificate and seal of office of the sheriff be sent to the registrar as well as particulars of charges for the cost of effecting such a service. The sheriff will, therefore, need to communicate the above three sets of documents. The electronic communication of the first document, that is, the summons, has already been addressed above. The second document to be communicated is the certificate and seal of office of the sheriff. To perform such communication electronically, the main obstacle will be the use of the seal of office of the sheriff on the certificate which will exclude the possibility of electronic communication as the law stands. To make such an electronic communication possible in the future, the above rule must be amended to allow for functional equivalents of a seal of office to be used; thus, the sheriff will be able to use an electronic signature on the certificate as a means of authentication. The electronic communication of the second document would in this way be possible. Lastly, the electronic communication of the third document or particulars of charges for the cost of effecting service

[1395] https://support.google.com/mail/answer/1385059?hl=en(accessed on 20/01/2015)

does not seem to create much difficulty. Firstly, nothing prevents such eventuality, and, secondly, electronic service is charge-free, so there is no charge to report.

The fifth stage is the exchange between the defendant and the registrar or clerk of the court and the plaintiff. This stage consists of the filing of the notice of intention to defend. The issue is to determine whether such an exchange can validly be performed by the use of electronic means. Before dealing with the validity *per se*, it should be pointed out that, in theory, it will be very convenient for such an intention to defend to be filed electronically, as it will save time and effort to do so. This will be even easier in the scenario envisaged above where the four preceding stages rely on electronic means. Even if such was not the case, insofar as the plaintiff includes his electronic address in the summons, the defendant can still use it to serve his notice of intention to defend on him. Will such a service comply with the rules of procedure?

It will, as rule 4A(1) of the Uniform Rules of Court accepts that the service of documents and notices other than documents initiating proceedings may be effected, amongst other means, by facsimile or electronic mail to the respective addresses provided. In addition, Chapter III, Part 2 of the ECT Act is applicable to such a service by facsimile or electronic mail,[1396] which does not need to be effected through the Sheriff.[1397] The filing with the registrar of originals of documents and notices cannot, however, be done by facsimile or electronic mail.[1398] Hence, for electronic filing with the registrar of original documents to be valid, subrule 4A(5) must be amended accordingly.

From the discussion on the service of court process conducted above, one can highlight the following aspects. The discussion was divided in court process used in application proceedings, that is, notice of motion on the one hand and court process used in action proceedings, that is, summons on the other hand. For each category it was important to examine the validity of such documents in electronic form and the legal issues raised in case of electronic service in terms of the Uniform Rules of Court and Magistrates' court rules. It was pointed out that these court rules exclude the validity of both categories of court process in electronic form as inferred from the

1396 Rule 4A(3)
1397 Rule 4A(4)
1398 Rule 4A(5)

modes of service provided in both court rules.[1399] In both cases electronic service is not listed among the accepted modes of service. Given these limitations by the above court rules to deal with such electronic service of court process, guidance was sought from Singapore and to a certain extent from England. In Singapore court process can be introduced by electronic means using the Electronic Filing System as provided by Order 63A. In England, it is also possible to file court process to courts by electronic means in terms of Practice Direction 5B. Apart from court process, however, other documents such as affidavits and pleadings can also be filed. Their regime seems to be less restrictive. It is discussed in the following lines.

5.3.1.2 Other documents

Other documents include, on the one hand, a number of supporting affidavits and annexures as well as the respondent's answering affidavits in application proceedings, and, on the other hand, pleadings in action proceedings.

5.3.1.2.1 Application proceedings

As has already been noted, application proceedings are, as a general rule, initiated by a notice of motion. The service of this process of court is discussed above.[1400] It has been further pointed out above that the notice of motion is accompanied by the founding affidavit. In addition to that, supporting affidavits may be necessary as well as any annexures thereto. The supporting affidavits and their annexures will then be attached to the notice of motion and served according to the rules explained above for the service of documents initiating proceedings.[1401]

After being served with the application papers, the respondent, if he intends to oppose the application, must file a notice of opposition.[1402] Within fifteen days after filing such notice, he must deliver his answering affidavit with any relevant documents.[1403] Then, the applicant may deliver a replying affidavit, which can be followed, at the discretion of the court, by further

1399 Rule 4 and rule 9 respectively
1400 Ch 5 par 5.3.1.1.1
1401 Ch 5 par 5.3.1.1.1
1402 Rule 5(d)(i)
1403 Rule 5(d)(ii)

affidavits by either party.[1404] Finally, the application is set down for hearing by the delivery of a notice to set down.[1405]

The procedure described above illustrates the amount of exchange taking place between parties with documents moving back and forth, and clearly ICTs can play a large role in facilitating such an exchange. In accordance with rule 4A examined above, the exchange can be validly performed using ICTs. Indeed the service of the notice of opposition and all other affidavits can be effected legally by facsimile or electronic mail. Regrettably, however, the filing with the registrar of a notice of set down will need to be in paper form, although a paperless procedure will speed up the whole process. It is appropriate to reiterate the position expressed above on the necessity to permit a full electronic procedure by amending subrule 4A (5) of the Uniform Rules of Court.[1406]

5.3.1.2.2 Action proceedings

In action proceedings, "other documents" refer to pleadings, that is, written statements made by the parties and containing each party's main allegations, in other words the material facts on which the plaintiff's claim is based and those on which the defendant's defence is based.[1407] They may also include other notices, such as the notice to set down. At this point it is important to distinguish between the pleading stage and the trial and evidence stage. The pleading stage is concerned only with the written statements and not with the evidence relied upon to support allegations, which evidence is presented at the trial and evidence stage through witnesses appearing in person or other evidence such as documents.[1408]

The main pleadings include the summons and particulars of claim, the notice of intention to defend, the plea and counter-claim, and the replication. A summons is a written judicial demand which institutes action proceedings. It either contains the particulars of claim (including the cause of action) in its body or these are attached to it. The notice of intention to defend is merely a notice informing the court and the plaintiff that the defendant intends to defend the action. The

1404 Rule 5(e)
1405 Rule 5(f)
1406 Ch 5 par 5.3.1.1.2
1407 Peté *et al Civil Procedure, a Practical Guide* 112
1408 Peté *et al Civil Procedure, a Practical Guide* 112

service of both the summons and notice of intention to defend has been addressed above.[1409] Regarding other mentioned pleadings, namely the plea and counter-claim and the replication, it is important firstly to point out that the plea is the defendant's reply to the plaintiff's particulars of claim and presents the defendant's defence to the plaintiff's claim, while the counter-claim is a distinct claim brought by the defendant against the plaintiff and associated with the existing action for convenience only.[1410] Finally, the replication is the plaintiff's response to the defendant's plea. All these pleadings are subject to rule 4A of the Uniform Rules of Court and can thus be exchanged by electronic means between parties. The setback however, remains in that they need to be filed with the registrar in paper form, which defeats the attempt to encourage the use of electronic means. Indeed, even if parties are allowed to exchange the pleadings electronically they still need to go to court to file the original document, which is clearly unsatisfactory as the benefits of technology are then only half enjoyed. It cannot be stressed enough that there is a need to unlock subrule 4A(5) not only to boost the use of technology but, even more, to take advantage of all the benefits it provides.

Regarding the service of other notices, such as a notice to set down, a case worth mentioning is the landmark case of *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens*.[1411] An application for substituted service by the plaintiff was made under this case to serve a notice of set down and pre-trial directions on the defendant by sending the notice via a Facebook message. This option was considered after all attempts made by the plaintiff to serve various notices on the defendant turned out to be unsuccessful. As noted by Steyn J, the application was possible only because an amendment to the Uniform Rules of Court provided for service by way of electronic mail.[1412] Noting changes in the technology of communication and the need for the law to recognise and accommodate those, Steyn J was satisfied that as much as in 1947 it was considered appropriate to order for substituted service to be effected by affixing a notice on the

1409 Ch 5 par 5.3.1.1.1

1410 Peté *et al Civil Procedure, a Practical Guide* 166 & 183

1411 (KZN)(unreported case no 6846/2006, 3-8-2012)

1412 *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens* (KZN)(unreported case no 6846/2006, 3-8-2012) at par [2]

door of a court building, in 2012 it should be appropriate to grant an order allowing substituted service to be effected by serving a notice by way of a Facebook message.[1413]

Unlike the service of documents initiating proceedings,[1414] the service of other documents as defined above can be effected legally by electronic means in accordance with rule 4A of the Uniform Rules of Court as confirmed in the above case. However, this rule does not provide for the possibility to file documents with the registrar by electronic means. This clearly is an obstacle to the promotion of electronic justice and should be amended accordingly in line with Order 63 A in Singapore and Practice Direction 5 B in England as discussed above.[1415] This point concludes the discussion on the legal issues raised by the introduction of technology to what can be referred to as the first phase of judicial proceedings consisting of the service of court process and exchange of various documents that follows. At the pre-trial phase, legal issues raised are even more important as is shown in the discussion on discovery below.

5.3.2 Discovery

5.3.2.1 Introduction

Discovery is a pre-trial procedure whereby, upon request, a party discloses to the requesting party all documents in his possession that might be relevant to the trial and eventually gives access to them. As noted in the previous chapters, technology has revolutionised the world as information is increasingly created, processed, stored and communicated electronically. The result is a preponderance of information stored electronically. Such a category of information is not exempt from discovery; actually given the fact that most information is electronically-stored, there is likelihood that discovery will in the future mostly concern electronically-stored information (ESI), if this is not the case already. This section is dedicated to analysing the discovery of ESI, also known as electronic discovery, which includes a variety of documents and data stored on a computer or similar device, such as e-mail, web pages, word processing files, computer databases, or documents stored on servers or back-up systems. The particularity of ESI is that it exists in a medium readable only through the use of a computer. Such media range from

---

1413 *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens* (KZN)(unreported case no 6846/2006, 3-8-2012) at par [1] & [2]

1414 Ch 5 par 5.3.1.1

1415 Ch 5 par 5.3.1.1.1

cache memory and magnetic disks (computer hard drives or floppy disks) to magnetic tapes passing by optical disks (DVDs or CDs).[1416] It differs from paper documents in that the latter are writings on paper that can be read without the aid of computers. The procedural rules that govern electronic discovery in South Africa are the same than those regulating traditional discovery. This section analyses these rules to ascertain their effectiveness in dealing with electronic discovery. Before dealing with South Africa, however, the section looks at the jurisdictions of Singapore and England and considers their approach to electronic discovery, the issues raised there, and how those countries managed to overcome them in order to see to what extent their experience can provide guidance to South Africa.

5.3.2.2 England

Electronic discovery was among the issues considered in the review of the civil litigation costs in England. Such costs were seen to be exorbitant in some areas of civil litigation and, therefore, constituted a hindrance to access to justice. The review resulted in a series of recommendations which led to the reform of certain aspects of the civil litigation, in particular discovery.

Jackson notes, with regard to discovery, that the existence of a massive amount of electronic documentation constitutes an acute dilemma for the civil justice system as there is, on the one end of the spectrum, the benefit that the full disclosure of electronic material may have in reaching the truth compared to the archaic discovery of documents, but, on the other end of the spectrum, however, the cost involved in the process of retrieving, reviewing and disclosing electronic material can be excessive.[1417] Such a dilemma must be addressed and the approach taken by Jackson in that process, and adopted here, is two-fold, firstly, to give an overview of E-disclosure[1418] with some benefits and pitfalls, and, secondly, to analyse rules governing the use of e-disclosure in litigation.[1419]

1416 *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery* (Sedona Conference SM Working Group Series 2004) (hereafter referred to as *The Sedona Principles (2004)*) 1

1417 Jackson *Review of Civil Litigation Costs: Preliminary Report Volume 2* 2009 (hereafter referred to as Jackson's *Interim Report* Vol 2) 373

1418 "Processes involved in giving disclosure of electronic material" Jackson's *Interim Report* Vol 2 373; E-disclosure should thus be understood as electronic discovery and *vice-versa*.

1419 Jackson's *Interim Report* Vol 2 373

5.3.2.2.1 Overview of e-disclosure

The overview of e-disclosure is addressed below in points A to C, dealing respectively with Description, Functioning and Rules and Practice Directions.

A. Description

E-disclosure is the process during which ESI is searched and organised for litigation.[1420] It will generally include the following five steps:

(i) identify the extent of the relevant documentation or information, where it is and in what form;

(ii) collect that documentation and information, removing duplicates or irrelevant material; categorise it for ease of review by the legal team and place it where the legal team can review it;

(iii) if the parties proceed with litigation, review the reduced amount of documentation and information for privileged material, decide what is suitable and necessary for disclosure; list it and disclose the list to the other parties;

(iv) provide the other parties with access to the disclosed documentation and information; and

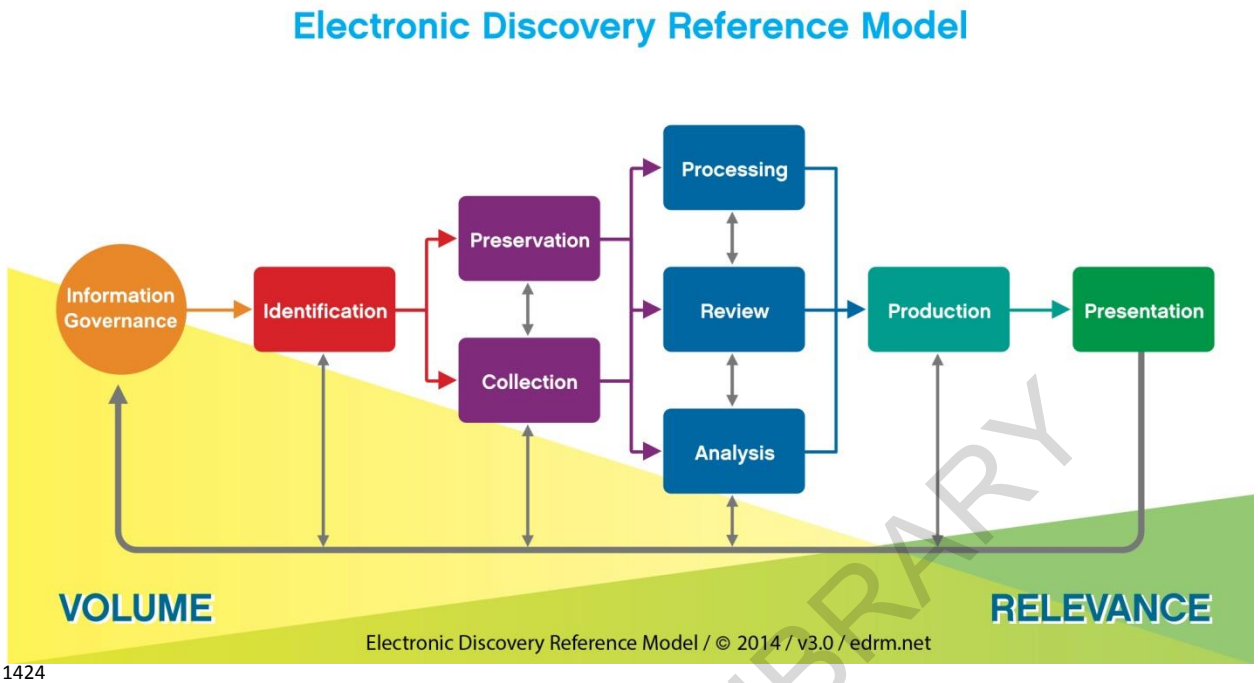
(v) review and organise the documentation and information disclosed by other parties, in order to facilitate the more detailed review by the legal team.[1421]

Traditionally these steps are conducted by accessing the room where documents are stored to copy and read them. Now that information is electronically stored, the approach must change; litigants must decide on what and where[1422] to search and for what purpose. They can use electronic devices or software tools, for example, or request the assistance of specialist companies.[1423] An interesting software tool is discussed below under point B.

B. Functioning

An interesting model used in the disclosure of ESI is the "Electronic Discovery Reference Model" (the EDRM). The diagram below illustrates how e-disclosure is conducted through the EDRM.

1420 Jackson's *Interim Report* Vol 2 376
1421 Jackson's *Interim Report* Vol 2 376
1422 Which servers, computers, back-up devices, mobile phone records?
1423 Jackson's *Interim Report* Vol 2 376



[1424]

A brief description of this diagram is given below by providing a short explanation of activities involved for each step.[1425]

Information governance is the organisation of information in an orderly and logical manner to facilitate the recovery of information when the need arises. It is comparable to a good filing system in a traditional setup.

Identification is the step during which relevant information to be searched for, and its location, is identified.

Preservation involves the protection of ESI against inappropriate alteration or destruction.

Collection is the retrieval of information from the location it was stored in and its transfer to a computer where it can be processed, reviewed or analysed.

Processing consists in the reduction of ESI and its converting, if necessary, to forms more suitable for review or analysis.

1424 http://www.edrm.net/resources/edrm-stages-explained (accessed on 4/5/2015)

1425 This includes information gathered from both Jackson's *Interim Report* Vol 2 378-379 and http://www.edrm.net/resources/edrm-stages-explained (accessed on 4/5/2015)

Review is the step where ESI is evaluated to determine its relevance and to identify privileged information.

During the analysis, the evaluation of the content and context of ESI is performed, including key patterns, people, topics and discussion.

Production is the delivery of ESI to others in an appropriate form and through the use of appropriate delivery mechanisms. Production can be done by means of a disc where information will be transferred beforehand or by means of a hosted website amongst other things.

Presentation, finally, is the step where ESI is displayed before audiences, especially in native or near-native form.

