A COMPARATIVE REVIEW OF LEGISLATIVE REFORM OF ELECTRONIC CONTRACT FORMATION IN SOUTH AFRICA

by

Sizwe Lindelo Snail ka Mtuze

A thesis submitted in partial fulfilment of the requirements

for the

Degree of LLM (Legis Legum Magister)

at the

University of South Africa

Supervisor: Prof Tana Pistorius

FEB 2015

SUMMARY

Electronic contracts in the new technological age and electronic commerce have brought about world-wide legal uncertainty. When compared to the traditional paper-based method of writing and signing, the question has arisen whether contracts concluded by electronic means should be recognised as valid and enforceable agreements in terms of the functional equivalence approach.

This study will examine the law regulating e-commerce from a South African perspective in contrast to international trends and e-commerce law from the perspective of the United States. The research investigates various aspects of contract formation such as time and place, validity of electronic agreements, electronic signatures, attribution of electronic data messages and signatures, automated transaction as well as select aspects of e-jurisdiction from a South African and United States viewpoint.

KEYWORDS

Attribution of electronic data messages and electronic signatures; automated transaction; electronic contract formation; cyberlaw; e-commerce; electronic writing; electronic agreements; electronic signatures; functional equivalence; technological neutrality; time and place of contract conclusion, e-jurisdiction;

DECLARATION

I, Sizwe Lindelo Snail, hereby confirm that the research entitled

A COMPARATIVE REVIEW OF LEGISLATIVE REFORM OF ELECTRONIC CONTRACT FORMATION IN SOUTH AFRICA

is my own work and that all sources used have been acknowledged.

Sizwe Lindelo Snail ka Mtuze

FEB 2015

ACKNOWLEDGEMENTS

I would like to thank God for giving me the strength, opportunity and the gift of knowledge to pursue this research project. I also want to thank my mother, Mrs Nomangwane Snail and my father, Dr Mgwebi Lavin Snail , for their unwavering support, patience, love and tolerance on those long nights that I spent in the study at home.

I owe my supervisor Prof Tana Pistorius my gratitude for constructively criticizing the work and for her sound mentorship, guidance and support.

I also thank my Editor, Kathleen Woods for cleaning up the English.

DEDICATION

This work is dedicated to all Snail family (Oomadiba) members and all Silwana (Ohlongwane) family members that have passed on.

Thank you for your support from the world beyond as we know it.

Camagu this one is for you …

CONTENTS

ABBREVIATIONS AND ACRONYMS

AAA	Authorized Accreditation Authority
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
AUCLCS	Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa
AU	African Union
CA	Certification Authority
CSIG	Convention on Contracts for International Sale of Goods
ECT Act	South African Electronic Communications Transactions Act, Act 25 of 2002
EDI	Electronic Data Interchange
E-sign Act	Electronic Signatures in Global and National Commerce Act
HS	Human Resources
ITU	International Telecommunications Union
LAN	Local Area Network
NCCUSL	National Conference of Commissioners on Uniform State Laws
SAAA	South African Accreditation Authority
SABS	South African Bureau of Standards
SAPO	South African Post Office
SMS	Short Message Service
TCP/IP	Transmission Control Protocol/ Internet Protocol
UCITA	Uniform Computer Information Transactions Act
UETA	Uniform Electronic Transactions Act
UNECIC	United Nations Convention on the Use of Electronic Communications in International Contracts, 2005
UNCITRAL	United Nations Commission on International Trade
URL	Uniform resource locator
US	United States of America
UCC	Uniform Commercial Code
UUCP	Unix-to-Unix Copy Program

CHAPTER I: INTRODUCTION

(a) Background to research problem

In terms of the functional equivalence approach,[1] the formation of electronic contracts in the new technological age and electronic commerce has brought with it world-wide legal uncertainty as to whether electronic contracts concluded by electronic means can be recognised as valid and enforceable agreements compared to the traditional paper-based method of writing and signing. It is a common perception that the law, and more particularly the law of contract, has been lagging behind in the development of solutions for the use of electronic communication in commerce. This has led to uncertainty which, in turn, creates an obstacle to trade at a national and international level.[2] The purpose of this study is to give an excursus on the law regulating e-commerce from a South African perspective.