In practice, e-disclosure is carried out either by external service providers specialising in the electronic disclosure field or by in-house specialists in electronic disclosure using appropriate software. It is also important to mention the existence, since 2003, of a body known as LIST whose purpose is to promote harmony in the use of technology in the litigation process and alternative dispute resolution.[1426]

Among the criticisms raised against e-disclosure there are, among other things: the cost of such process owing to the fees of experienced service providers used and experienced lawyers; the fact that there is no guarantee that the process will reveal key information; and the possibility for a litigant to hide important information in a mass of information making any effective search either too difficult or too expensive.[1427] With a good understanding of the functioning of a software tool such EDRM used in electronic discovery, one can now discuss rules and practice directions relevant for the discovery of ESI. This exercise is undertaken below under point C.

C. Rules and Practice Directions

Part 31 of the Civil Procedure Rules governs discovery in general, including electronic discovery. This Part is, however, supplemented by Practice Direction 31A & B, with the later dealing specifically with the disclosure of electronic documents. These three sets of rules are

[1426] Jackson's *Interim Report* Vol 2 379
[1427] Jackson's *Interim Report* Vol 2 379

discussed successively below from 1-3. The last point under this point C, that is, point 4, deals with the *Digicel* case.

1. Part 31

A certain number of provisions of Part 31 deserve attention because of their impact on electronic disclosure. These include Rule 31.5(3)(c) which requires that the report which must be filed and served before the first case management conference should, in the case of electronic documents, describe how such electronic documents are stored. In addition, it is important to highlight Rule 31.6 and Rule 31.7. The former deals with standard disclosure and the types of documents required to be disclosed under such a category.[1428] The last-mentioned rule is closely related to the first one and provides for the duty of search that is applicable when conducting a standard disclosure. That duty implies that the party concerned should make a reasonable search.[1429] These two principles are even more important in case of electronic disclosure as the potential amount of discoverable ESI is quite huge and can lead to exorbitant costs, which ultimately may prevent access to justice. They are further addressed under Practice Direction 31A and 31B below, as well as in the *Digicel* case also discussed below.

2. Practice Direction 31A

Under Practice Direction 31A two paragraphs can be highlighted as far as electronic disclosure is concerned, paragraph 2A.1 and paragraph 2A.2. The former clarifies the definition of document under Rule 31.4 of the Civil Procedure Rules by stressing that this definition is broad and extends to electronic documents. It, thus, covers: electronic communication, by e-mail or other; word processed documents and databases; documents readily accessible from computer systems; and other electronic devices and media. It also includes documents stored on servers and back-up

[1428] Three types of documents are required to be disclosed under standard disclosure:
a) Documents on which a party relies;
b) Documents affecting his or another party's case or supporting another party's case; and
c) Documents required to be disclosed under a relevant practice direction.

[1429] The reasonableness of a search is decided according to four factors, including
a) The number of documents involved;
b) The nature and complexity of the proceedings;
c) The ease and expense of retrieval of any particular document; and
d) The significance of any document which is likely to be located during the search.

systems and "deleted" electronic documents. Also falling under the definition of 'document' is metadata or information stored or associated with electronic documents.

Paragraph 2A.2 refers to Practice Direction 31B and its additional provisions on electronic disclosure discussed below.

3. Practice Direction 31B

This Practice Direction constitutes the central document governing electronic disclosure in England. Its purpose is to help parties to agree on a proportionate and cost-effective e-disclosure process.[1430] To achieve this, it provides for five general principles that the parties must take into account when dealing with e-disclosure. These include:

1. The necessity to manage electronic documents efficiently in order to minimise costs;
2. The use of technology to ensure an efficient and effective document management process;
3. The necessity to give disclosure in a manner which satisfies the overriding objective;
4. In case of inspection, documents must be made available in a form that puts the receiving party on a par with the originator in terms of capacities to access, search, review and display; and
5. The excessive burden on time and cost the receiving party may incur because of disclosure of irrelevant electronic documents.[1431]

In addition, when litigation is contemplated, parties have an obligation to preserve disclosable documents, including electronic documents that are supposed to be deleted in accordance with a document retention policy or in the normal course of business.[1432]

An important emphasis is put by PD 31B on the interaction between parties in the management of the e-disclosure process. Parties are, thus, required to discuss as early as possible important issues pertaining to e-disclosure, such as the use of technology in the management of electronic documents and the conduct of proceedings, for example: to create lists of documents to be disclosed; to give disclosure by means of documents in electronic format; or to present

1430 Par 2 of PD 31B
1431 Par 6 of PD 31B
1432 Par 7 of PD 31B

documents or other materials to court during trials.[1433] The discussions preceding the case management conference must extend to the disclosure of electronic documents *per se*, and address the related matters, such as the types of electronic documents under the control of the parties and places where they are held (computer systems, electronic devices and media), storage systems and document retention policies.[1434]

It has been pointed out above that, when giving standard disclosure, a party must make a reasonable search. Recognising that such search can be burdensome and costly in the case of the discovery of electronic documents, Par 9(2) of PD 31B requires parties to discuss as early as possible the scope of a reasonable search for electronic documents. Factors relevant in deciding the reasonableness of a search have been mentioned above,[1435] and it serves no purpose to repeat them here, except to stress that the factor relating to the ease and expense of retrieval of a document is very important for electronic documents. The assessment of this factor in the case of electronic documents will review the following six points:

1. The accessibility of the electronic documents on computer systems, servers, back-up systems and other relevant electronic devices and media considering changes in hardware or software systems necessary to access such documents;
2. The location of the electronic documents, data, computer systems, servers, back-up systems and other electronic devices or media containing the documents;
3. The probability of locating relevant data;
4. The cost of recovering electronic documents;
5. The cost of disclosure or provision for inspection of electronic documents; and
6. The likelihood of materially altering electronic documents during recovery, disclosure or inspection.[1436]

In addition, it is important to highlight an additional factor to ascertain the reasonableness of a search specific to electronic documents and this is the availability of documents or contents of documents from other sources.[1437] In other words, if an electronic document or its content is

[1433] Par 8 of PD 31B
[1434] Par 9(1) of PD 31B
[1435] Fn 1429 above
[1436] Par 21(3) of PD 31B
[1437] Par 21(4) of PD 31B

available from another source, it would be unreasonable to request a search from a source that will be more burdensome and costly.

Apart from the scope of reasonable search, parties must also discuss the use of tools and techniques, if applicable, in the control of the burden and cost of e-discovery.[1438] Tools and techniques to be considered include Keyword Searches, software tools, Data Sampling, methods to identify duplicate or privileged documents, and the use of a staged approach to e-discovery or a limitative approach in terms of which discovery will be limited to certain categories of documents selected by date, custodian or type.[1439] Some of these tools and techniques are self-explanatory, while others require a bit of explanation such as Data Sampling or Keyword Search. Data Sampling is "the process of checking data by identifying and checking representative individual documents."[1440] Keyword Search is "a software-aided search for words across the text of an Electronic Document."[1441] This may be used if a full review of each and every electronic document would be unreasonable. Keyword Search or other automated methods of search cannot, however, be used in isolation as they may either fail to identify important documents that need to be disclosed or pick a massive amount of irrelevant documents whose disclosure will negatively affect the receiving party because of the time and cost necessary to process such irrelevant information.[1442] Parties must, therefore, consider associating Keyword Search or other automated methods with additional techniques, such as the manual review of certain documents or any other steps that may justify the selection.[1443]

Parties must not forget in their discussions to deal with the following additional questions:[1444]

1. How to preserve electronic documents and prevent their loss before the trial?
2. What electronic format to use in the exchange of electronic documents?
3. In what formats and using what methods must electronic documents be provided for inspection?

1438 Par 9(3) of PD 31B
1439 Par 9(3) of PD 31B
1440 Par 5(1) of PD 31B
1441 Par 5(6) of PD 31B
1442 Par 26 of PD 31B
1443 Par 27 of PD 31B
1444 Par 9(4)-(8) of PD 31B

4. What basis should be used for charging or sharing the costs for the provision of electronic documents? And are arrangements about such costs final or reviewable by an order for costs subsequently made?
5. Would it be appropriate to use the services of a neutral electronic repository to store electronic documents?

Finally, parties may exchange information by means of an Electronic Documents Questionnaire, particularly information relating to the scope, extent and most appropriate format for the disclosure of electronic documents in the proceedings.[1445]

PD 31B contains a certain number of other important provisions, for example those applicable in case there is no agreement or court order regarding the provision of electronic copies of disclosed documents. In such an instance it is required that such copies be provided in native format, that is, in the original form in which they were created by a computer software programme, so that metadata relating to the date of creation is preserved.[1446] Another provision in PD 31B worth mentioning is the provision dealing with the use of specialised technology. According to this provision, if access to certain electronic documents is best accomplished by technology not easily available to the recipient of the disclosure, the disclosing party shall make available specialised technology to facilitate inspection.[1447]

After reviewing the rules and practice directions pertaining to the disclosure of electronic documents, it will be interesting to see how these principles have been applied in practice. The *Digicel* case provides insight to that issue.

4. The Digicel case

This case concerns an application by the claimants for an order for specific disclosure of certain classes of documents, including electronic documents. In respect of the latter, the claimants sought an order compelling the defendants to restore relevant back-up tapes to allow the searching of the e-mail accounts of certain former employees. In addition, the claimants

1445 Par 10 of PD 31B
1446 Par 33 of PD 31B
1447 Par 36 of PD 31B

requested an order for a new keyword search to be conducted by the defendants on all electronic documents, including those resulting from the restoration of back-up tapes.

a. Overview of e-disclosure in practice

Before dealing with the application of disclosure rules and directions in this case, it appears relevant to give an overview of e-disclosure in practice by reviewing the steps taken by the defendants in this case. The first step was to carry out a search on electronic documents. Such a search, including a keyword search, revealed a total of 1140000 documents which were transmitted to the defendants' lawyers in the form of DVDs or CDs and on hard drive. Most of these documents were electronic documents, including e-mails, retrieved from current servers, PCs and laptops. No electronic documents were, thus, extracted from back-up tapes. Documents transmitted to lawyers were either split into sub-folders or not. In the last case they were sent directly to an information management and litigation support solutions provider known as LDM Global to be placed on a database, while sub-folder documents were further subjected to a manual review to remove irrelevant documents before being sent to LDM Global. In total, all the documents that were sent to LDM Global to be placed on the database amounted to 625000 documents. The creation of such database involved the extraction of metadata to make electronic de-duplication possible. De-duplication of the documents was performed; in other words duplicates were removed. This step was followed by both the conversion of the remaining documents into an image format, allowing for their review and redaction on screen, and the creation of an optical character file for each document, thus providing a readable image.[1448]

After the defendants' positive search terms review, the 625000 documents on the database were reduced to 370000 documents that were again subject to de-duplication to reduce them further to 197000 documents. This last class of documents was resent to the defendants' lawyers and placed on their database for a manual review for relevance. At the end of the day, 5212 documents were disclosed, which amounted to 28983 pages and could fill 83 lever arch files.

[1448] *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch),[2009] 2 All ER 1094 at par 23 & 24

The whole process cost the defendants around £2 million in fees and £175.000 in disbursement. In addition, it took around 6700 man hours of lawyers' time.[1449]

This process gives a good illustration of how cumbersome and costly e-disclosure can be. This is why it is important for the process to be well managed in compliance with appropriately designed principles. How did the court apply these principles in this case?

b. Application of disclosure principles by the Court

The relevant principles applicable in this case were discussed above when dealing with Part 31 of the CPR and its two Practice Directions 31A and 31B. They included principles relating to the definition of document, to standard and specific disclosure, duty of search including the notion of reasonable search, cooperation between parties in handling e-disclosure. It is important to see how they are applied in this case.

As noted above, the claimants in this case were seeking for an order for specific disclosure. This is because in their opinion standard disclosure, in accordance with the first order to disclose, was not performed satisfactorily. One needs, thus, to review the requirements for standard disclosure. The documents that need to be disclosed by way of standard disclosure are described above.[1450] In addition, there is a duty of search required from the party who must disclose, a duty entailing the party to make a reasonable search of documents to be disclosed under standard disclosure. With that in mind, was the search by the defendants as described above reasonable? Views differ on this point, as the defendants claim that the search was reasonable under the circumstances. They submit that it would be very difficult to restore back-up tapes, the cost of the process would be high and disproportionate, and the process was likely to reveal few relevant documents. The claimants, however, argued that the search had not been reasonable as it had not extended to back-up tapes and had not used enough keywords.[1451]

The court started its discussion by pointing out the provisions in Practice Direction 31 (before its split in PD 31A and PD 31B) relating to the advice that was provided to parties to discuss issues

---

1449 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch),[2009] 2 All ER 1094 at par 25

1450 See fn 1428 above

1451 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 45

that might arise in respect of searches for electronic documents at an early stage.[1452] It must be stressed that this was the position at the time of the hearing of the application. Since then there was a change in the nature of the discussion between parties, and it then became an obligation and no longer an option. The message conveyed by the Court by raising this point is that, had such early discussions taken place, parties could have avoided unilateral decisions by the defendants' lawyers and their consequences in the form of the application. On the allegations of the parties regarding the reasonableness or not of the search, the Court held that:

> The Defendants have not carried out a reasonable search in all the circumstances of this case insofar as they omitted to search for, and in, the e-mail accounts of the 7 specified individuals, to the extent that those e-mail accounts may exist in the back-up tapes which have survived.[1453]

The court, therefore, ordered the restoration of back-up tapes in order to identify and enable the search of e-mail accounts of the 7 individuals. For that purpose, the parties' lawyers were directed to discuss how this could be achieved.[1454] In addition the court ordered that the e-mail accounts to be restored as part of this process be subject to a keyword search comprising the original words selected by the defendants as well as the additional words identified by the court.[1455] Regarding the e-mail accounts searched as part of the initial process, the Court ordered that they be subject to a new search using the additional key words.[1456]

As illustrated by this case, discovery of electronic documents must be approached carefully as failure to do so can give rise to disputes. Cooperation is a key ingredient to avoid not only disputes of fact but also of law. As noted by the court with reference to an American case, it is not appropriate to equate traditional paper-based discovery with the discovery of e-mail files because of the "sheer volume of electronic information", the lack of any coherent filing system for archived e-mails, and the use by data archival systems of obsolete magnetic tapes causing

---

1452 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 47

1453 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 67

1454 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 70

1455 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 92

1456 *Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 95

huge costs to translate the data into useable form.[1457] This point needs to be highlighted again in the discussion of discovery in South Africa. But before dealing with this jurisdiction, a review of Singapore is appropriate.

5.3.2.3 Singapore

As was the case in England, Singapore also felt the need to reflect on the subject of discovery. A consultation paper, called Review of Discovery in Civil Litigation, was thus issued to explore ways to revise and update the law as it existed at the time and the practice and management of discovery. Electronic discovery was also addressed in the consultation paper. This paper is briefly discussed below before the current law, that is Order 24 of the Rules of Court and Part V of the ePractice Directions, are dealt with.

5.3.2.3.1 Consultation Paper

In respect of electronic discovery, the Paper considered the regime in existence at the time in Singapore and how it could be improved. The regime was established by Practice Direction No 3 of 2009 (PD 3) which provided for an opt-in framework. In other words, parties could request or apply for the application of such electronic regime when dealing with discovery and inspection of ESI as well as the supply of electronic copies of such ESI.[1458] The Paper unsuccessfully recommended that an electronic discovery plan be mandatory where most documents have been created or stored electronically, and where the use of technology would make the resolution of the matter speedy, inexpensive and efficient.[1459] In addition, to deal with potential wastage of time and cost the Paper suggested a compulsory regime for the meetings and discussions between parties on discovery matters.[1460] As will be seen below in the discussion of the ePractice Directions, this recommendation was not retained either.

The Consultation Paper also discussed the relevance of the traditional discovery process in the digital age, asking whether it was still relevant to start by enumerating the documents on a list of

1457 *Byers v Illinois State Police* 53 Fed R Serve 3d 740 (N D Ill May 31, 2002) cited by *Digicel* (*St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors* [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094 at par 41

1458 43A(1) of PD 3

1459 *Review of Discovery in Civil Litigation Consultation Paper* 2009 (hereafter referred to as *Singapore Discovery Consultation Paper*) 8-9

1460 *Singapore Discovery Consultation Paper* 13

documents, proceed with inspection and the taking of copies. It argues that such an approach may no longer be efficient, especially in cases involving voluminous documents. Hence it was seen to be important to focus on what lawyers really want, that is, copies of the documents. A good approach, therefore, would, according to the Paper, be to provide soft copies of discoverable electronic documents in native format and defer inspection which should be undertaken discretionarily and be ordered only when necessary.[1461] This is a sound approach as it contributes to a more expeditious, efficient and inexpensive e-litigation process. In addition, it was suggested that the court be given the power to adopt a new approach when discovery is done by means of a direct exchange of discoverable documents.[1462]

The Consultation Paper also deals with discovery in selected jurisdictions, including England. It addresses most of the issues discussed above under the English jurisdiction.

5.3.2.3.2 Order 24

Order 24 of the Rules of Court governs the discovery and inspection of documents. It has a general application and includes general provisions found in any text of a similar nature, such as Part 31 of the Rules of Court in England discussed above. Such provisions include: the order to give discovery by making and serving a list of documents to the other party; the types of documents concerned by discovery; the principle for discovery to be ordered only if it is necessary to dispose fairly of a cause or a matter or to save cost; and the right to inspect documents referred to in the list and take copies. All these principles have been discussed above so it serves no purpose to repeat them here. It should be highlighted, however, that, in contrast to Part 31, Order 24 contains no specific provisions relating to electronic discovery which is specifically regulated by Part V of the ePractice Directions discussed below.

5.3.2.3.3 Part V of the ePractice Directions

A. Introduction

Before dealing with Part V of the ePractice Directions, it seems appropriate to give a general introduction to the ePractice Directions. This is another example that shows that Singapore is

1461 *Singapore Discovery Consultation Paper* 30
1462 *Singapore Discovery Consultation Paper* 30

still leading the way as far as the integration of technology in the justice system is concerned. Indeed, since its launch in 2010, the ePractice Directions or the online version of the Practice Directions is deemed to be the authoritative version with all amendments made directly online in real time. The revised version has been in operation since 1 January 2013 and consolidates all previous practice directions of the Supreme Court, including Part V dealing with the discovery and inspection of electronically stored documents.

B. Discovery and inspection of electronically stored documents

Part V of the ePractice Directions provides a "framework for proportionate and economical discovery, inspection and supply of electronic copies of electronically stored documents."[1463] From the above, an important principle as far as e-discovery is concerned can be highlighted, namely the necessity for a proportionate and economical e-discovery process. This is an important principle already encountered as it ensures that the workload and cost relating to e-discovery is maintained under reasonable limits. It is in harmony with rules 7 and 13 of Order 24, as reiterated by paragraph 48 of ePractice Directions, in terms of which "an order for discovery and production of documents for inspection shall not be made unless such an order is necessary either for disposing fairly of the cause or matter or for saving costs." To assess whether e-discovery is proportionate and economical, one needs to look at the following six factors:

(1) the number of electronic documents involved;
(2) the nature of the case and complexity of the issues;
(3) the value of the claim and the financial position of each party;
(4) the ease and expense of the retrieval of any particular electronically stored document or class of electronically stored documents;
(5) the availability of electronically stored documents or class of electronically stored documents sought from other sources; and
(6) the relevance and materiality of any particular electronically stored document or class of electronically stored documents which are likely to be located to the issues in dispute.[1464]

1463 Par 44(1) of the ePractice Directions
1464 Par 48 of the ePractice Directions

All these factors are the same as those used in England to determine the reasonableness of an e-disclosure search, save for the value of the claim and the financial position of each party.[1465] Similarly the ease and expense of retrieval of electronic documents in factor 4 is determined by using the same criteria as those adopted in England,[1466] albeit in a simplified form. These criteria are as follows:

(i) the accessibility, location and likelihood of locating any relevant documents;

(ii) the costs of recovering and giving discovery and inspection, including the supply of copies, of any relevant documents; and

(iii) the likelihood that any relevant documents will be materially altered in the course of recovery, or the giving of discovery or inspection.[1467]

Part V, which contains 15 paragraphs, is applicable either on the initiative of the parties or of the court. It must be stressed, however, that parties are encouraged to consider its application in the following cases:

(a) where the claim or the counterclaim exceeds $ 1 million;

(b) where documents discoverable by a party exceed 2,000 pages in aggregate; or

(c) where documents discoverable in the case or matter comprise substantially of electronic mail and/or electronic documents.[1468]

This mere encouragement is contrary to the recommendation of the Consultation Paper which favours a mandatory application of Part V in the case of the three above-mentioned scenarios.[1469] This would have been in line with the situation in England, as discussed in the *Digicel* case. England moved from encouraging parties to meet and discuss issues related to e-discovery to compelling them to do so. If one looks at the consequences of not having done so in the *Digicel* case, it must be right to say that a mandatory regime should be the best way to go about it.[1470] Singapore, unfortunately, does not agree. At least it is good that the court has the power to order the application of the framework on its own motion. On a similar note, parties are invited to good faith collaboration when discussing issues relating to the discovery and inspection of ESI,

[1465] Ch 5 par 5.3.2.2.1 C 3
[1466] Ch 5 par 5.3.2.2.1 C 3
[1467] Par 48(d) of the ePractice Directions
[1468] Par 44(2) of the ePractice Directions
[1469] *Singapore Discovery Consultation Paper* 8
[1470] Ch 5 par 5.3.2.2.1 C 4

including: the scope of discoverable documents; voluntary disclosures, preservation of documents; use of search terms, preliminary searches or data sampling, staged e-discovery process; and the format and manner of supplying copies of discoverable documents.[1471] Parties are also referred to the check list of issues for good faith collaboration.[1472] The discussions between parties will result in the adoption of the electronic discovery plan which will be presented to the court for approval.[1473] If they are unable to agree on such plan, the interested party may apply to the court for an order. To that effect he must submit a draft electronic discovery plan supported by an affidavit detailing the unsuccessful efforts made in good faith to agree on an electronic discovery plan.[1474]

The electronic discovery plan deals with a certain number of issues as pointed out above, among which there is the scope of discoverable documents. It is interesting to have a closer look to a special category of electronic information, namely metadata, and see how it is discoverable. Metadata refers to non-visible information embedded in or associated with ESI created by a software application (application metadata) or by the operating or storage system (system metadata). It is stored either internally within the ESI or externally in a separate file or database.[1475] It is the place of storage that will determine how metadata is discovered. Metadata internally stored is discoverable as part of the ESI in which it is embedded, while externally stored metadata is discoverable as separate information from the ESI with which it is associated. The latter shall be discoverable only upon the specific request for discovery of such information. Otherwise, only internally stored metadata shall be discovered.[1476]

The scope of discoverable documents is closely related to the scope of the search that must be conducted to reveal such documents. Such search must be reasonable. It is conducted using search terms or phrases and limits on the scope of the search, such as limits in relation to the custodians or repositories of information or limits in relation to the period of creation, reception and modification of ESI.[1477] A reasonable search shall extend to ESI not reasonably accessible

1471 Par 45(1) of the ePractice Directions
1472 Appendix E Part 1 of the ePractice Directions
1473 Par 45(2) of the ePractice Directions
1474 Par 45(3) of the ePractice Directions
1475 Par 44(5) of the ePractice Directions
1476 Par 46(1) of the ePractice Directions
1477 Par 47(1) of the ePractice Directions

(for example deleted documents or documents archived using backup software) only if certain conditions are met. The principle of proportionality and economy in terms of paragraph 48 of the ePractice Directions must be adhered to, on the one hand, and the requesting party must demonstrate that the relevance and materiality of such ESI outweighs the cost and burden of retrieving and producing it, on the other hand.[1478] It can be concluded from this paragraph that reasonable search is carried out using the same principles in Singapore as in England.[1479] The result of the search, however, is disclosed to the requesting party without any review for relevance in the former jurisdiction contrary to the latter jurisdiction as was pointed out in the *Digicel* case.[1480]

The communication of the result of the search to the requesting party is also described in Part V of the ePractice Directions. It is stated under that Part that copies of ESI shall generally be supplied in native format, that is, in this context, the format in which the electronic document is ordinary stored and in one or more read-only optical disc(s).[1481] This will include internally stored metadata unless parties agree or the court orders otherwise, that is, for the deletion, removal or alteration of metadata because of privilege concerns. In such a case, documents must be supplied in a reasonable usable format after the removal of metadata protected by privilege.[1482]

After the supplying of the copies, the beneficiary party may request an inspection of ESI in accordance with Order 24 of the Rules of Court. The requested party is expected to provide reasonable means and assistance for such an inspection of ESI in its native format.[1483] The inspection can extend to computer databases, and such inspection shall be carried out in accordance with an inspection protocol adopted by the parties.[1484] In addition, parties are entitled to conduct a forensic inspection of electronic media or recording devices. This will be subject to

1478 Par 47(2) of the ePractice Directions
1479 Ch 5 par 5.3.2.2.1 C 3
1480 Par 47(3) of the ePractice Directions; Ch 5 par 5.3.2.2.1 C 4
1481 Par 52(1) of the ePractice Directions
1482 Par 52(2) of the ePractice Directions
1483 Par 50(1) of the ePractice Directions
1484 Par 50(3) of the ePractice Directions

certain conditions, namely that the electronic medium or recording device must have been discovered, and there must be an inspection protocol.[1485]

It must be asked whether the inspection of ESI is still relevant in the digital age, given the fact that electronic copies that are supplied are exactly the same as the original information stored in the computer, systems, servers, backup tapes, etc. from where they originate. It is, thus, welcome that a provision in the ePractice Directions has considered this possibility and allows for discovery to be done by the supply of copies *in lieu* of inspection if the management of documents and conduct of proceeding using technology can make the cause or matter to be disposed of justly, expeditiously and economically.[1486]

The topic of e-discovery has been discussed successively in England and Singapore. It can be highlighted from the discussion that both jurisdictions have followed a similar approach. While acknowledging that the general principles governing traditional discovery should apply to e-discovery, they also recognize the need for a specific regime for the latter to cater for the specificities of ESI and the need to control the burden and cost of retrieving ESI and producing it. With this as background, it is interesting to examine the situation in the South African jurisdiction.

5.3.2.4 South Africa

In South Africa, discovery is governed by Rule 35 of the Uniform Rules of Court and rule 23 of the Magistrates' courts rules. These two rules are examined below with reference to e-discovery.

5.3.2.4.1 Rule 35 of the Uniform Rules of Court

Rule 35 deals with the discovery, inspection and production of documents. It contains up to 15 subrules, of which the most relevant to the issues under examination is arguably subrule (1) that reads as follows:

> Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within twenty days of all documents and tape recordings relating to any matter in question in such action (whether such matter is one arising between the party requiring

[1485] Par 51(1)&(2) of the ePractice Directions
[1486] Par 53(1) of the ePractice Directions

> discovery and the party required to make discovery or not) which are or have at any time been in the possession or control of such other party. Such notice shall not, save with the leave of a judge, be given before the close of pleadings.

For the purpose of this discussion, two important terms or phrases can be highlighted from this provision, "discovery" and "documents and tape recordings". The first term is crucial as it constitutes the subject matter of this discussion, and the second group of terms or phrase is important insofar as it delineates the scope of the first term. This subrule constitutes the basis upon which discovery is requested and made, and it, therefore, requires special attention.

Discovery, as previously mentioned, allows each party to an action to have knowledge of information in the possession or control of the opposing party that might be relevant to the action. In High Court proceedings, parties will rely on Rule 35(1) to request such information. Information here refers to documents and tape recordings. It is, thus, logical to analyse the true meaning of "documents" and "tape recordings" to ascertain whether it can be extended to ESI and if it can be done satisfactorily.

A. Documents

In contrast to the situation in England, the word 'document' is not defined in the South African Uniform Rules of Court. This implies that one needs to look for a definition elsewhere. In chapter 2 of this thesis, different definitions of document (drawn from various sources) were provided. They include those provided by the Civil Proceedings Evidence Act, in terms of which a document includes any book, map, drawing or photograph, and by the Criminal Procedure Act, under which a document includes "any device by means of which information is stored or recorded". In addition, a common law definition is found in *R v Daye*,[1487] where "document" is defined as "any written thing capable of being evidence" regardless of the material on which it was written.[1488] The first two definitions appear not to be able to accommodate ESI as they seem to focus more on a tangible medium, while the last one is formulated so widely that it might include ESI. Having said that, it will be not incorrect to argue that the use of "include" in the first two definitions suggests that the meaning of document is not restricted to the enumeration

[1487] 1908 2 KB 330 at 340

[1488] Ch 2 par 2.2.4.3

provided, but may be understood to extend to the ordinary meaning of the word.[1489] This approach was considered in *Le Roux and Others v Viana NO and Others*.[1490] In that case, one of the issues was whether certain electronic documents recorded on a hard drive could qualify as documents in terms of section 69 of the Insolvency Act 24 of 1936 and, therefore, be susceptible to seizure under that section.[1491] The court found no difficulty in answering in the affirmative by relying on the ordinary meaning of the term document as provided by the *Concise Oxford English Dictionary* (10th edition revised) that defines a document as "a piece of written, printed or electronic matter that provides information or evidence or that serves as an official record".[1492]

The lesson that can be drawn from this case is that the decision made by the court regarding the definition of document is context based. This means that, with a different set of facts or a different statute the conclusion might be different. Thus, given the fact that "document" under Rule 35(1) will be used in disputes relating to different statutes providing different meanings to the word document, it will be appropriate for the Uniform Rules of Court to insert a uniform definition of "document" that can be used for discovery in any circumstance, especially for ESI and, thus, remove any uncertainty. A good model to consider is the approach followed by England, which was to provide a general definition of document, specify that it extends to electronic documents, and give a few examples,[1493] unless it is submitted that "document" under Rule 35(1) does not contemplate electronic documents, which should instead fall under tape recordings. This eventuality is discussed below.

1489 The meaning of "includes" in a statute was considered in *De Reuck v Director of Public Prosecutions* 2004 (1) SA 406 (CC). It was held that the correct sense must be ascertained from the context in which used. If the primary meaning of the term was well known and not in need of definition and the items in the list introduced by "includes" went beyond the primary meaning, the purpose of that list was then usually taken to be to add to the primary meaning so that "includes" was not exhaustive.

1490 2008 (2) SA 173 (SCA)

1491 *Roux and Others v Viana NO and Others* 2008 (2) SA 173 (SCA) at par 6

1492 *Le Roux and Others v Viana NO and Others* 2008 (2) SA 173 (SCA) at par 10

1493 Rule 31.4 of the Civil Procedure Rules read with Par 1 & 5(3) of PD 31B

B. Tape recordings

Unlike the word document, tape recording is defined in the Uniform Rules of Court as including "a sound track, film, magnetic tape, record or any other material on which visual images, sound or other information can be recorded."[1494]

The obvious question to ask is whether ESI falls under that definition. From the onset it is right to say that media susceptible to containing ESI such as compact disks, computer disks, and hard drives clearly fall within the meaning of tape recording.[1495] This view is supported by the authors of *Erasmus: Superior Court Practice* as reported by van Dorsten. They correctly submit that the definition of tape recording is wide enough to include any medium on which visual images, sound and other information can be recorded. They are further correct in stressing that the emphasis on the definition is put on the medium on which the information is recorded which is discoverable and not the information itself.[1496] In this regard, van Dorsten reports that, in the unreported case of *Metropolitan Health Corporate (Pty) Ltd v Neil Harvey and Associates (Pty) Ltd and Another (WCC),*[1497] backup tapes of a company's electronic information were found to be discoverable.[1498]

To respond to the question regarding ESI, based on the above it is totally logical to affirm that ESI in itself does not fall within the meaning of tape recording as contemplated here. To illustrate this one may take the example of an e-mail. An e-mail can be stored on various media, such as a computer, a flash drive, a server, a backup tape, and so on, but such medium is separate from the email itself which has a distinct existence. A request for discovery of tape recordings under Rule 35(1) will, therefore, include all the above-mentioned media and not necessarily the email which will, at the end of the day, defeat the whole purpose of discovery. Technology has changed, and a definition that focused too much on the material on which information could be recorded, as initially information and medium were intermingled, can no longer be satisfactory in an era where information has an identity separate from the medium. Such information can be

1494 Rule 35(15) of the Uniform Rules of Court
1495 Peté *et al Civil Procedure, a Practical Guide* 2 228
1496 Farlam & van Loggerenberg *Erasmus: Superior Court Practice* 2011 at B1 – 262B) as cited by van Dorsten "Discovery of electronic documents and attorneys' obligations" Nov 2012 *De Rebus* 36
1497 (unreported case no 10264/10, 19-82011) (Baartman J)
1498 Van Dorsten "Discovery of electronic documents and attorneys' obligations" 36

everywhere and nowhere, even in the cloud. The current definition of tape recording, therefore, cannot be extended satisfactorily to information created, stored and retrieved in electronic form and should be applied only to its primary objective of a material on which information is permanently recorded. Having reached such conclusion, the only avenue left for the discovery of ESI is under document with all the shortfalls identified above. Although the courts have inherent powers to ensure proper discovery in spite of unclear or inadequate discovery rules, it remains imperative to accord due attention to the issue of the discovery of ESI. Even if ESI could fall under the extended definition of document, there are still many other issues that will need to be considered by courts to be able to give proper guidance with regard to the handling of discovery of ESI. The best way to deal with such situation is to follow the examples of both Singapore and England by amending the rules of court accordingly or adopting the necessary practice directives.

Infology, a respondent to the SALRC Discussion Paper 131 on the review of the law, made the following suggestion for the amendment of Rule 35(1) of the Uniform Rules of Court and its equivalent in Magistrates'courts rules, that is to replace the current wording with "*documents and tape recordings including electronically stored information and related metadata"*.[1499]

The submission of Infology is clearly an attempt in the right direction; it does, however, create a bit of confusion as it is not clear whether "electronically stored information and related metadata" is included in tape recordings, documents, or both. If it is included in tape recordings then it should be listed in the definition of tape recording instead under Rule 35(15) of the Uniform Rules of Court; if it falls under documents, than it must follow directly after "documents". It is not possible that it can fall under both as the wording clearly suggests that "documents" and "tape recordings" are distinct concepts, firstly, because of the use of the word "and" between "documents" and "tape recordings" and not "including", and, secondly, because "tape recording" has been defined as a separate concept in the rules. Based on the above, the right approach would be to leave Rule 35(1) as it is and insert a definition of "document" in the rules that will extend to electronically stored information and related metadata.