The absence of face-to-face negotiations in a number of significant electronic transactions (including click-wrap and web agreements for sale or licensing of software and other goods) means that the website terms and conditions are usually unilaterally imposed by the owner of the website in question and will not be negotiated and not physically signed by the other party.[3] The original principles of contract law are out-dated and it is clear that at the time these principles were formulated the world was run on paper and ink. Certainly, the meeting of minds in cyberspace was never envisaged and the validity and effect of electronics in commercial communication was never contemplated.[4] The use of electronic communications for the purposes

[1] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, Part I, Resolution 51/162 adopted by 85th General Assembly at a plenary meeting (A/51/628) (December, 1996) available at www.uncitral.org/en-index.html.
[2] S Eiselen 'Principles of the UNECIC' in *Sharing International Commercial Law across National Boundaries*, (2008) at 106.
[3] T Pistorius 'Formation of internet contracts: Contractual and security issues' (1999) 11 *SAMLJ* at 286.
[4] T Pistorius 'From snail mail to e-mail - a South African perspective on the web of conflicting rules on the time e-contracting' (2006) 39 *CILSA* at 179.

of trade posed unexpected and complex legal problems and it was clear, as early as the early 1980s, that there was a need for legal redress of these issues on both local and international levels.[5]

(b) Aim of the study

The focus of this study is the extent to which the legal barriers to electronic contract formation and related e-commerce issues have been effectively addressed by legislative intervention in South Africa. This work also intends to address the effectiveness of the South African Electronic Communications and Transactions Act (hereafter referred to as the ECT Act) [6] in regulating e-commerce in comparison to the legal position in the United States of America (US). It will also try and answer whether South Africa can accede to the United Nations Conventions on the use of Electronic Communication in International Contracts [7] (hereafter UNECIC). Various aspects will be looked into with regard to contract formation such as time and place, validity of electronic contracts, electronic signatures, attribution of electronic data messages and signatures, automated transaction, as well as select aspects of e-jurisdiction.

The legal issues will be examined from a South African standpoint and are reviewed on a comparative basis with international Model laws and Conventions and laws of the US. In carrying out the aims of this research it was decided that this study would only be limited to the legal issues as outlined above. To go further than these issues, would be beyond the scope of the guidelines as proposed by the United Nations Commission on International Trade (UNCITRAL) Model Law [8] and the UNECIC (2005)[9].

[5] Ibid.
[6] Act 25 of 2002.
[7] UNCITRAL'Convention on the Use of Electronic Communications in International Contracts'. Resolution 60/21 adopted at the 60th session of the General Assembly (December 2005) available at http://www.uncitral.org/en-index.html (accessed on the 1st March 2015).
[8] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, Part I, Resolution 51/162 adopted by 85th General Assembly at a plenary meeting (A/51/628) (December, 1996) available at www.uncitral.org/en-index.html.

The legal issues addressed in this dissertation have a direct bearing on commercial transacting on the internet and are of great importance.

(c) Outline of the study

Chapter II explains the technology that forms the basis for e-commerce. The topic is introduced by a discussion of the historical development of the internet. The technology used to generate the data messages and the transmission thereof as well as the creation of electronic signatures (digital signatures) will also be discussed. This technical background forms a basis to illustrate that legal challenges have been created by e-commerce and with it, legal uncertainties have materialised.

Chapter III of the study examines international law instruments such as (a) the UNCITRAL Model Law on E-commerce which is based on the functional equivalence principle; and (b) the UNCITRAL Model Law on Electronic Signatures,[10] which is, in turn, based on the 'technological neutrality' principle and the party autonomy principle, which have helped forge the South African Electronic Communication and Transactions Act, (ECT Act), and (c) the UNECIC, which came into effect after the ECT Act and which has created a firm platform for further legal debate.