[1499] SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 2015 (hereafter referred to as SALRC *Discussion Paper 131 on the review of the law of evidence*) 81

Another suggestion by Infology is to amend Rule 35(2)(a) of the Uniform Rules of Court which deals with the documents that must be included on the affidavit when making discovery. It suggests the following addition to Rule 35(2)(a): "…*and the manner in which such documents and tape recordings are retained including, in the case of electronically stored information, the electronic file formats in which they are retained*".[1500] With regard to ESI, the addition is pertinent as it is important to the party requesting discovery to know the manner in which ESI is retained as well as its electronic file format. Since such information is important for ESI only, one might question whether this addition is well formulated. A better formulation would probably be to restrict the addition to ESI so that it would read as follows: …*and in case of electronically stored information, indicate the manner in which it is retained as well as its electronic file format*". Having said that, a holistic approach should be preferred as it would have the advantage of dealing with all issues identified as peculiar to the discovery of electronically stored information. This can be done by adding a rule such as Rule 35A, entitled electronic discovery or by adopting practice directives focusing exclusively on e-discovery. Such an approach could, without any difficulty, accommodate the last suggestion of Infology relating to inspection. Infology submits to amend Rule 35(6) of the Rules of Court so that a party may require any party who has made discovery to make available for inspection "*in a format reasonably specified by such party or, if not so specified, in a form in which they are ordinarily retained or another reasonable usable form"* any documents or tape recordings…[1501]

The proposals by Infology, as well as any other important issues relating to discovery of ESI that need to be considered in the reform of the rules of court in South Africa, are further discussed below.[1502]

5.3.2.4.2 Rule 23 of the Magistrates' court rules

Rule 23 deals with the discovery of documents in Magistrates' courts, with subrule (1)(a) reading as follows:

> Any party to any action may require any other party thereto, by notice in writing, to make discovery on oath within 20 days of all documents and tape, electronic, digital or other forms of

[1500] SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 81
[1501] SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 81
[1502] Ch 5 par 5.3.2.4.3

> recordings relating to any matter in question in such action, whether such matter is one arising between the party requiring discovery and the party required to make discovery or not, which are or have at any time been in the possession or control of such other party.

Rule 23 in general was amended in 2010 to harmonise it with Rule 35, thus subrule 23(1)(a) is almost a replica of subrule 35(1), save for a few differences. As for cases in the High Court, discovery in Magistrates' courts will concern documents and tape recordings. In addition to that, however, discovery in Magistrates' courts will extend to electronic, digital and other forms of recordings. It will be interesting to analyse the second category, as documents and tape recordings have been discussed above.

A. Electronic and digital recordings

The first reaction prompted by the new rule 23(1)(a) is a very positive one considering all the reservations made previously with regard to "document" and "tape recording" and their shortcomings in dealing with ESI. This was the initial reaction by van Dorsten who submitted that this is a step in the right direction. The learned advocate, however, feels that the terms electronic or digital recordings do not adequately cover ESI.[1503] According to him, the term "recording" is limited in scope as illustrated by the definition he suggests of "recorded broadcast or performance" or "a disc or tape on which sounds or visual images have been recorded".[1504] Since this definition focuses primarily on the storage medium and not on the information itself, clearly it cannot adequately deal with the discovery of ESI, he contends.[1505] He, therefore, proposes the use of the term "stored" associated with information as this implies that the information is retained or entered for future electronic retrieval.[1506]

The argument developed by van Dorsten makes sense based on the definition of "recording" he provides. This definition, however, albeit correct, is narrow in scope as recording can be defined widely enough to include ESI. It can, for example, also be defined as the product of a process of

---

1503 Van Dorsten "Discovery of electronic documents and attorneys' obligations" 35

1504 (http://oxforddictionaries.com/definition/english/recording?q=recording, accessed 20-9-2012) as quoted by Van Dorsten "Discovery of electronic documents and attorneys' obligations" 35

1505 This reminds one of the arguments developed in the discussion of the definition of tape recording, Ch 5 par 5.3.2.4.1 B

1506 Van Dorsten "Discovery of electronic documents and attorneys' obligations" 35

"registering or preserving something by a machine, instrument or device."[1507] Defined that way it can have a corresponding meaning to "record". This view is even reinforced by the definition of "tape recording" which extends to a "record".[1508] The Electronic Transaction Act 2010 of Singapore defines record as, "information that is inscribed, stored or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[1509] In addition, electronic record is defined in the same Act as a "record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another".[1510] These two definitions from Singapore clearly show it is possible to interpret electronic and digital recordings widely enough to encompass ESI easily. To address the concerns of van Dorsten, a simple insertion in the Magistrates' court rules of a definition of electronic or digital recording copied on the model of Singapore should suffice, although it is not indispensable.

B. Other forms of recordings

This expression leaves an additional avenue for the discovery of ESI, although it can correctly be submitted that the terms "electronic" or "digital recordings" fulfil that purpose already. It will be interesting to see what items van Dorsten would include in the category of "other forms of recordings" in the light of the definition of recording he put forward above.

This concludes the discussion on the two rules governing electronic discovery in South Africa. Some inadequacies have been identified regarding certain definitions for instance. There are, however, many other issues pertaining to e-discovery that need to be discussed and their regime in South Africa to be determined. This is done below.

5.3.2.4.3 Specific matters pertaining to e-discovery not covered by Rules 23 & 35

As already noted when dealing with the matter in England and Singapore, electronic discovery raises a certain number of specific issues that require special treatment. The main reason is that

1507 *Oxford English Dictionary* available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/159883?rskey=iD1wne&result=1&isAdvanced=false#eid (accessed on 08/06/2015)

1508 Rule 23(16) of the Magistrates' Courts Rules

1509 S 2(1) of the Singapore Electronic Transactions Act 2010

1510 S 2(1) of the Singapore Electronic Transactions Act 2010

e-discovery deals with a type of information that distinguishes itself from traditional documents by its massive volume. While recognising the benefit that full discovery of such ESI may have in revealing the truth, one needs to remain mindful of the cost and burden involved in the process of retrieving, reviewing and disclosing ESI to avoid rendering justice unaffordable. This balance requires well thought and designed rules and directives taking into consideration the specific nature of ESI. These rules and directions must deal with, amongst other matters: the cooperation between the parties in the management of e-discovery to ensure a proportionate and cost-effective e-discovery process; the different types of ESI and their discovery mode, in particular metadata and not reasonably accessible documents; the storage of ESI; the preservation of ESI; the reasonable search of ESI; the format and the manner of supplying copies of discoverable ESI; and the inspection of ESI.

A. Cooperation between parties

It goes without saying that cooperation among parties is crucial in the management of e-discovery. Failure to engage in such practice may result in disastrous consequences as pointed out in the *Digicel* case above.[1511] Parties should, thus, be advised to discuss as early as possible issues of relevance to discovery of ESI and ideally agree on an electronic discovery plan. These discussions are mandatory in England. In South Africa there appears to be no specific provisions in the rules requiring or encouraging discussions between parties when dealing with discovery, save maybe for the opportunity provided under the pre-trial conference rule to parties to identify issues of disagreement, to try to find a common ground on these issues, and to decide on the best way to conduct the trial.[1512] The pre-trial conference, however, clearly takes place too late to permit appropriate discussions on the management of the e-discovery process. In most cases it happens only after discovery. It is, therefore, imperative that a reform of the discovery rules deals also with this aspect as has been the case in both England and Singapore.[1513]

1511 Ch 5 par 5.3.2.2.1 C 4

1512 Rule 37 of the Uniform Rules of Court; Peté *et al Civil Procedure, a Practical Guide* 250

1513 Ch 5 par 5.3.2.2.1 C 3 & 4; Ch 5 par 5.3.2.3.1 & 5.3.2.3.3 B

B. Proportionate and cost-effective e-discovery process

To guarantee a proportionate and cost-effective e-discovery process, there must be appropriate measures in place, including factors of assessment. These are currently lacking in South Africa. There is, therefore, a need to remedy this situation. The factors to consider include the number of electronic documents involved, the nature of the case and the complexity of the issues, and the ease and the cost of retrieving electronic documents, to name but a few.[1514]

C. Types of ESI and their discovery mode

For the purpose of discovery, a distinction can be made amongst three types of ESI, namely readily accessible documents, not reasonably accessible documents, and metadata. In the reform of the discovery regime in South Africa, provision must be made for these three categories and the mode of discovery for each. Both England and Singapore can serve as a model.[1515]

D. Storage and preservation of ESI

It is important to identify the places ESI can be stored to determine where research must be conducted. A possible way to do this is by including the storage places in the definition of the types of ESI under point C above. In addition, a provision regulating the preservation of ESI should be considered to avoid deleting important information once litigation is already contemplated because of internal document retention policy or ordinary business practice.[1516]

E. Reasonable search of ESI

The importance of a reasonable search when dealing with ESI cannot be overstressed as it contributes to a proportionate and cost-effective e-discovery process. South Africa must, therefore, define specific criteria to ascertain the reasonableness of a search. It can draw inspiration from England or Singapore.[1517]

1514 These factors and others are presented in the discussion of England and Singapore Ch 5 par 5.3.2.2.1 C 1 & Ch 5 par 5.3.2.3.3 B respectively

1515 Par 5 & 28 of PD 31B and par 44 & 46 of the ePractice Directions respectively

1516 Par 7 of PD 31B

1517 Par 20-22 of PD 31B and par 47 of the ePractice Directions respectively

F. Format and manner of supplying copies of discoverable ESI

The general trend is for copies of discoverable ESI to be supplied in native format. The manner of supply varies from using a read-only optical disc to the direct exchange of discoverable documents and other methods. This is an important aspect as far as discovery is concerned and deserves due attention. Guidance can be gained from both England and Singapore.[1518]

G. Inspection of ESI

There is a choice to be made by South Africa on the relevance of inspection of ESI in the digital age as electronic copies are identical to original electronic documents and inspection may simply become a redundant exercise. Singapore has adopted a very useful and interesting approach by providing for the possibility for discovery to be made by the supply of electronic copies of ESI *in lieu* of inspection.[1519] South Africa should follow suit.

In the light of the above, it is clear that the current regime governing discovery in South Africa is inappropriate for the discovery of electronic stored information and it, therefore, requires a reform. Such a reform should consider the issues raised above, including the definition of 'document' and the points A-G as well as the approach in England and Singapore. The recommendation by the SALRC for the Rules Board for Courts of Law to be assisted with a working group with technical expertise in this exercise is welcome.[1520]

This concludes the discussion on discovery, a pre-trial procedure whereby, upon request, a party discloses to the requesting party all documents in his possession that might be relevant to the trial and eventually gives access to them. With the advent of technology, the nature of information to be disclosed has changed as information is increasingly created, processed, stored and communicated electronically. In addition the amount of information required to be disclosed is higher. In light of the above the section was dedicated to analysing the discovery of ESI, also known as electronic discovery. It discussed the relevant rules governing this procedure in England, Singapore and South Africa.

1518 Par 33 of PD 31B and par 52 of the ePractice Directions respectively
1519 Par 53 of the ePractice Directions
1520 SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 82

In England before dealing with the legal aspect, namely the relevant rules, a description of e-discovery was provided as well an overview of the functioning of EDRM, a software tool used for the discovery of ESI.[1521] In respect of the legal aspect Part 31 of the Civil Procedure Rules was briefly discussed before dealing successively with PD 31A, PD 31B and the *Digicel* case. PD 31B is particularly interesting as it deals with all aspects specific to e-discovery and constitutes therefore a good source of information for South Africa. *Digicel* is also a good example of how e-discovery can get out of control if not well managed.[1522]

The second jurisdiction dealt with was Singapore. The regime applicable to electronic discovery consists of Order 24 of the Rules of Court and Part V of the ePractice Directions with the former governing discovery in general and the latter dealing specifically with the discovery and inspection of electronically stored documents. Singapore clearly follows a similar approach to England, that is, acknowledge that the general principles governing traditional discovery should apply to e-discovery, but also recognize the need for a specific regime for the latter to cater for the specificities of ESI and the need to control the burden and cost of retrieving ESI and producing it.[1523]

South Africa was the last jurisdiction discussed. As discovery is governed by Rule 35 of the Uniform Rules of Court and rule 23 of the Magistrates' courts rules, these two rules were examined with reference to e-discovery. It was submitted that the above rules are inadequate to deal effectively with e-discovery. To address these shortcomings reference should be made to England and Singapore and follow the approach taken there, that is, keep these rules with minor amendments in relation to definitions to govern discovery in general and introduce a rule dealing specifically with e-discovery.[1524] The discussion on discovery completes the pre-trial procedure. The next point below deals with the preparation of documents for use in court, this is the trial phase.

[1521] Ch 5 par 5.3.2.2.1
[1522] Ch 5 par 5.3.2.2.1
[1523] Ch 5 par 5.3.2.3.3
[1524] Ch 5 par 5.3.2.4

5.3.3 Preparation of documents for use in court

This paragraph gives an overview of certain rules in Singapore relevant to the preparation of documents for use in court in a paperless environment. It serves as information and is worth considering in the process of the adaptation of rules of court in South Africa to embrace the digital age. These rules concern mainly the electronic creation and filing of bundles of documents.

In terms of paragraph 69(1) of the ePractice Directions, as a general rule "all documents for use at any hearing in Court must be filed using the Electronic Filing Service at least 1 clear day in advance of the hearing."[1525] Parties may, however, choose not to file bundles of authorities and opt to use the paper form of these.[1526] But if they choose the electronic filing of bundles, the following directions apply:

(a) Index pages and create bookmarks in the PDF file of each reference in the index;
(b) The bookmark's name should correspond to the reference's name in the index;
(c) Arrange chronologically or in some logical order all PDF documents; and
(d) The page number of each bundle of documents must correspond to the page number of the PDF version of that bundle.[1527]

In addition, bundles of documents may be created online and filed through the Electronic Filing Service in proceedings, using such Electronic Filing Service. The PDF electronic bundle may contain:

(a) documents in the electronic case file; and
(b) documents that have been uploaded into the electronic case file by solicitors or other persons given access to the shared folder in the electronic case file.[1528]

This brief paragraph concludes the discussion on the rules of procedure and electronic justice.

1525 The documents affected by this paragraph are varied and include not only written submissions, skeletal arguments, opening statements but also different types of bundles (documents, pleadings, affidavits and core).

1526 Par 69(3) of the ePractice Directions

1527 Par 70(4) of the ePractice Directions

1528 Par 70(5) of the ePractice Directions

5.4 Conclusion

This chapter has discussed e-justice from a two-fold perspective, technical and legal. From a technical perspective, the chapter has provided an overview of technologies and applications used in the judicial system dividing these into three categories, namely: applications used to support court administrative staff and judges; applications allowing the exchange of information between courts, parties and the general public; and applications that facilitate the presentation of electronic evidence in court.[1529] All these applications have been discussed with reference to England, Singapore and South Africa.

The discussion on the first category included firstly a point on basic technologies used by both administrative staff and judges and consisting of Office applications before dealing with specific applications supporting each category. An overview of the selected jurisdictions showed that Office applications are available in all courts in England and Singapore. In South Africa, however, because of difficulty to get recent data, there is uncertainty regarding the current situation. Based on figures from 2002, the availability is limited.[1530]

In respect of applications specific to administrative staff the focus was on the computerised case management, an organisational tool used by administrative staff members in managing cases from the entry point to the end of the case. The situation in the three jurisdictions covered showed that England is not among the top 12 European countries with the most effective and complete level of computerisation of the management and administration of courts.[1531] In South Africa, it seems that case management systems are available only in certain courts in spite of the CPP project.[1532] The model in that regard remains Singapore which has developed a very effective computerised case management system known as the Civil System. There is almost no detail on a case that cannot be found on the Civil System. It allows the tracking of a case from its inception to its finalisation with mechanisms to detect any problem with such a case, including any form of inactivity or any breach by the parties of a court order.[1533]

1529 Ch 5 par 5.2.2
1530 Ch 5 par 5.2.2.1.1
1531 Ch 5 par 5.2.2.1.2 A
1532 Ch 5 par 5.2.2.1.2 C
1533 Ch 5 par 5.2.2.1.2 B

Regarding applications for supporting judges, the discussion dealt with individual tools designed to help judges in their daily activities and included office tools, legal research tools, and judgment and sentencing tools. In England a project known as JUDITH contributed to the use of computers by judges for their daily activities.[1534] In Singapore judges have been equipped with laptops since July 2001 and can access the Supreme Court's network from their homes via the Citrix server and prepare their hearings by reading electronic cases or carrying out the necessary legal research in that respect.[1535] In South Africa, the Digital Nervous System or DNS project, although not designed specifically for judges, contained applications relevant for judges, such as the Internet, the e-mail, online applications, or electronic databases.[1536] The picture of the DNS project at mid-2002 showed a project well on track.[1537] There is, however, no clear indication of whether IT projects focusing only on judges have been introduced in South Africa. In addition no information was found on the applications specific to judges that are currently in use in South African courts.[1538]

The second category of ICT applications used in the judicial system that was discussed consists of applications allowing the exchange of information between courts, parties and the general public. These applications include, among other things, a court website where information regarding the court's organisation and activities can be found; downloadable forms might also be available on the website to permit for the electronic submission of claims. Other important tools for the electronic communication and information exchange between the courts and their environment include electronic registers, business or land registers, for example, or text-messaging application allowing parties to be informed of the status of their case on the court list.[1539] The situation of these applications in the selected jurisdictions is as follows. England follows a centralised approach for the provision of information regarding the courts with court information now provided on the Ministry of Justice website www.justice.gov.uk, but currently in the process of moving to www.gov.uk. In addition for the electronic exchange of court documents there is the Money Claim Online (MCOL) which is a HMCTS Interned-based service

1534 Ch 5 par 5.2.2.1.3 A
1535 Ch 5 par 5.2.2.1.3 B
1536 Ch 5 par 5.2.2.1.3 C
1537 See Ch 5 par 5.2.2.1.1 above
1538 Ch 5 par 5.2.2.1.3 C
1539 Ch 5 par 5.2.2.2

for claimants and defendants to make, or to respond to, a money claim on the Internet in a convenient and secure way.[1540] In Singapore court information can be obtained from the Supreme Court's website, the Mobile Information Service or via the infokiosks available within the premises of the Supreme Court. In addition the filing and service of court documents can easily be done through the Electronic Filing System. The vision of a paperless courtroom is a reality in Singapore.[1541] In contrast, South Africa is lagging behind despite the fact that general court information is available from the website of the Department of Justice and Constitutional Development www.justice.gov.za. In respect of the electronic exchange of information there is a big gap with Singapore. Apparently South Africa is still at a theoretical level with the CPP although a pilot project was initiated. There is no indication that electronic exchange of information is taking place at this stage in South Africa.[1542]

The last category of ICT applications used in the judicial system comprises applications used in the courtroom. They include hardware and software designed to help parties in the presentation of their case in court, such as computers and multimedia screens, video conferencing, electronic evidence presentation software, and so on. In 2012, the UK counted 12 specifically equipped EPE courtrooms, in other words courtrooms equipped with Electronic Presentation of Evidence facilities.[1543] In Singapore, the first technology court was introduced 20 years ago and offered advanced technologies such as a digital recording system, audio-visual facilities and video conferencing. Since then there has been even more advances with The Technology Court 2.[1544] In South Africa an important technology used in the courtroom is video conferencing. It was for instance used with success in *S v De Grandhomme and Another*,[1545] case during which witnesses scattered around the world were able to give evidence through video conferencing.[1546]

After discussing ICT applications used in the judicial system the chapter dealt with the legal perspective by addressing the legal challenges that the implementation of some of these applications may raise. The analysis consisted in the assessment of rules of civil procedure and

1540 Ch 5 par 5.2.2.2 A 2
1541 Ch 5 par 5.2.2.2 B
1542 Ch 5 par 5.2.2.2 C
1543 Ch 5 par 5.2.2.3 A
1544 Ch 5 par 5.2.2.3 B
1545 (C) 4-12-97 (case SS18/97 unreported)
1546 Ch 5 par 5.2.2.3 B

their effectiveness in dealing with electronic justice, in particular rules governing the filing and service of documents, discovery, and documents to be used at court's hearings.[1547]

In respect of the filing and service of documents, the discussion dealt with the service of court process on the one hand and the service of other documents on the other hand. With regard to court process, the discussion was divided in court process used in application proceedings, that is, notice of motion and court process used in action proceedings, that is, summons. For each category one examined the validity of such documents in electronic form and the legal issues raised in case of electronic service in terms of the Uniform Rules of Court and Magistrates' court rules. It was pointed out that these court rules exclude the validity of both categories of court process in electronic form as inferred from the modes of service provided in both court rules.[1548] In both cases electronic service is not listed among the accepted modes of service. Hence, it was submitted that there was a need to amend the rules accordingly to include electronic service in the list of acceptable modes of service of court process.[1549] To achieve this, guidance can be obtained from Singapore and to a certain extent from England. In Singapore court process can be introduced by electronic means using the Electronic Filing System as provided by Order 63A. In England, it is also possible to file court process to courts by electronic means in terms of Practice Direction 5B.[1550]

The service of other documents such as affidavits and pleadings was then discussed. Unlike the service of documents initiating proceedings above,[1551] the service of other documents as defined above can be effected legally by electronic means in accordance with rule 4A of the Uniform Rules of Court as confirmed in *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens*.[1552] However, this rule does not provide for the possibility to file documents with the registrar by electronic means. This clearly is an obstacle to the promotion of electronic justice

1547 Ch 5 par 5.3
1548 Rule 4 and rule 9 respectively
1549 Ch 5 par 5.3.1.1
1550 Ch 5 par 5.3.1.1
1551 Ch 5 par 5.3.1.1
1552 (KZN)(unreported case no 6846/2006, 3-8-2012)

and should be amended accordingly in line with Order 63 A in Singapore and Practice Direction 5 B in England.[1553]

In respect of discovery, the discussion highlighted the following aspects. Firstly discovery is a pre-trial procedure whereby, upon request, a party discloses to the requesting party all documents in his possession that might be relevant to the trial and eventually gives access to them. Secondly with the advent of technology, the nature of information to be disclosed has changed as information is increasingly created, processed, stored and communicated electronically. In addition the amount of information required to be disclosed is higher. Thirdly this section was dedicated to analysing the discovery of ESI, also known as electronic discovery with reference to relevant rules governing this procedure in England, Singapore and South Africa.[1554]

In England before dealing with the legal aspect, namely the relevant rules, a description of e-discovery was provided as well an overview of the functioning of EDRM, a software tool used for the discovery of ESI.[1555] In respect of the legal aspect Part 31 of the Civil Procedure Rules was briefly discussed before dealing successively with PD 31A, PD 31B and the *Digicel* case. PD 31B is particularly interesting as it deals with all aspects specific to e-discovery and constitutes therefore a good source of information for South Africa. *Digicel* is also a good example of how e-discovery can get out of control if not well managed.[1556]

In Singapore the regime applicable to electronic discovery consists of Order 24 of the Rules of Court and Part V of the ePractice Directions with the former governing discovery in general and latter dealing specifically with the discovery and inspection of electronically stored documents. Singapore clearly follows a similar approach to England, that is, acknowledge that the general principles governing traditional discovery should apply to e-discovery, but also recognize the need for a specific regime for the latter to cater for the specificities of ESI and the need to control the burden and cost of retrieving ESI and producing it.[1557]

1553 Ch 5 par 5.3.1.1.1
1554 Ch 5 par 5.3.2
1555 Ch 5 par 5.3.2.2.1
1556 Ch 5 par 5.3.2.2.1
1557 Ch 5 par 5.3.2.3.3

South Africa was the last jurisdiction discussed. As discovery is governed by Rule 35 of the Uniform Rules of Court and rule 23 of the Magistrates' courts rules, these two rules were examined with reference to e-discovery. It was submitted that the above rules are inadequate to deal effectively with e-discovery. To address these shortcomings reference should be made to England and Singapore and follow the approach taken there, that is, keep these rules with minor amendments in relation to definitions and introduce a rule dealing specifically with e-discovery.[1558]

The last section in Chapter 5 has dealt with documents to be used at court's hearings. It provided an overview of certain rules in Singapore relevant to the preparation of documents for use in court in a paperless environment. It served as information and is worth considering in the process of the adaptation of rules of court in South Africa to embrace the digital age. These rules concern mainly the electronic creation and filing of bundles of documents.[1559] This concludes the substantive part of the thesis. The next chapter below provides a summary of the main conclusions reached in the discussions conducted throughout the thesis as well as recommendations.

[1558] Ch 5 par 5.3.2.4
[1559] Ch 5 par 5.3.3

CHAPTER 6 SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

6.1 Introduction

This thesis set out to analyse the legal challenges that may be raised by the introduction of e-justice in South Africa from both the viewpoint of the law of evidence and that of the law of civil procedure. It started from the premise that the widespread use of ICTs has led the world to a new era, the electronic age, where most information is created, processed, stored and communicated electronically. This reality has resulted in the transformation of modes of social and economic organisation.[1560] The administration of justice, which is not immune to these changes, needs to transform as well. Such transformation is, however, possible only if the necessary legislative infrastructure in respect of the law of evidence and of law of civil procedure is in place.[1561] This final chapter highlights the fundamental issues covered in the body of the thesis relating to electronic evidence and procedure at the start. Secondly, it provides recommendations when *lacunae* have been identified. Lastly, it suggests some areas for future research.

6.2 Legal issues from the viewpoint of the law of evidence

Before addressing the legal issues raised from the viewpoint of the law of evidence, it is appropriate to stress why the law of evidence is relevant in the first place. The relevance of the law of evidence flows from the fact that the advancement of technology has created an entirely new source of evidence, electronic evidence.[1562] The thesis has sought, therefore, to determine whether rules of evidence in South Africa could effectively deal with electronic evidence.[1563] To do that, it was imperative firstly to define electronic evidence. This was done by means of a broad definition borrowed from Mason who defines electronic evidence as "data (comprising the output of analogue devices or data in digital format) that is manipulated, stored or communicated by any man-made device, computer or computer system or transmitted over a communication system, that has the potential to make the factual account of either party more probable or less

[1560] Ch 1 par 1.1
[1561] Ch 1 par 1.2
[1562] Ch 1 par 1.1
[1563] Ch 1 par 1.2

probable than it would be without the evidence."[1564] The definition is wide enough to include not only evidence in the form of photographs, films, tape and video recordings, but also computer and machine-generated evidence, including evidence in digital format. After the clarification of the meaning of electronic evidence, legal issues around the admissibility and weight of such evidence were discussed to answer the question of the adequacy of the South African law of evidence in dealing with electronic evidence. This required an examination of both the common law and statutory law.[1565]

The first issue focussed upon was the legal nature of electronic evidence, necessary to determine the applicable rules. The analysis revealed a mixed nature, that is, electronic evidence can, on the one hand, fall under traditional categories of evidence, such as real evidence or documentary evidence. On the other hand, it can be viewed as *sui generis* evidence with a special regime.[1566]

6.2.1 Electronic evidence and real evidence

The admissibility of electronic evidence as real evidence was analysed by highlighting both electronic evidence in analogue format and electronic evidence in digital format. Such an analysis shows that the traditional rules applicable to real evidence are perfectly applicable to electronic evidence. In other words, if electronic evidence, properly identified as real evidence, is relevant and there is no rule of evidence excluding its reception, it will be admitted in evidence. Under what circumstances then is electronic evidence admissible as real evidence? From the case law of both England and South Africa discussed in the thesis, to be admissible as real evidence, electronic evidence must have been generated without the intervention of the human mind; in other words, it must have been automatically produced.[1567] Electronic evidence accepted as real evidence, however, needs proper testimonial foundations to be of any assistance in demonstrating the truth of the statement contained in it.[1568]

1564 Mason *Electronic Evidence* (2012) 25; Ch 2 par 2.3.1

1565 Ch 3 in general

1566 Ch 2 par 2.1

1567 See the English case *The Statue of Liberty* 1968 1 WLR 739. This case has been used as an authority in South Africa as well. For a discussion on the admissibility and weight of electronic evidence as real evidence see, in general, Ch 3 par 3.2

1568 Ch 2 par 2.2.4.2 and Ch 3 par 3.2.1

6.2.2 Electronic evidence and documentary evidence

The admissibility and weight of electronic evidence as documentary evidence was discussed in England through the following pieces of legislation: the Bankers' Books Evidence Act 1879; the Civil Evidence Act 1995; and the Criminal Justice Act 2003. All these statutes permit the admission of electronic evidence as a form of documentary evidence. For example the definition of "document" in terms of section 13 of the Civil Evidence Act 1995 is so broad that it can easily accommodate electronic documents. In respect of the South African jurisdiction, the discussion has covered common law, the CPEA, the CPA on the one hand and the Computer Evidence Act 57 of 1983 and the ECT Act on the other hand. The rules provided by these Acts are applicable to electronic documents, however, not all them can be applied satisfactory, for example section 34 of the CPEA fell short to deal with electronic documents in *Narlis v South African Bank of Athens*,[1569] because of a definition of document too narrow in scope.[1570] The Computer Evidence Act 57 of 1983, which was adopted in response to the above case, was very much criticised because it put too much emphasis on authenticated computer printouts. Its repeal by the ECT Act was welcome. The ECT Act is a big step forward, like the Model Law on E-commerce from which it originates, it provides for the admissibility of data messages in evidence as long as they respect the normal rules of evidence which should not, however, deny them admissibility in evidence only because they are in electronic format. For example, if a data message is adduced in evidence as a document, to be admissible it must satisfy the ordinary requirements for the admissibility of documents, including the requirements of originality and authenticity.[1571] The application of these principles to electronic documents based on the traditional understanding of original and authentication is, however, unsatisfactory. It is welcome that these shortcomings have been addressed by the principle of functional equivalence adopted by the UNCITRAL Model Laws and followed by the ECT Act. Indeed, whereas traditionally "original" is defined as a medium on which information was fixed for the first time, based on the principle of equivalence, originality, in the case of electronic information, is determined by using two criteria, the guarantee of integrity and the capacity for the information to be displayed or

1569 1976 2 SA 573 (A)
1570 Ch 3 par 3.4.2.1.1 A
1571 The admissibility and weight of electronic evidence as documentary evidence is dealt with at Ch 3 par 3.4

produced to the person to whom it is to be presented.[1572] In the same way, the authenticity of electronic documents can be established by means of a process or system such as an electronic signature which will prove that the document originates from the person to whom it is attributed.[1573]

6.2.3 Electronic evidence and hearsay rule

The hearsay rule has been discussed, and its relevance when dealing with electronic evidence was highlighted. The relationship is so close that some authors, including Teppler, consider all computer-generated information as hearsay.[1574] In compliance with case law, however, the submission of this thesis is that it is important to determine how the information was generated. If it was generated automatically, that is, without the intervention of a human being, then it is not hearsay but real evidence; on the other hand, if there was a direct human involvement in its creation, then considerations of hearsay nature may be applicable. In fact such electronic evidence will qualify as hearsay only if its probative value depends upon the credibility of any person other than the person giving such evidence. It was pointed out that the regime of hearsay in England and South Africa was amended significantly through legislative intervention. England has adopted an inclusionary approach toward hearsay making almost all hearsay admissible,[1575] while South Africa is still preferring an exclusionary approach but much more flexible to allow the admission of more hearsay evidence.[1576] In consequence electronic hearsay is well accommodated under the regime currently existing in both England and South Africa.[1577]

6.2.4 *Sui generis* evidence

The thesis has argued that electronic evidence may in some circumstances be considered as a *sui generis* form of evidence.[1578] The reason for this is that, because of the special characteristics of electronic information, traditional rules of evidence alone are inefficient in dealing with electronic evidence in digital format. The characteristics include the dependence on machinery

1572 Ch 3 par 3.4.2.1.3 B 2 (d)
1573 Ch 2 par 2.2.4.3.2; Ch 3 par 3.4.2.1.1 B; Ch 3 par 3.5 and Ch 4
1574 Teppler "Digital data as hearsay" 18; Ch 3 par 3.3.3.2
1575 S 1(1) of the Civil Evidence Act 1995
1576 The Law of Evidence Amendment Act 45 of 1988 in general
1577 See Ch 3 par 3.3 on the relationship between the admissibility and weight of electronic evidence and the hearsay rule; Ch 3 par 3.5
1578 Ch 1 par 1.2 and Ch 3.4.2.1.4

and software, the mediation of technology, the technical obsolescence, the high volume and easy replication of information, the nature of the storage medium, the difficulty of deletion and destruction of electronic information and the existence of metadata.[1579] When applying traditional principles and rules to electronic evidence, therefore, one must not ignore the special nature of such evidence and the necessity to take into account the principle of functional equivalence.[1580]

6.2.5 The ECT Act and electronic evidence

The thesis also examined the adequacy of the ECT Act to govern electronic evidence outside the commercial sphere in accordance with the SALRC question issued for comment.[1581] After reviewing the Model Law on E-commerce, the conclusion was reached that there are no substantive grounds for why the Model Law which is restricted to commercial activities could not be extended to civil and criminal proceedings as has been done by the ECT Act. To the recommendation of the SALRC to enact a single statute containing all provisions pertaining to electronic evidence in terms of the ECT Act, the CPA and the CPEA, it was submitted, in line with the majority of the respondents, that it was not necessary as the ECT Act is fine, and any inconsistencies between the CPA and CPEA in dealing with electronic evidence could easily be removed by amending and supplementing existing provisions in terms of both Acts.[1582]

6.2.6 Electronic signatures

Electronic signatures were discussed in great detail in chapter 4. Acknowledging that electronic evidence faces challenges in respect of notions of authenticity, integrity and non-repudiation of evidence, it was argued that an electronic signature can address these challenges. The analysis included international initiatives, relating to the UN and EU, on the one hand; and on the other hand national initiatives with reference to the jurisdictions of England, Singapore, and South Africa. In respect of the UN, all instruments discussed in Chapter 4 recognise electronic signatures. The Model Law on Electronic Signatures, however, deals with the subject in more detail and was therefore given more attention. Indeed it offers practical standards against which

1579 Ch 2 par 2.3.2
1580 Ch 3 par 3.4.2.1.3 B and Ch 3 par 3.5
1581 Ch 3 par 3.4.2.1.1 B 2 (g)
1582 Ch 3 par 3.4.2.1.3 B 2 (g) and Ch 3 par 3.5

the technical reliability of electronic signatures may be measured. It further provides a link between such technical reliability and the legal effectiveness that might be expected from a given electronic signature.[1583] It is an interesting initiative in that it contributes to enabling or facilitating the use of electronic signatures and provides equal treatment to both users of paper-based documentation and users of computer-based information. [1584] Regarding the EU, from the discussion on the eSignature Directive, it was concluded that the legal framework provided by this Directive facilitates the use of electronic signatures and contributes to their legal recognition within the Internal Market. It was submitted that this effort by the EU was in line with the global effort by the UN above.[1585]

Under national initiatives, the section on England discussed the Electronic Communications Act 2000 and the Electronic Signatures Regulations 2002. The 2000 Act transposes the eSignature Directive into England's national law while the 2002 Regulations deal with certain aspects of this Directive, for example advanced electronic signatures. Both texts constitute the legal framework for electronic signatures in England, complemented by case law. They contribute to the legal recognition and admissibility of electronic signatures in England.[1586]

In Singapore the discussion on electronic signatures focused on the Electronic Transactions Act 2010 with a few references to the Electronic Transactions Act 1998. The legal framework in this jurisdiction, which is in harmony with the international initiatives above, promotes the use of electronic signatures in Singapore.[1587]

Lastly, in South Africa, electronic signatures are governed by the ECT Act. This Act adopts the so-called two-tier approach promoted by the Model Laws on Electronic Commerce and Electronic Signatures by providing for two types of electronic signature, namely an electronic signature and an advanced electronic signature and the effect of both. The Act was analysed and similarities with the Model Laws and the eSignature Directive highlighted. For example the definition of advanced electronic signature under the ECT Act is almost identical to that of the

1583 Par 4 of the Guide to Enactment of the UNCITRAL Model Law on Electronic Signatures (2001); Ch 4 par 4.3.1.1.2 and par 4.4 above
1584 Ch 4 par 4.3.1.1.2
1585 Ch 4 par 4.3.1.2.2 B
1586 Ch 4 par 4.3.2.1 and par 4.4
1587 Ch 4 par 4.3.1 and par 4.4

eSignature Directive.[1588] The discussion extended to the application procedure for advanced electronic signatures, in other words the accreditation and to circumstances where the law requires a signature and how an electronic signature can satisfy such requirement. Attention was also given to more stringent conditions regarding signatures, for example the electronic notarisation. Finally regard was made to case law with a couple of cases which have considered the use of an electronic signature and its legal effect.[1589]

In conclusion a review of different forms of electronic signatures was conducted. It included typing a name, clicking, browse wrap, personal identification number and password, e-mail address, scanned manuscript signature and digital signature.[1590] The latter enjoyed more attention and was discussed from both technical and legal perspective, with a review of case law.[1591] A description of the functioning of a digital signature system has revealed that such a type of signature can accomplish the essential effects desired of a signature from a legal point of view, for example: ensuring the authenticity of the identity of the signer of a message; the integrity of the message; and the exclusion of the possibility of the repudiation of the message by the parties.[1592] This marks the end of the summary of conclusions relating to the law of evidence. The next point below deals with the summary of conclusions made throughout the thesis on the legal issues from the viewpoint of the law of civil procedure.