Chapter IV deals with the common law principles of the law of contract and the legal position as it was prior to legislative reform. The requirements for contract formation (offer and acceptance) formalities, attribution and automated transactions are discussed. Many of the principles to be dealt with in this section are still applicable and were not amended by

[9] UNCITRAL'Convention on the Use of Electronic Communications in International Contracts'. Resolution 60/21 adopted at the 60th session of the General Assembly (December 2005) available at *http://www.uncitral.org/en-index.html* , (accessed on the 1st March 2015).

[10] UNCITRAL Model Law on Electronic Signatures. Resolution 56/80 adopted by the 87th plenary meeting of the General Assembly (December, 2001) available at *www.uncitralwww.uncitral.org/en-index.htm*.

the ECT Act. The difficulties in applying common-law principles to electronic commerce are highlighted throughout the chapter.

Chapter V addresses the legislative development and history in enacting the ECT Act in South Africa. The validity and enforceability of data messages, writing and signature requirements, and time and place of receipt of a data message are addressed. This section is concluded by brief comment on e-jurisdiction issues and the extent to which the ECT Act conforms to international law and practice as expounded in Chapter III.

Chapter VI of this dissertation contains a comparative study of the position obtained in the US on electronic communications law and how it deals with the same legal problems addressed in this work. The chapter will commences with an overview of the sources of law that govern conduct within the US. The chapter then deals with the law that regulates contracts in the offline environment and then further examines the different pieces of legislation, namely: the Uniform Computer Information Transactions Act of 2002 (UCITA)[11]; the Uniform Electronic Transactions Act of 1999 (UETA)[12]; and the Electronic Signatures Act of 2005 (E-sign)[13] that impact upon the current legal regime with specific emphasis on the online environment. It will conclude with a short discussion on online e-jurisdiction and how the US courts deal with this vexatious legal issue.

In Chapter VII of this work, the South African legal position is summarised and critically analysed with reference to US law and the UNECIC. In this chapter a critical appraisal is made of the provisions of the ECT Act on contract formation. The South African position on electronic signatures and the attribution of data messages are also to be reviewed. This chapter also assesses whether South Africa is ready to accede to the UNECIC and proposed amendments to the ECT Act. This is followed by a

[11] Uniform Computer Information Transaction, 1999.
[12] Uniform Electronic Transactions Act, 1999.
[13] Electronic Signature in Global and National Commerce, 30 June 2000.

short discussion on the African Union (AU) African regional initiative to regulate e-commerce.

Finally, Chapter VII concludes by recommending several amendments to the ECT Act for the effective regulation of e-contract formation in South Africa.

CHAPTER II: TECHNOLOGICAL BACKGROUND TO LEGAL PROBLEM

(a)What is the internet?

Over the years different South African writers and jurists in the information technology field have attempted to formulate a universally acceptable definition of the internet. Smith defines the internet as: '[a] network of computer networks'.[14] This definition, although crisp, does not fully describe the internet as it fails to encompass both its physical and technical applications.

The writers, Benzine and Garland, on the other hand, defined the internet as: 'a worldwide network of networks that are connected to each other into one single logical network, all sharing a common addressing scheme'.[15]

This definition also does not escape serious criticism, as its second part is misleading. It falsely creates the impression that the internet uses one single platform of communication when, in fact, there are diverse computer networks that communicate on different platforms within the same context of the term.[16]

The distinction between a computer platform and a network is that a platform is usually a format of communication whereas a network refers to the physical aspect of the infrastructure facilitating the communication of data messages. Schneider extended the definition and defined the internet as: 'a large system of interconnected computer networks that spans the globe which can be used by people throughout the world by means of electronic

[14] G Smith *Smith's Guide to the Internet* (1997) at 1.
[15] Benzine & Garland *Accessing and Using the Internet* (1995) at 26.
[16] S Snail 'Electronic Contracts in South Africa - A comparative analysis' (2008) 2 *JILTL* at 1, available at http://go.warwick.ac.uk/jilt/2008_2/snail (accessed 13 January 2009).

data communication'.[17] Such electronic data communication comprises of electronic mail, online versions of newspapers, magazines, academic journals, SMSs and e-books.