6.3 Legal issues from the viewpoint of the law of civil procedure

It is important to start this section by reminding one of the relevance of dealing with procedure, and, in particular, civil procedure. As noted, the change in the nature of information following the electronic revolution necessitates a transformation of the justice system by means of technology.[1593] Such electronic transformation raises issues from a procedural point of view. It was, therefore, crucial to examine these. The emphasis was put on the law of civil procedure because of the greater amount of exchange of information taking place in civil proceedings compared with criminal proceedings, and the choice made was deliberate so as to avoid, as much

1588 Ch 4 par 4.3.1.2.2 A and par 4.3.2.3.1
1589 Ch 4 par 4.3.2.3.1 and par 4.4
1590 Ch 4 par 4.3.3
1591 Ch 4 par 4.3.7
1592 Ch 4 par 4.3.3.7 and par 4.4
1593 Ch 1 par 1.1

as possible, criminal proceedings and all the constitutional issues that they may raise.[1594] Before addressing these legal issues, however, a technical overview of e-justice was provided.[1595]

6.3.1 Technical overview of e-justice

E-justice was defined as referring to the use of information and communication technologies in the administration of justice. It is a specific field under the broad concept of e-Government which refers to the use of ICTs for administrative procedures.[1596] Three categories of technologies and applications used in the judicial system were identified and documented in the thesis, namely: applications used to support court administrative staff and judges; applications allowing the exchange of information between courts, parties and the general public; and applications that facilitate the presentation of electronic evidence in court.[1597] The extent of the availability of these technologies in England, Singapore and South Africa was discussed before dealing with procedural legal aspects which primarily concern the last two types of application.[1598] It can be stated that Singapore is a reference as far as the three categories of applications are concerned. This jurisdiction has reached a point where a paperless courtroom is a reality.[1599] From a legal point of view, the exercise was to analyse comparatively the rules of civil procedure and to determine their effectiveness in dealing with e-justice.[1600] This was done essentially by reviewing rules for the service of documents and rules for the discovery of documents.[1601]

6.3.2 Service of documents

The service of two types of documents was considered, court process on the one hand, and other documents, such as notices and pleadings, on the other hand. In respect of the court process, a review of the Uniform Rules of Court and the Magistrates' court rules revealed the limitations of both set of rules in dealing with the electronic service of court process. Neither a notice of

1594 Ch 1 par 1.2
1595 Ch 2 par 2.4.2 and Ch 5 par 5.2
1596 Ch 2 par 2.4.2 and Ch 5 par 5.2.1
1597 Ch 5 par 5.2.2
1598 Ch 5 par 5.2
1599 Ch 5 par 5.2.2.2 B
1600 Ch 1 par 1.2
1601 Ch 5 par 5.3

motion in application proceedings nor a summons in action proceedings can, therefore, be filed electronically to the registrar or clerk of the court in South Africa. The electronic filing of a process of court is not possible at this stage because electronic filing is not listed among the modes of accepted service. In addition, there is a specific requirement in terms of the Magistrates' court rules for a process of court to be on A4 standard paper.[1602] In the case of action proceedings, for instance, there is a clear distinction between the service of a document initiating proceedings, such as a summons, and the service of subsequent documents and notices in the suit. The first category is excluded from electronic service while the second category can be carried out electronically.[1603]

The service of other documents, such as notices (notice of opposition or notice of intention to defend) and pleadings can be validly performed using ICTs as it was held in *CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens*.[1604] The filing with the registrar of a notice of set down will, however, need to be in paper form. This is another rule preventing the full implementation of e-justice.[1605]

For all these identified obstacles, it was deemed appropriate to look at Singapore and England to find out how they managed to overcome them.[1606]

6.3.2.1 Singapore

Singapore is definitely a good example when it comes to the design and implementation of e-justice. It has developed a very successful litigation system, known as the Electronic Filing System which, amongst other things, allows lawyers to file documents electronically to courts and to serve court documents to other law firms.[1607] To achieve this success, Singapore had to design appropriate rules, which are contained in Order 63A.[1608] In respect of the obstacles identified above, one may highlight, as elements to consider: the powers given to the Registrar to establish an electronic filing service and to determine the documents required to be filed using

1602 Rule 1(4)(c)
1603 Rule 17(3)(d) & (e) of the Uniform Rules of Court; Ch 5 par 5.3.1.1.1 and par 5.4
1604 (KZN)(unreported case no 6846/2006, 3-8-2012)
1605 Ch 5 par 5.3.1.2.1 and par 5.3.1.2.2 and par 5.4
1606 Ch 5 par 5.3.1.1
1607 Ch 5 par 5.3.1.1.1
1608 Ch 5 par 5.3.1.1.1

such service; the online access to the electronic filing service or access through a service bureau equipped with the necessary assistance capacity; the use of an identification code to satisfy the requirement of a signature for documents communicated using the electronic filing service. In addition Order 63A deals with the time when service begins to run as well as how affidavits in electronic form may be filed in Court using the electronic filing service.[1609]

6.3.2.1 England

In England, specified documents may be filed by parties to specified courts by e-mail or *via* an online forms service.[1610] A practice direction describes the conditions under which the communication or filing of documents can be done.[1611] It is worth mentioning that, when a document is filed electronically, it is not required to send a copy of that document to court.[1612] It can also be pointed that payment facilities are available on the online forms service for a claim requiring the payment of a fee.[1613] To a certain extent, England, too, can help South Africa to overcome some of the obstacles identified above.

6.3.3 Discovery of documents

Electronic discovery or the discovery of electronically-stored information was analysed extensively.[1614] This is a very important subject as the development of technology has generated a massive amount of electronic information, such as e-mail, web pages, word processing files, computer databases, or documents stored on servers or back-up systems. All that information needs to be searched, reviewed and discovered in case of litigation.[1615] How effective is the current regime governing electronic discovery in South Africa?

A review of Rule 35 of the Uniform Rules of Court and rule 23 of the Magistrates' court rules was conducted and that has highlighted a certain number of shortcomings. The lack of a clear definition of document, including ESI, creates uncertainty. In addition, a certain number of

1609 Ch 5 par 5.3.1.1.1
1610 Par 1.1 and par 1.2 of Practice Direction 5B
1611 Practice Direction 5B
1612 Par 8.1 of Practice Direction 5B
1613 Par 6.2 of Practice Direction 5B; Ch 5.3.1.1.1
1614 Ch 5 par 5.3.2
1615 Ch 5 par 5.3.2.1

issues specific to electronic discovery are not covered by these rules. These include: the cooperation between the parties in the management of e-discovery to ensure a proportionate and cost-effective e-discovery process; the different types of ESI and their discovery mode, in particular metadata and not reasonably accessible documents; the storage of ESI; the preservation of ESI; the reasonable search of ESI; the format and the manner of supplying copies of discoverable ESI; and the inspection of ESI.[1616]

To address these pitfalls the thesis found it appropriate to look to the jurisdictions of Singapore and England.

6.3.3.1 Singapore

In Singapore the regime applicable to electronic discovery consists of Order 24 of the Rules of Court and Part V of the ePractice Directions with the former governing discovery in general and latter dealing specifically with the discovery and inspection of electronically stored documents. Singapore clearly follows a similar approach to England, that is, acknowledge that the general principles governing traditional discovery should apply to e-discovery, but also recognize the need for a specific regime for the latter to cater for the specificities of ESI and the need to control the burden and cost of retrieving ESI and producing it.[1617] Issues raised above under South Africa may be solved by looking at Part V.[1618]

6.3.3.2 England

Discovery was also the subject of a review in England which resulted in the reform of the discovery regime. The current regime comprises Part 31 of the Civil Procedure Rules and Practice Directions 31 A and 31 B. Part 31 governs discovery in general, while Practice Direction 31 B deals specifically with the discovery of electronic documents and Practice Direction 31 A deals with a few aspects relevant to electronic discovery, in particular the definition of "document" which includes, for example, "deleted" electronic documents and metadata or information stored or associated with electronic documents.[1619] For most issues

1616 Ch 5 par 5.3.2.4.3
1617 Ch 5 par 5.3.2.3.3
1618 Ch 5 par 5.3.2.3
1619 Par 2A.1

identified as not covered by Rule 35 and rule 23 in South Africa, guidance can be obtained from Practice Direction 31B.

This concludes the summary of conclusions made for both the perspectives of the law of evidence and the law of civil procedure. With such background one can state below recommendations put forward by the thesis.

6.4 Recommendations

The identification of legal issues raised by e-justice in South Africa in the preceding lines would not be complete if it were not accompanied by recommendations on how to tackle these issues. Recommendations are provided below based on a separation between the law of evidence and the law of civil procedure.

6.4.1 Recommendations regarding the law of evidence

In respect of electronic evidence in general, it is recommended that a manual to guide the collection and production of such evidence in court be developed in order to ensure a proper understanding of the technical aspects involved in producing electronic evidence in court.

Regarding the application of principles of documentary evidence such as original and authenticity to electronic evidence, the development of a handbook which will provide guidelines on how to assess integrity of information is recommended.

Regarding the inconsistencies between the CPA and the CPEA in respect of the definition of document, it is recommended that both definitions be amended and a uniform definition of document, which will clearly include electronic-stored information, be adopted.

6.4.2 Recommendations regarding the law of civil procedure

In respect of e-justice in general, it is recommended that a policy document on the promotion of e-justice be adopted by the Department of Justice and Constitutional Development with clear strategies on how to ensure success. In addition, the judiciary, at the highest level, must take the lead in carrying out the electronic transformation of the justice system in South Africa which will

ensure a world-class judiciary, in other words a dynamic judiciary, which will be able to keep pace with the rapidly changing needs of society.

On the service of documents, it is recommended that the Rules of Court be amended in order to ensure:

1. the legal validity of an electronic process of the court;
2. the electronic filing of such court process;
3. that electronic filing be given the same status as other modes of service;
4. that other notices, in particular a notice to set down, can be filed electronically to court;
5. that an electronic filing system be introduced.

On electronic discovery, it is recommended that the following be included in the Rules of Court:

1. a definition of document which should specifically include electronically-stored information such as metadata;
2. An entire rule, for example Rule 35 A in the Uniform Rules of Court, specifically regulating electronic discovery. Such a rule should deal with: the co-operation between the parties in the management of e-discovery to ensure a proportionate and cost-effective e-discovery process; the different types of ESI and their discovery mode, in particular metadata and not reasonably accessible documents; the storage of ESI; the preservation of ESI; the reasonable search of ESI; the format and the manner of supplying copies of discoverable ESI; and the inspection of ESI. To that end, it is submitted that the recommendation by the SALRC for the Rules Board for Courts of Law to work on these issues with the assistance of a working group with technical expertise is appropriate.[1620]

6.5 Areas for future research

This thesis has focused on issues raised by e-justice from the viewpoint of both the law of evidence and the law of the civil procedure. It should be noted, however, that there are other areas which could benefit from research. These include:

1. E-justice in the criminal justice system;

[1620] SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 81

2. E-justice and information security;
3. E-justice and data protection; and
4. E-justice and the promotion of human rights.

BIBLIOGRAPHY

1. Books and reports

American Bar Association (ABA) *Digital Signatures Guidelines* 1996

(abbreviated as ABA *Digital Signatures Guidelines*)

Brazell *Electronic Signatures and Identities, Law and Regulation* 2008

(abbreviated as Brazell *Electronic Signatures and Identities, Law and Regulation*)

Buckley, Tank, Whitaker & Kromer *The Law of Electronic Signatures and Records* 2004

(abbreviated as Buckley *et al The Law of Electronic Signatures and Records*)

Campbell (ed) *E-Commerce and the Law of Digital Signatures* 2005

(abbreviated as Campbell *E-Commerce and the Law of Digital Signatures*)

Cerrillo & Fabra *E-justice: Using Information Communication Technologies in the Court System* 2009

(abbreviated as Cerrillo & Fabra *E-justice*)

Choo *Evidence* 2006

(abbreviated as Choo *Evidence*)

Christie & Bradfield *Christie's The Law of Contract in South Africa* (6th ed) 2011

(abbreviated as Christie & Bradfield *Christie's The Law of Contract in South Africa*)

Chung & Byer *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*, 4 BUJ Sci & TECH L 5 8 1997

(abbreviated as Chung & Byer *The Electronic Paper Trail: Evidentiary Obstacles to Discovery and Admission of Electronic Evidence*)

David & Brierly *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law* (2nd ed) 1978

(abbreviated as David & Brierly *Major Legal Systems in the World Today: An Introduction to the Comparative Study of Law*)

Dennis *The Law of Evidence* (4th ed) 2010

(abbreviated as Dennis *The Law of Evidence*)

Du Plessis *A Self Help Guide: Research Methodology and Dissertation Writing* 2007

(abbreviated as Du Plessis *A Self Help Guide: Research Methodology and Dissertation Writing*)

English Law Commission *Electronic Commerce: Formal Requirements in Commercial Transactions, Advice from the Law Commission 2001*

(abbreviated as English Law Commission *Electronic Commerce*)

Farlam & Van Loggerenberg *Erasmus: Superior Court Practice* 2011

(abbreviated as Farlam & Van Loggerenberg *Erasmus: Superior Court Practice*)

Forder & Quirk *Electronic Commerce and the Law* 2001

(abbreviated as Forder & Quirk *Electronic Commerce and the Law)*

Forsyth & Pretorius *Cane's The Law of Suretyship*

Halsburg *Laws of England*, vol 7

(abbreviated as Halsburg *Laws of England*)

Harris & Crowley (ed) *The Sedona Glossary: For E-Discovery and Digital Information Management* (3rd ed) 2010

(abbreviated as Harris & Crowley *The Sedona Glossary: For E-Discovery and Digital Information Management*)

Heyink *Electronic Signatures for South African Law firms* (Guidelines: Oct 2014)

(abbreviated as Heyink *Electronic Signatures Guidelines*)

Heyink *Information Security Guidelines for Law firms* (2001)

(abbreviated as Heyink *Information Security Guidelines*)

Hoffman & Zeffert *The South African Law of Evidence* (4th ed) 1988

(abbreviated as Hoffman & Zeffert *The South African Law of Evidence*)

Hoffmeister *Social Media in the Courtroom, A New Era for Criminal Justice?* (2014)

(abbreviated as Hoffmeister *Social Media in the Courtroom)*

Huxley *Evidence the Fundamentals* (2nd ed) 2010

(abbreviated as Huxley *Evidence the Fundamentals*)

Jackson *Review of Civil Litigation Costs: Preliminary Report Volume 2* 2009

(abbreviated as Jackson's *Interim Report* Vol 2)

Keane & McKeown *The Modern Law of Evidence* (9th ed) 2012

(abbreviated as Keane & McKeown *The Modern Law of Evidence*)

Lange & Nimsiger *Electronic Evidence and Discovery: What Every Lawyer Should Know* 2004

(abbreviated as Lange & Nimsiger *Electronic Evidence and Discovery: What Every Lawyer Should Know*)

Lodder, Oskamp & Schmidt (ed) *IT Support of the Judiciary in Europe* 2001

(abbreviated as Lodder *et al IT Support of the Judiciary in Europe*)

Malek (ed) *Phipson on Evidence* (16th ed) 2005

(abbreviated as Malek *Phipson on Evidence*)

Mason (ed) *Electronic Evidence: Disclosure, Discovery and Admissibility* 2007

(abbreviated as Mason *Electronic Evidence: Disclosure, Discovery and Admissibility*)

Mason (ed) *Electronic Evidence* (2nd ed) 2010
(abbreviated as Mason *Electronic Evidence* (2010))

Mason *Electronic Signatures in Law* (2nd ed) 2007

(abbreviated as Mason *Electronic Signatures in Law* (2007))

Mason *Electronic Signatures in Law* (3rd ed) 2012
(abbreviated as Mason *Electronic Signatures in Law* (2012))

Mc Conville & Chui *Research Methods for Law* 2010
(abbreviated as Mc Conville & Chui *Research Methods for Law*)

Munday *Evidence* (4th ed) 2007
(abbreviated as Munday *Evidence*)

Murphy *Murphy on Evidence* (11th ed) 2009

(abbreviated as Murphy *Murphy on Evidence*)

Musson & Stebbings (ed) *Making Legal History, Approaches and Methodologies* 2012

(abbreviated as Musson & Stebbings *Making Legal History, Approaches and Methodologies*)

Oskamp, Lodder & Apistola (ed) *IT Support of the Judiciary, Australia, Singapore, Venezuela, Norway, The Netherlands and Italy* 2004

(abbreviated as Oskamp *et al IT Support of the Judiciary*)

Overly *Overly on Electronic Evidence in California* 1999

(abbreviated as Overly *Overly on Electronic Evidence in California*)

Papadopoulos & Snail (ed) *Cyberlaw@SAIII: The Law of the Internet in South Africa* 2012

(abbreviated as Papadopoulos & Snail *Cyberlaw@SAIII*)

Peté, Hulme, Du Plessis, Palmer & Sibanda *Civil Procedure a Practical Guide* (2nd ed) 2013

(abbreviated as Peté *et al Civil Procedure, a Practical Guide*)

SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings*

(Postponement of Criminal Cases via Audiovisual Link) 2003

(abbreviated as SALRC *Project 113: Report on the Use of Electronic Equipment in Court Proceedings*)

SALRC Issue Paper 27, and Project 126, *Review of the Law of Evidence: Electronic Evidence in Civil and Criminal Proceedings: Admissibility and Related Issues* 2010

(abbreviated as SALRC Issue Paper 27, *Review of the Law of Evidence* 2010)

SALRC *Discussion Paper 131 on the Review of the Law of Evidence* 2015

(abbreviated as SALRC *Discussion Paper 131 on the Review of the Law of Evidence*)

Schellekens *Electronic Signatures, Authentication Technology from a Legal Perspective* 2004

(abbreviated as Schellekens *Electronic Signatures, Authentication Technology from a Legal Perspective*)

Schwikkard & Van der Merwe *Principles of Evidence* (2nd ed) 2002

(abbreviated as Schwikkard & Van der Merwe *Principles of Evidence* (2002))

Schwikkard & Van der Merwe *Principles of Evidence* (3rd ed) 2009

(abbreviated as Schwikkard & Van der Merwe *Principles of Evidence* (2009))

Smedinghof (ed) *Online Law, the SPA's Legal Guide to Doing Business on the Internet* 1996
(abbreviated as Smedinghof *Online Law*)

Tapper *Computer Law* (4th ed) 1989
(abbreviated as Tapper *Computer Law*)

Tapper *Cross & Tapper on Evidence* (12th ed) 2010
(abbreviated as Tapper *Cross & Tapper on Evidence*)

Van der Merwe *Computers and the Law* 1986
(abbreviated as Van der Merwe *Computers and the Law*)

Van der Merwe *et al Information and Communications Technology Law* 2008
(abbreviated as Van der Merwe *Information and Communications Technology Law* (2008))

Van der Merwe *et al Information and Communications Technology Law* (2nd ed) 2016
(abbreviated as Van der Merwe *Information and Communications Technology Law* (2016))

Wright & Winn *The Law of Electronic Commerce* (3rd ed) 1999
(abbreviated as Wright & Winn *The Law of Electronic Commerce*)

Woolf *1995 Interim Report on Access to Civil Justice*

Woolf *1996 Final Report on Access to Civil Justice*

Zeffert & Paizes *The South African Law of Evidence* (2nd ed) 2009
(abbreviated as Zeffert & Paizes *The SA Law of Evidence*)

Zeffert & Paizes *Essential Evidence* 2010
(abbreviated as Zeffert & Paizes *Essential Evidence*)

Zweigert & Kotz *An Introduction to Comparative Law* (3rd ed) 1998

(abbreviated as Zweigert & Kotz *An Introduction to Comparative Law*)

Interdisciplinary Centre for Law and Information Technology (ICRI) *The Legal and Market Aspects of Electronic Signatures Final Report* Study for the European Commission – DG Information Society 2003

(abbreviated as ICRI *The Legal and Market Aspects of Electronic Signatures*)

Evidence-Based Governance in the Electronic Age, Case Study: Legal and Judicial Records and Information Systems in South Africa, A World Bank/International Records Management Trust Partnership Project, July 2002

(abbreviated as *Evidence-Based Governance in the Electronic Age Case Study*)

The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Discovery (Sedona Conference SM Working Group Series 2004)

(abbreviated as *The Sedona Principles (2004)*)

Review of Discovery in Civil Litigation Consultation Paper 2009 (Singapore)

(abbreviated as *Singapore Discovery Consultation Paper*)

Simmons & Simmons *E-Commerce Law, Doing Business Online* 2001
(abbreviated as Simmons & Simmons *E-Commerce Law*)

Shorter Oxford English Dictionary 2nd ed vol 2

A Guide to UNCITRAL: Basic Facts about the United Nations Commission on International Trade Law 2013 available at http://www.uncitral.org/pdf/english/texts/general/12-57491-Guide-to-UNCITRAL-e.pdf (accessed on 1/10/2015)

2. Articles

Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals" Sept 2000 *Pacific Rim Law & Policy Journal* 9 591

(abbreviated as Blochlinger "Primus inter pares: Is the Singapore judiciary first among equals")

Christianson & Mostert "Digital signatures" May 2000 *De Rebus* 26

(abbreviated as Christianson & Mostert "Digital signatures")

CEPEJ Report on "European judicial systems –Edition 2008 (2006 data): Efficiency and quality of justice"

CEPEJ Report on "European judicial systems –Edition 2014 (2012 data): Efficiency and quality of justice"

Collier "Machine-generated evidence and related matters" in Schwikkard & Van der Merwe (ed) *Principles of Evidence* 2002 379

(abbreviated as Collier "Machine-generated evidence and related matters")

Collier "Evidently not so simple: Producing computer print-outs in court" 2005 *Juta's Bus L* 13(1) 6

(abbreviated as Collier "Evidently not so simple")

Cucu "The requirement for metadata production under *Williams v Sprint/United Management Co:* An unnecessary burden for litigants engaged in electronic discovery" 2007 *Cornell Law Review* 93 221

(abbreviated as Cucu "The requirement for metadata production under *Williams v Sprint/United Management Co"*)

Delport "Die Wet op Rekenaargetuienis" 1983 *Obiter* 140

(abbreviated as Delport "Die Wet op Rekenaargetuienis")

Department of Justice and Constitutional Development (South Africa) "E-justice: Piecing IT together" available at http://www.justice.gov.za/docs/other%20docs/2004_ejustice_booklet.pdf (accessed on 31/11/2012)

(abbreviated as Department of Justice and Constitutional Development (South Africa) "E-justice: Piecing IT together")

De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)" 2010 *SALJ* 558

(abbreviated as De Villiers "Old 'documents', 'videotapes' and new 'data messages' – a functional approach to the law of evidence (part 1)")

Dunlop "Chapter 20: South Africa" in Campbell (ed) *E-Commerce and the Law of Digital Signatures* 2005 559

(abbreviated as Dunlop "Chapter 20: South Africa")

Ebden "Computer evidence in court" 1985 *SALJ* 687

(abbreviated as Ebden "Computer evidence in court")

Forum of European Supervisory Authorities (FESA) for Electronic Signatures "Working paper on advanced electronic signatures" 12 October 2004

(abbreviated as FESA"Working Paper")

Forum of European Supervisory Authorities (FESA) for Electronic Signatures "Public statement on server based signature services" 17 October 2005

(abbreviated as FESA "Public statement on server based signature services")

French "The admissibility of computer records in the SA law of evidence – a comparative survey" 1982-1983 *Natal University Law Review* 123

(abbreviated as French "The admissibility of computer records in the SA law of evidence – a comparative survey")

Givens "The admissibility of electronic evidence at trial: courtroom admissibility standards" 2003 *Cumberland Law Review* 34(1) 95

(abbreviated as Givens "Electronic evidence admissibility standards")

Goode "The admissibility of electronic evidence" *2009-2010 Rev Litig* 29(1) 1

(abbreviated as Goode "The admissibility of electronic evidence")

Hofman "Chapter 17: South Africa" in Mason (ed) *Electronic Evidence* 2010 675

(abbreviated as Hofman "Chapter 17: South Africa")

Hofman "Electronic evidence in criminal cases" *2006 SACJ* 3 257

(abbreviated as Hofman"Electronic Evidence in criminal cases")

Howie "Evidence led via electronic media" Nov 1998 *De Rebus* 49

(abbreviated as Howie "Evidence led via electronic media")

Ibbetson "Comparative legal history: a methodology" in Musson & Stebbings (ed) *Making Legal History*: *Approaches and Methodologies* 2012 131

(abbreviated as Ibbetson "Comparative legal history: a methodology")

Kelman "*Job v Halifax PLC* (not reported) Case number 7BQ00307, commentary by Alistair Kelman" 2009 *Digital Evidence and Electronic Signature Law Review* 6 235

(abbreviated as Kelman "*Job v Halifax PLC* (not reported) Case number 7BQ00307, commentary by Alistair Kelman"

Kim "Electronic evidence: Singapore's approach" July 2002 *Law Gazette* 1

(abbreviated as Kim "Electronic evidence: Singapore's approach")

Mason "The evidential foundations" in Mason (ed) *Electronic Evidence: disclosure, discovery and admissibility* 2007 66

(abbreviated as Mason "The evidential foundations")

Meintjes-Van der Walt "Electronic evidence" in Papadopoulos & Snail (ed) *Cyberlaw@ SA III: The law of the Internet in South Africa* 2012

(abbreviated as Meintjes-Van der Walt "Electronic evidence")

Oei "Digital Signatures" in Smedinghof (ed) *Online Law, the SPA's Legal Guide to Doing Business on the Internet* 1996 41

(abbreviated as Oei "Digital signatures")

Pattenden "Common law exceptions to the rule against hearsay: Evidence of reputation or family tradition; published works; public information; bankers' Books; Ancient Documents" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 910

(abbreviated as Pattenden "Common law exceptions to the rule against hearsay")

Pattenden "Res gestae and certain other exceptions to the hearsay rule in criminal proceedings" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 877

(abbreviated as "Res gestae and other exceptions to the hearsay rule")

Pattenden "The rule against hearsay" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 772

(abbreviated as Pattenden "The rule against hearsay")

Reed "What is a Signature?" 2000 *The Journal of Information, Law and Technology (JILT)* 3 1 available at http://elj.warwick.ac.uk/jilt/00-3/reed.html/ (accessed on 01/04/2014)

(abbreviated as Reed "What is a signature?")

Salmond "The superiority of written evidence" 1890 *LQR* 6(1) 75

(abbreviated as Salmond "The superiority of written evidence")

Skeen "Evidence and computers" 1984 *SALJ* 675

(abbreviated as Skeen "Evidence and computers")

Snail & Hall "Electronic wills in South Africa" 2010 *Digital Evidence and Electronic Signature Law Review* 7 67

(abbreviated as Snail & Hall "Electronic wills in South Africa")

Steele "Computer-produced print-out reliable as evidence" 1983 *SALJ* 510

(abbreviated as Steele "Computer-produced print-out reliable as evidence")

Sze "Chapter 3: Singapore" in Oskamp, Lodder & Apistola (ed) *IT Support of the Judiciary, Australia, Singapore, Venezuela, Norway, The Netherlands and Italy* 2004 45

(abbreviated as Sze "Chapter 3: Singapore")

Teppler "Digital data as hearsay" 2009 *Digital Evidence and Electronic Signature Law Review* 6 9

(abbreviated as Teppler "Digital data as hearsay")

Van der Merwe "Documentary evidence (with specific reference to hearsay)" 1994 *Obiter* 80

(abbreviated as Van der Merwe "Documentary evidence")

Van Dorsten "Discovery of electronic documents and attorneys' obligations" Nov 2012 *De Rebus* 34

(abbreviated as Van Dorsten "Discovery of electronic documents and attorneys' obligations")

Van Rijswijck "South Africa justice system goes hi-tech" online publication 9 Nov 2011 available at http://www.southafrica.info (accessed on 25/11/2014)

(abbreviated as Van Rijswijck "South Africa justice system goes hi-tech")

Velicogna "Justice systems and ICT: What can be learned from Europe" 2007 *Utrecht Law Review* 3(1) 129 available at http://www.utrechlawreview.org (accessed on 7/11/2014)

(abbreviated as Velicogna "Justice systems and ICT: What can be learned from Europe")

Velicogna "ICT within the court in the e-justice era" available at http://effectius.com/yahoo_site_admin/assets/docs/ICT_within_the_court_in_the_e-justice_Era_by_Marco_Velicogna.207234735.pdf (accessed on 23/10/2015)

(abbreviated as Velicogna "ICT within the court in the e-justice era")

Watney "Admissibility of electronic evidence in criminal proceedings: An outline of the South African legal position" 2009 *JILT* 1

(abbreviated as Watney "Admissibility of electronic evidence in criminal proceedings")

Whale "Hearsay in civil proceedings" in Malek (ed) *Phipson on Evidence* (17th ed) 2009 814

(abbreviated as Whale "Hearsay in civil proceedings")

Willassen "Line based hash analysis of source code infringement" 2009 *Digital Evidence and Electronic Signature Law Review* 6 210

(abbreviated as Willassen "Line based hash analysis of source code infringement")

3. Internet links

AIDE "Digital forensics" available at http://www.appyide.org/working-groups/digital-forensics/ (accessed on 29/10/15)

Anonymous "Analog vs Digital" available at http://www.diffen.com/difference/Analog_vs_Digital(accessed on 07/03/2013)

Anonymous "Automated teller machines" available at

http://www.history.com/topics/inventions/automated-teller-machines (accessed on 29/08/2014)

Anonymous "EDRM stages" available at http://www.edrm.net/resources/edrm-stages-explained (accessed on 04/05/2015)

Anonymous "Security mechanics" available at http://etutorials.org/Networking/Wireless+lan+security/Chapter+2.+Basic+Security+Mechanics+and+Mechanisms/Security+Mechanics/ (accessed on 06/08/2014)

Business Dictionary available at *http://www.businessdictionary.com/definition/personal identification-number-PIN.html* (accessed on 28/08/2014)

Dictionary reference available at http://dictionary.reference.com/browse/telegraphy (accessed on 16/02/14)

Google Apps "Read receipts" available at https://support.google.com/mail/answer/1385059?hl=en (accessed on 20/01/2015)

Gov.UK "Make a money claim online" available at https://www.gov.uk/make-money-claim-online (accessed on 22/01/2015)

http://www.exploit-db.com/wp-content/themes/exploit/docs/14963.pdf (accessed on 06/08/2014)

https://www.justice.gov.uk/news/features/moving-to-gov.uk (accessed on 21/01/2015)

https://www.moneyclaim.gov.uk/web/mcol/welcome (accessed on 22/01/2015)

http://www.wordwebonline.com/en/RONEOGRAPH (accessed on 12/05/2016)

Oxford English Dictionary available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/159883?rskey=iD1wne&result=1&isAdvanced=false#eid (accessed on 08/06/2015)

Oxford English Dictionary available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/52611?redirectedFrom=digital#eid (accessed on 06/03/2013)

Oxford English Dictionary available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/7029?redirectedFrom=analogue#eid (accessed on 07/03/2013)

Oxford English Dictionary available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/37975?redirectedFrom=computer#eid121196826 (accessed on 07/03/2013)

Oxford English Dictionary available at http://0-www.oed.com.oasis.unisa.ac.za/view/Entry/185182?redirectedFrom=source+code#eid21845861 (accessed on 07/03/2013)

SAAA Accreditation certificate of LAWTRUST available at https://www.lawtrust.co.za/documents/DOCCertificate.pdf (accessed on 12/10/2015)

SAAA Accreditation certificate of SAPO available at https://www.trustcentre.co.za/docs/Accreditation_Award_Certificate.pdf (accessed on 12/10/2015)

SFO Operational Handbook 2012 available at http://www.sfo.gov.uk/media/106019/electronic_presentation_of_evidence_sfo_operational_handbook_topic.pdf (accessed on 27/01/15)
(abbreviated as *SFO Operational Handbook*)

LIST OF CASES

1. South African cases

Balzun v O'Hara [1964] 3 All SA 368 (T)

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

Barrett v Executors of O'Neil 1879 K 104

Blyth v Van den Heever 1980 1 SA 191 (A)

Boon v Vaughan & Co Ltd 1919 TPD 77

Botha v S 2010 2 All SA 116 (SCA)

CMC Woodworking Machine (Pty) Ltd v Pieter Odendaal Kitchens (unreported case no 6846/2006, 3-8-2012)

De Reuck v Director of Public Prosecutions 2004 (1) SA 406 (CC)

Diners Club SA (Pty) Ltd v Singh and Another 2004 (3) All SA 568 (D)

Ex Parte Rosh 1998 1 All SA 319

Fourlamel (Pty) Ltd v Maddison 1977 1 SA 333 (A)

Gemeenskapsontwikkelingsraad v Williams and Others (1) 1977 (2) SA 692 (W)

Goldblatt v Fremantle 1920 AD 123

Harvey v Niland and Others (5021/2015) [2015] ZAECGHC 149; 2016 (2) SA 436 (ECG); (2016) 37 ILJ 1112 (ECG) 2015