The most legally comprehensive definition of the internet can be found in the first edition of Buys' work, namely:

> 'an integrated computer network, through which users, by means of communication devices, are connected to each other by means of TCP/IP (the development of the protocol can largely be attributed to Vint Cerf and Robert Khan who co-designed the TCP/IP, the process with which data moves around the internet) family Protocols.'[18]

This is the most favourable definition as it encompasses every aspect of the internet - both its physical and technical attributes - and it seems consistent with the definition of 'internet'[19] as found in Section 1 of the ECT Act.

Telkom SA v Napa Maepe and two others[20] was the first South African ruling where the internet was described and defined. Judge Du Plessis gave an apt 'technological layman's' overview of the workings of the network by his definition of the internet as 'a number of computers linked together to share information'.

The internet can also be defined as, 'a collection of packet-switching computer networks that are glued together by software protocols such as the

[17] G Schneider 'Electronic Commerce' (2006) at 55.
[18] R Buys 'Cyberlaw @ SA: The law of the Internet in South Africa' (2001) at 12.
[19] '[An] interconnected system of networks that connect computers around the world using TCP/IP and includes future version thereof.'
[20] *Telkom SA Limited v Napa Maepe, South Africa Telecommunications Regulatory Authority and The Internet Service Providers' Association* (TPD) unreported case, case number 258940/97.

Transmission Control Protocol and the Internet [P]rotocol, respectively known as TCP/IP'.[21]

(b) Historical overview of the development of the internet

In the mid-1960s, the Department of Defense of the United States government decided to set up the Advanced Research Project Agency (ARPA). Its main objective was to test and experiment with a new technology called 'packet switching' for a project that was initially aimed at the formation of a data network, to curb data losses that could occur in the case of a nuclear attack against the US.[22] This would be done by using computer link-ups via the different types of communication available at the time. During the following two decades the evolving network was used primarily by academic institutions, scientists and the US government.[23]

The appeal the network had to these bodies is obvious; it allowed disparate institutions to connect to each other's computing systems and databases as well as share data via e-mail and other communication platforms. In 1979, Tom Truscott and Jim Ellis (Duke University, Durham, NC), along with Steve Bellovin (University of North Carolina, Chapel Hill), set up a system for distributing electronic newsletters originally between Duke and the University of North Carolina using dial-up lines and the 'Unix-to-Unix Copy Program' (UUCP).[24]

[21] A Alhadeff & M Cohen 'Functionality of Value-added Network Service and their Liability' (2004) in R Buys(ed), Cyberlaw @ SA II at 232.
[22] K Giridhar 'Packet Switched Data Network and it Evolution' (2013) in *UNESCO* – available at http://www.eolss.net/sample-chapters/c15/e1-25-01-02.pdf (accessed on the 10 June 2014) as well as A Archbold *Are Contracts Concluded on the Internet Valid and Enforceable?: An Analysis of the Law Applicable to Contracting on the Internet* (Unpublished LLM thesis University of Cape Town 1999) at 5.
[23] Ibid.
[24] D A Wheeler 'The Most Important Software Innovations' (2008), available at *http://www.dwheeler.com/innovation/innovation.html*. (accessed on 10 February 2009).

This was the beginning of the informal network (USENET) which supported online forums on a variety of topics, and it took off once Usenet was bridged with the Advanced Research Projects Agency Network (ARPANET).[25] Usenet was to become the prototype for what is known today as the World Wide Web (WWW). Over the years, it was tested and improved. In 1989, two commercial e-mail services, namely MCI Inc and CompuServe became the first e-mail service providers to supply private persons and companies with e-mail services as we know them today - although in its simplest form.[26]

(c)Data transmission over the internet

The Transmission Control Protocol/Internet Protocol (TCP/IP) communication procedure, mentioned earlier, allows computers connected to networks to link with each other by transmitting data packets to one another to create a chain of communication. Once the sending device transmits a data message via the internet, the TCP breaks down the big data packet into small data transmission packets and puts them into digital envelopes in a particular sequence that state the sender's and recipient's addresses.