Hersch v Nel 1948 (3) SA 686 (AD)

Herstigte Nasionale Party van Suid-Afrika v Sekretaris van Binnenlandse Sake en Immigrasie 1979 4 SA 274 (T)

Hewan v Kourie NO 1993 3 SA 233 (T)

Hewan v Kourie NO and Another 1993 3 SA 233 (T)

*Hlongwane and Others v Rector, St Francis College and Others*1989 3 SA 318(D)

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

Le Roux and Others v Viana NO and Others 2008 (2) SA 173 (SCA)

Luttig v Jacobs 1951 (4) SA 563

Lynes v International Trade Developer Inc 1922 NPD 301

Mabena v Brakpan Municipality 1956 1 SA 179 (T)

Macdonald v The Master 2002 (5) SA 64

Mafika v SABC Ltd 2010 5 BLLR 542 (LC)

Mamushe v S 2007 4 All SA 972 (SCA)

Metedad v National Employer's General Insurance Co Ltd 1992 1 494 (W);*1992 1 SA 494 (W)*

Mnyama v Gxalaba and Another 1990 1 SA 650 (C)

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

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

Nedbank Ltd v Mashiya and Another 2006 4 SA 422 (T)

Protea Technology Limited & another v Wainer & others [1997] 3 All SA 594 (W)

R v Amod & Co Ltd 1947 3 SA 32 (A)

R v Behrman, 1957 1 SA 433 (T)

R v Daye 1908 2 KB 330

R v Lombard 1957 (2) SA 42 (T)

R v Maruvey 1918 NPD 29

R v Matanda, 1923 AD

R v Matthews 1960 1 SA 752 (A)

R v Nhlanhla 1960 3 SA 568 (T)

R v Pelunsky 1914 AD 360

R v Regan 1887 16 Cox CC 203

R v Zungu 1953 3 SA 660 (N)

Re Trollip, 12 SC 243

S B Jafta v Ezemvelo KZN Wildlife 2008 10 BLLR 954 (LC)

S v Adendorff 2004 2 SACR 185 (SCA)

S v Baleka 1986 4 SA 192 (T)

S v Baleka and Others 1986 4 SA 1005 (T)

S v De Grandhomme and Another (C) 4-12-97 (case SS18/97 unreported)

S v Fuhri 1994 2 SACR 829 (A)

S v H 1981 2 SA 586 (SWA)

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

S v Koralev and Another 2006 (2) SACR 298

S v M 2008 2 SACR 613 (SCA)

S v Mashiyi and Another 2002 2 SACR 387

S v Mbanjwa 2000 2 SACR 100 (D)

S v Molimi 2008 2 SACR 76 (CC)

S v Motata Unreported Case No: 63/968/07 Magistrate Court for the Regional Division of Gauteng, Johannesburg

S v Mpofu 1993 2 SACR 109 (N)

S v Mpumlo 1986 3 SA 485 (E)

S v Ndhlovu and Others 2002 2 SACR 325 (SCA)

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

S v Nieuwouldt 1990 4 SA 217 (A)

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

S v Shaik and Others 2007 1 SA 240

S v Singh and Another 1975 1 SA 330 (N)

S v Terblanche 1981 1 SA 791 (T)

S v Tshabalala 1980 3 SA 99 (A)

S v Tuge 1966 4 SA 565 (A)

S v Waldeck 2006 2 SACR 120 (NC)

Seccombe and Others v Attorney-General and Others 1919 TPD 270

Singh v Govender Brothers Construction 1986 4 SA 613 (N)

Skilya Property Investments (Pty) v Lloyds of London Underwriting 2002 3 SA 765 (T)

Spring Forest Trading v Wilberry (725/13) [2014] ZASCA 178

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

Trend Finance (Pty) Ltd v Commissioner for SARS 2005 (4) All SA 657 (C)

Utilisation v Wilkes (Biccari Interested Party) 2003 2 SA 590

Van den Berg v Coopers & Lybrand Trust (Pty) Ltd and Others 2001 2 SA 242 (SCA)

Van Nierkerk v Smith 1952 3 SA 17 (T)

Van Vuuren v Van Vuuren 2 Searle 116

Watts and Darlow v R 1919 NLR 108

Weltz and Another v Hall and Others 1996 (4) SA 1073 (C)

Wilken v Kohler 1913 AD 135

Woods v Walters 1921 AD 303

2. English cases

Alderson v Clay 1816 1 Stark 405; 171 ER 511

Baker v Dening (1838) 8 A&E 94

Barker v Wilson 1980 2 All ER 81

Beauvais v Green 22 TLR 816

Bennett v Brumfitt (1867) LR 3 CP 30

British Estate Investment Society Ltd v Jackson (HM Inspector of Taxes) [1956] TR 397 37 Tax Cas 79, 35 ATC 413, 50 R&IT 33, High Court of Justice (Chancery Division)

Brown v Secretary of State for Social Security 1995 COD 260

Brydges v Dix (1891) 7 TLR 215

Castle v Cross 1985 1 All ER 87 QBD

Dass (an infant) v Masih 1968 2 All ER 226

Digicel (St Lucia) Ltd & Ors v Cable & Wireless Plc & Ors [2008] EWHC 2522 (Ch), [2009] 2 All ER 1094

Firstpost Homes Ltd v Johnson and others [1995] 1 WLR 1567

France v Dutton [1891] 2 QB 208

Godwin v Francis (1870) LR 5 CP 295

Goodman v J Eban Ltd [1954] 1 QB 550

Hall v Cognos Limited Industrial Tribunal Case No 1803325/97

Hill v. Hill [1947] Ch 231

*Job v Halifax PLC*2009 (unreported) Case number 7BQ00307

Lazarus Estates Ltd v Beasley [1956] 1 QB 702

London County Council v Vitamins Ltd, London County Council v Agricultural Food Products Ltd [1955] 2 QB 218

McBlain v Cross (1872) LT 804

Morton v Copeland 16 CB 517

Murison v Cook and Another [1960] 1 All ER 689

Newborne v Sensolid (Great Britain) Ltd [1954] 1 QB 45

Pelopidas (owners) v TRSL Concord (owners) [1999] 2 Lloyd's Rep 675, 2 All ER (Comm) 737

PNC Telecom plc v Thomas [2003] BCC 202

Pryor v Pryor (1860) 29 LJPM&A 114

R v Briddick 2001 EWCA Crim 973

R v Clarke 1995 2 Cr App Rep 425

R v Derodra 2001 1 Cr App R 41

R v Feltis (Jeremy) 1996 EWCA Crim 776

R v Flynn and St John 2008 EWCA Crim 970

R v Fowden and White 1982 Crim LR 588 CA

R v Gilham [2009] EWCA Crim 2293, 173 CL&J 749

R v Governor of Brixton Prison, ex p Levin 1997 AC 741

R v Grimer 1982 Crim LR 674, 126 Sol Jo 641 CA

R v Hookway 1999 Crim LR 750

R v Humphris 2005 EWCA Crim 2030

R v Inhabitants of Holy Trinity, Kingston-on-Hull 1827 7 B&C 611; 108 ER 851

R *v Loveridge* 2001 EWCA Crim 973

R v M (R) 2003 EWCA Crim 3067

R v Maqsud Ali, R v Hussain [1966] 1 QB 688 [1965] 2 All ER 464 [1965] 3 WLR 229 CA

R v McShane 1977 66 Cr App Rep 97

R v Ore [1998 unreported] Birmingham Crown Court

R v Peach 1995 2 Cr App Resp 333 159 JP 412

R v Pettigrew 1980 71 Cr App R 39 CA

R v Rice 1963 1 QB 857 CCA (Ch 10)

R v Stevenson and Others 1971 1 All ER 678

R v Stockwell 1993 97 Cr App Rep 260 CA

R v Williams 1984 1 WLR 971

R v Wood 1983 76 Cr App Rep 110 CA

Re a debtor (No 2021 of 1995) *ex parte, Inland Revenue Commissioners v The debtor; Re a debtor* (No 2022 of 1995) *ex parte, Inland Revenue Commissioners v The debtor* [1996] 2 All ER 345 Ch D

Re Byrd 3 Curt 117

Re Doe d Phillips v Evans 2 LJ Ex 193

Redding in re (1850) 14 Jur 1052, 2 Rob Ecc 339

Saunders v Anglia Building Society [1971] AC 1004

Subramaniam v Public Prosecutor 1956 1 WLR 965

Sunley v Gowland White Ltd 2003 EWCA Civ 240

The Statue of Liberty 1968 1 WLR 739

3. American cases

Ardery v Smith 35 Ind App 94 73 NE 840

Arista Records LLC v Tschirhart 2006 WL 2728927

Byers v Illinois State Police 53 Fed. R Serve. 3d 740 (NDIII May 31 2002)

Coleman (Parent) Holdings Inc v Morgan Stanley & Co Inc Civil Action No 06 CV 0882 (RCL) (DDC)

CompuServe, Incorporated v Patterson 89 F3d 1257 (6th Cir 1996)

Crestwood Shops, LLC v Hilkene 197 SW 3d 641 (Mo App WD 2006)

Feldman v Citibank NA; Pickman v Citibank NA NY City Civ Ct 443 NYS 2d 43

Griffith v Bonawitz 73 Neb 622 103 NW 327 (1905)

Haywood Securities Inc v Ehrlich 149 P 3d 738 (Ariz 2007) (USA)

Ibcos Computers Ltd v Barclays Mercantile Highland Finance Ltd 1994 FSR 275

JSO Associates Inc v Price 2008 WL 904703 (NY Sup) 239 NYLJ 72 2008 NY Slip Op 30862 (U)

Judd v Citibank NY City Civ Ct 435 NYS 2d 210

Kloian, d/b/a Arbor Management Company v Domino's Pizza LLC 733 NW 2d 766 (Mich App 2006)

L C Services v Brown [2003] EWHC 3024 (QB) at [53] and [54], [2003] All ER (D) 239 (Dec)
Landeker v Co-operative Bldg Bank 130 NY Supp 780

M.A. Mortenson Company Inc v Timberline Software Corporation 998 P 2d 305 (Wash 2000)

People v Doggett 83 Cal App 2d 405, 188 P2d 792

Person v Google Inc 456 F Supp 2d 488 (SDNY 2006)

PHE, Incorporated dba Adam & Eve v Department of Justice 139 FRD 249 (DDC 1991)

S v Montgomery (unreported WLD case no A814/05 (25 May 2005)

State v Gaskins No 06CA0086-M (Ohio App 9 Dist Aug 13 2007)

U.S. v Hamilton 412 F3d 1138 2005 WL 1519112 (10th Cir 2005)

United States v Triumph Capital Group Inc 211 FRD 31 (D Conn 2002)

Williams v Sprint/United Management Company 230 FRD 640 (D Kan 2005); 2005 WL 2401626 (D Kan 2005)

Zubulake v UBS Warburg LLC 217 FRD 309 (SDNY 2003) and 216 FRD 280 (SDNY)

4. Singapore cases

Chua Sock Chen v Lau Wai Ming [1989] SLR 1119

Kim Eng Securities Pte Ltd v Tan Suan Khee [2007] 3 SLR 195

SM Integrated Transware Pte Ltd v Schenker Singapore (Pte) Ltd [2005] SGHC 58

5. Other foreign cases

Case 1486: 2006 judgment 19.10.2006, available online in Finnish at www.finlex.fi (reported by Mason *Electronic Signatures in Law* (2012) 113)

Case number IV.ÚS 319/05 (issued on 24 April 2006) (Czech Republic)

Case of the Cour de Cassation, soc 17 May 2006 04-46706 (France)

Citigroup Pty Ltd v Weerakoon 2008] QDC 174 (16 April 2008) (Australia)

Combined cases 106/04/JH (140/04/JH and 147/04/JH, judgment MAO: 161/04, 162/04, 163/04 of 27.8.2004) available in Finnish at www.finlex.fi (reported by Mason *Electronic Signatures in Law* (2012) 113)

Faulks v Cameron [2004] 32 Fam LR 417 [2004] NTSC 61 (Australia)

FG Münster 11 K 990/05 F (Germany)

Getup Ltd v Electoral Commissioner [2010] FCA 869 (13 August 2010) (Australia)

Hopes v HM Advocate 1960 SC (J) 106 (Scotland)

Juan Carlos Samper Posada v Jaime Tapias, Hector Cediel and others Decision 73-624-40-89-002-2003-053-00 (Colombia)

McGuren v Simpson [2004] NSWSC 35 (Australia)

MKM Capital Property Limited v Corbo and Poyser (12 December 2008 unreported) (No SC 608 of 2008) ACT Supreme Court, Master Harper (Australia)

N КГ-А 40/8531-03-П (Russia)

R v Peters 1886 16 QBD 636, 641 (Australia)

R v Zundel 1987 75 CCC (3d) 449 (Canada)

LIST OF STATUTES, BILLS, REGULATIONS AND OTHER INSTRUMENTS

1. South Africa

Abolition of Juries Act 34 of 1969

Accreditation Regulations in terms of the ECT Act 25 of 2002 published in the GG No 8701 of 20 June 2007

Act 4 of 1908

Administration of Justice (Further Amendment) Act 11 of 1927

Black Administration Act 38 of 1927

Civil Proceedings Evidence Act 25 of 1965

Companies Act 71 of 2008

Computer Evidence Act 57 of 1983

Constitution of the Republic of South Africa of 1996

Consumer Protection Act 68 of 2008

Copyright Act 98 of 1978

Criminal Procedure Act 51 of 1977

Criminal Procedure Amendment Act 65 of 2008

Criminal Procedure Amendment Act 86 of 1996

Cybercrimes and Cybersecurity Bill 2015

Draft Cybersecurity Policy of South Africa GG No 32963 of 19 February 2010

Electronic Communications Act 36 of 2005

Electronic Communications and Transactions Act 25 of 2002

Electronic Government, the Digital Future: A Public Service IT Policy Framework, February 2001

Films and Publications Act 65 of 1996

Free State Ordinance 12 of 1906

General Law Amendment Act 50 of 1956

General Law Amendment Act 68 of 1957

Interpretation Act 33 of 1957

Law of Evidence Amendment Act 45 of 1988

Magistrates Court Act 32 of 1944

National Credit Act 34 of 2005

National Information Society and Development Plan

Native Trust and Land Act 18 of 1936

Rental Housing Act 50 of 1999

Revenue Laws Amendment Act 60 of 2008

Road Traffic Act 29 of 1989

Rules Regulating the Conduct of Proceedings of Magistrates' Courts of South Africa (abbreviated as the Magistrates' Court Rules)

Sexual Offences Act 23 of 1957

Skills Development Act 97 of 1998

Stamp Duties Act 77 of 1968

Supreme Court Act 59 of 1959

Transvaal Ordinance 21 of 1966

Transvaal Proclamation 8 of 1902

Uniform Rules of Court

Wills Act 7 of 1953

2. England

Bankers' Books Evidence Act 1879

Child Support Appeal Tribunals (Procedure) Regulations 1992

Civil Evidence Act 1968

Civil Evidence Act 1995

Civil Procedure Rules

Companies (Forms Amendment No 2 and Company's Type and Principal Business Activities) Regulations 1990

Companies Act 1985

Conveyance by Rail of Military Explosives Regulations 1977

Copyright (Librarians and Archivists) (Copying of Copyright Material) Regulations 1989

Corruption Act 94 of 1992

County Court (Forms) Rules 1982

Crime (International Co-operation) Act 2003

Criminal Evidence Act 1995

Criminal Justice Act 1988

Criminal Justice Act 2003

Documentary Evidence Act 1868

Documentary Evidence Act 1882

Electronic Communications Act 2000

Evidence Act 1938

Family Proceedings Rules 1991

Imprisonment and Detention (Air Force) Rules 1980

Imprisonment and Detention (Army) Rules 1979

Insolvency Act 1936

Insolvency Rules 1986

Interpretation Act 1978

Law of Property (Miscellaneous Provisions) Act 1989

Law of Property Act 1925

Police and Criminal Evidence Act 1984

Practice Direction 5B- Electronic Communication and Filing of Documents
(abbreviated as Practice Direction 5B)

Practising Certificate Regulations 1976

Solicitors Act 1932

Statute of Frauds 1677

The Civil Procedure Rules 1998

Trade Marks Rules 1994

Wills Act 1953

3. Singapore

Electronic Transactions Act 1998

Electronic Transactions Act 2010

Evidence Act 1996

Order 24 of the Rules of Court

Supreme Court Practice Directions
(abbreviated as e-Practice Directions)

4. Other jurisdictions

Act on Electronic Services and Communication in the Public Sector (13/2003, 24.1.2003 Laki sähköisestä asioinnista viranomaistoiminnassa) (Finland)

Act on Electronic Signatures (14/2003, 24.2.2003 Laki sähköisistä allekirjoituksista) (Finland)

Administrative Judicial Procedure Act (586/1996, 26.7.1996 Hallintolainkäyttölaki) (Finland)

Directive 2000/31/EC on certain aspects of information society services, in particular electronic commerce, in the Internal Market
(abbreviated as Directive on Electronic Commerce or E-Commerce Directive)

Directive 1999/93/EC on a Community framework for electronic signatures
(abbreviated as eSignature Directive or Directive on Electronic Signatures)

Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services as amended by Directive 98/48/EC

Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts

Federal Rules of Evidence (US)

Securities and Exchange Commission Regulations (US)

UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998
(abbreviated as Model Law on Electronic Commerce or E-Commerce)

UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001
(abbreviated as Model Law on Electronic Signatures)

United Convention on the Use of Electronic Communications in International Contracts 2005
(abbreviated as the Electronic Communications Convention)