The IP then adds a header to the sequence in which it writes information about what routes to take to get to the recipient. This intertransmission of digital envelopes takes place on virtual high capacity information highways called 'routers'. The packets are then transmitted from one router to the other (the distance and time of a message is dependent on what routers it will have to take and the level of network activity) much the same way an

[25] Ibid.
[26] Martin Campbell-Kelly 'The History of the Interent' (2013) at http://www.palgravejournals.com /jit/journal/v28/n1/full/jit20134a.html (accessed on 27 October 2015).

envelope which travels between postal sub-stations before reaching its recipient.[27]

On arrival at the recipient's server, the IP/TCP protocol reverses the process by assembling the small data packets to its full original size. The data package and the message is then fully restored and readily accessible.[28]

The prevailing uncertainty regarding authenticity, integrity and accuracy of electronic messages resulted in the development of electronic signatures. Blyth defined an electronic signature as, 'any letters, characters or symbols manifested by electronic or similar means and executed or adopted by a party with an intent to authenticate a writing', or 'data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication'. [30]

Several methods exist to electronically sign documents which vary from very simple methods, such as the insertion of a scanned signature, to very advanced methods using encryption technology called cryptography. For the purposes of this discussion, only cryptography, biometrics and digital signatures will be dealt with.

Cryptography is the study and practice of hiding the contents of a message, used from ancient times to the present.[31] Encryption on the other hand is the electronic process whereby the message (in this case an electronic data message) is converted by way of a mathematical calculation into a series of coded numbers and symbols that can successfully hide the contents of the original message and can only be restored to its original form

[27] K Giridhar op cit note 23 at 3.
[29] Ibid.
[30] Blyth S E 'Digital Signature Lawof the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) 11 Richmond Journal of Law & Technology 2 at 1, available at http://law.richmond.edu/jolt/v11i2/article6.pdf (accessed on 18 March 2012).

once the decoding process has been completed with the relevant decoding code or key.[30]

For instance, the sentence, 'She sells shells by the sea-shore' sent by e-mail to a specific recipient could be encrypted to 'ET8494UDKDI797H85K23G' and the said encrypted message can only be read if the recipient of the message has the relevant key and relevant decoding software.

There are two mathematical families that can disguise a data message in digital form, namely symmetric cryptography systems and asymmetric cryptography systems. Symmetric (secret key) cryptography has been in use for a thousand years and includes any form where the same key is used both to encrypt and to decrypt the text involved. One of the simplest forms, also known as the Caesar cipher, conceals messages by shifting the alphabet in so many places in one direction or another.[31]

A variation of this system involves an arbitrary ordered alphabet of the same length as the one used for the plain message.[33] In such an instance the key will be a long sequence of numbers such as 2, 4, 7, 9, 11, 12 . . . indicating the A would map to R, T to F, V to T, and so on, or a less ingenious scheme involving letters from a sentence of a particular novel or poem.[34]

The above scheme has proved to be ludicrously weak and modern schemes use complex computer-generated mathematical algorithms. Modern schemes based on difficult mathematical problems are very effective and reliable in concealing the encrypted message.

---

[32] Mason S 'Electronic Signatures: The Technical and Legal Ramifications' (1999) Computer and Law at 37.
[33] M Mactaggart 'Introduction to Cryptography, Part 2: Symmetric Cryptography' (2001) at 1, available at *www.ibm.com/developerworks/library/s-crypt02.html* (accessed on the 12 February 2010.)
[34] Ibid.
[35] Mason op cit note 32 at 26.

The effectiveness of this system depends on the strength of the algorithm and the length of the key number. The longer the key number the better the strength of the security. For instance, it would take a super computer 2 885 years to decipher a 56-bit key.[35]

Unlike asymmetric cryptography (which will be discussed later) where there is a public element to the process and where the private key is almost never shared, symmetric cryptography normally requires the key to be shared and simultaneously kept secret within a restricted group. [36]

So it is simply not possible for a person to view the encrypted data with a symmetric cipher without access to the original key. The disadvantage of this system is that when the key falls in the wrong hands, the entire message and security is compromised. This makes clients and e-commerce providers reluctant to use symmetric cryptography because first, they would have to send out a huge number of keys and secondly, once the said keys have fallen into the wrong hands, the message's authenticity cannot be guaranteed.

Thirdly, it places a huge burden on the e-commerce provider to maintain and keep a good and secure record system of keys given to clients. [37]?

[36] Mactaggart op cit note 33.
[37] Mason op cit note 32 at 32.

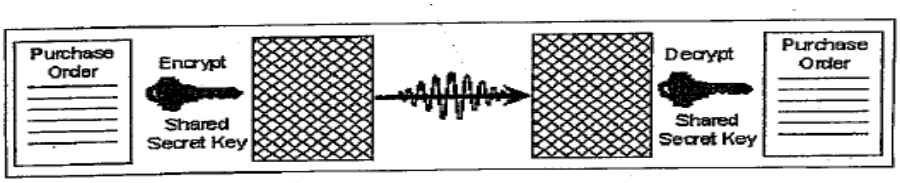


Figure 1: Symmetric Key [36]

Asymmetric cryptography (public key) (as per Figure 1 above) , on the other hand, does not require the same secret for both encryption and decryption which, in the case of symmetric cryptography, can make its security-enabling feature vulnerable to unauthorized access.[37] Mason distinguishes asymmetric cryptography between private public key and trusted third party technologies.[38]

The private public key asymmetric cryptography generally uses two mathematically related keys that are used to work together in such a way that a plain text encrypted with the one key can only be decrypted with the other. One of these keys, the private key, will be kept private by one individual and the second key, the so-called public key, needs to be made public as widely as possible.

[36] S Nagalingam *Comparative Review of Electronic Contract* (2000) (UP-Thesis) at 23.
[37] Mactaggart op cit note 33.
[38] Mason op cit note 32 at 38.
[41] Nagalingam op cit note 37.
[42] Ibid.

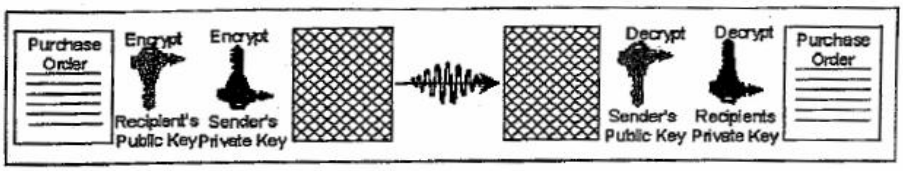


Figure 2: Asymmetric Key [41]

Symmetric cryptography unfortunately has its vulnerabilities. In contrast, it is important to mention that asymmetric cryptography has both strengths and weaknesses. The most important of these weaknesses being (a) impersonation and (b) that the technology is much slower than symmetric cryptography.[42] Mactaggart also mentioned that both asymmetric and symmetric cryptography techniques, if used in conjunction with each other, can be very beneficial and complementary to give an elegant and efficient, extreme high-level security verification system.

The next point to be discussed is the digital signature. Christianson and Mostert defined it as follows: 'A digital signature is a data item which accompanies a digitally encoded message and which can be used to ascertain both the originator of the message and the fact that the message has not be alerted since it left the originator'.[43] Digital signatures, as contemplated, involve the use of a private and public key pair that are issued by a Certification Authority (CA).[44]

A CA is a third party which can be a private or public body that acts to certify the data flow between a person and their private key and who verifies the identity of the person requesting the key pair. The private key, on the other hand, is distributed only to the key owner whereas the public key can

[43] M Mactaggart 'Introduction to cryptography, Part 3: Asymmetric cryptography' (2001) at 1, available at *www.ibm.com/developerworks/library/s-crypt03.html* (accessed on 12 February 2010).

[44] G Christianson & W Mostert 'Digital signatures' (2000 May) 28 *De Rebus* at 34.

be found by accessing a CA's public database. The trusted CA guarantees the authenticity of the public key. [45]

The CA issues an electronic authentication certificate that identifies the CA and the user of the certificate, it also contains the subscriber's public key and is digitally signed with the CA's private key. The information contained in the certificate may include the level of inquiry carried out before the certificate was issued. Another important aspect of the digital signature is that messages which are sent through insecure communication channels certify that the data sent and received by the recipient is that of the sender.[46]

Digital signatures are the equivalent of the traditional handwritten signature and, if properly used, are even more difficult to forge than the traditional handwritten signature. They are also important to prove non-repudiation of agreements as they may, in certain instances, even use a time stamp. The use of encryption technology to create 'digital signatures' makes it possible to verify that: (a) persons exchanging documents electronically are who they say they are; (b) the message exchanged between them has not been altered; (c) the sending party cannot deny having sent them; and (d) that the messages were sent by the parties. Encryption therefore provides electronic communication with authentication, integrity, non-repudiation and confidentiality.[47]

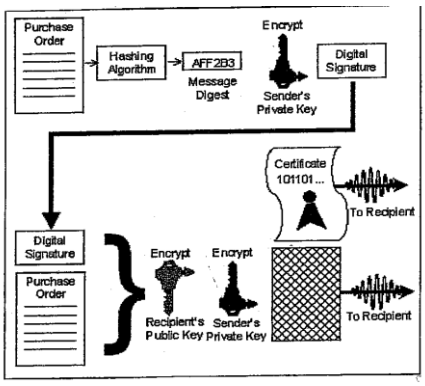
The electronic document is run through an algorithm known as a hashing algorithm prior to it being sent as represented below in Figure 3.

[45] J Coetzee 'The Electronic Communication and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 *SLR* at 513.
[46] M Erdle 'Contracting on-line: Electronic Creation of Effective Contracts' availbale (accessed on 3rd January 2008). Also see the views of J Angel 'Why use digital signatures for electronic commerce?' (1999) *JILT* 2 at 4.

The hashing algorithm then produces a 'message digest' which is a unique hexadecimal value.[48]

The message digest is then encrypted using the sender's private key by creating an electronic file which will, at a later stage, be decrypted with the sender's public key. The resulting file is then referred to as the 'digital signature'. The digital signature is then once again encrypted along with the original data message and the resulting encrypted file is sent with the sender's certificate in a normal data transmission.[49]

Figure 3: Hashing Algorithm



[47] J S Forster 'Electronic Contracts and Digital Signatures – The Future is Closer Than You Think' (2000) 3, available at *www.corinball.com/articles/art-digitalcontracts.html* (accessed 12 February 2009).
[48] Nagalingam op cit note 37.
[49] Ibid.

(d) Legal challenges created by the use of electronic data communication in contract negotiation

The use of electronic data messages for both commercial and non-commercial purposes has been on the steady increase over the years through the invention and evolution of various data communication devices. Electronic commerce is no longer a predication; it is an economically significant reality as the internet is the world's fastest growing commercial marketplace.[50]

There are in principal four different ways of e-contracting but the first and most important method of internet contracting is similar to a negotiation of one or more infrequent transactions by exchange of letters and documents – known as e-mail contract formation.[51] In this method the parties can exchange e-mail messages and even attachments setting out the terms and conditions of their contract in detail. This is quite similar to offer and acceptance between the parties by way of letter or faxes.[52] The second method, similar to contract formation via a mail order, is known as contracting on the World Wide Web (www). In this method, one party maintains the website at which goods and services are advertised. The prospective buyer accesses the website and then completes an electronic form whereby goods or services are ordered from the seller.[53]

The third method is where the parties trade under the framework of an Electronic Data Interchange agreement (EDI). The EDI can be defined as 'computer-to-computer transmission of data in a standardized format'.[54]

[50] J Loetz & C du Plessis 'Electroniese Koopkontrakte: 'n Tegnologiese Hemel of Hel (deel-1)' (2004) *De Jure* at 1.
[51] D Kidd Jr & W Daughtery Jr 'Adapting Contract Law to Accommodate Electronic Contracts' (2000) 26 *RCTLJ* at 232.
[52] Loetz & du Plessis op cit note 50 at 4.
[53] Pistorius op cit note 3 at 286.
[54] UNCITRAL Model Law on E-Commerce op cit note 5.

Such EDI enables businesses to exchange documents over either the internet or their private networks.[55] Private EDI networks are used by large businesses when buying goods and are preferred by smaller businesses as it reduces costs.[56] This is the primary electronic commerce medium; it is only applicable and valid between the contracting businesses that have assented to it.[57]

The final and the fourth method of contracting electronically is when users, while chatting online in a virtual chat-room, make offers and accept offers that result in valid and binding contract formation.[58] The question may be raised whether an electronic mail, SMS message or other form of data communication, which is a form of data message, could be sufficient to signify a party's intent to be contractually bound.

The ECT Act, which has been guided by the UNCITRAL Model Law, has now entrenched the position in South Africa that digitally negotiated and electronically signed contracts are fully valid and enforceable.[59]

It is clear that the complexity of the technological aspects of electronic contract formation is far from the traditional methods of contract formation as it has brought with it new forms and ways to communicate offers and acceptance. It has also created new methods of electronically signing documents which not only fulfil some of the traditional functions of a signature but have also raised the value of the signatures.

[55] Ibid.
[56] Jae Shim, A A Qureshi, J G Siegel & R M Siegel *The International Handbook of Electronic Commerce* (2000) at 141.
[57] Nagalingam op cit note 37 at 6.
[58] Loetz & du Plessis op cit note 50 at 4.
[59] Section 12 and Section 13 of the ECT Act.

The said new developments in technology have clearly created new legal issues that will be examined in closer detail in the following chapters.

CHAPTER III: INTERNATIONAL RESPONSES TO LEGAL PROBLEMS CREATED BY ELECTRONIC CONTRACTS

(a) Introduction to international response

The transnational nature of electronic commerce and its disregard for traditional jurisdictional borders, together with the lack of domestic laws dealing with electronic commerce, created legal uncertainty in most jurisdictions.[60] Although businesses are adapting to the electronic environment, legal rules continue to stipulate that certain transactions or documents are to be in writing.[61] This was seen as an impediment to the development of electronic commerce and it was soon realised by many countries that accommodation of the electronic medium as a legally acceptable medium would be essential in years to come.[62]

In response to this lacuna UNCITRAL and governments of various countries called for the drafting of internationally recognised uniform electronic transactions legislation.[63] In 1985, UNCITRAL drafted and adopted the 'Recommendation on the Legal Value of Computer Records'.[64] At the time of its drafting, it was seen as a document, but since the development of the Model Laws one would rather call it the 'policy document' which laid the basis for the harmonization of electronic communications laws on an international level.

---

[60] UNCITRAL secretariat 'Electronic Commerce and International Legal Harmonisation: Time to go beyond the Functional Equivalence?' (2003) Paper prepared by members of the UNCITRAL secretariat and presented at the *ICT and E-Business Strategies for Development High-level Regional Conference for Transition Economies* Geneva, 20-21 October 2003.

[61] Ibid

[62] A Davies 'The Development of Laws on Electronic Documents and E-commerce Transactions' (2008) *Library of Parliament (Canada)* at 1.

[63] S Pitiyasak 'Electronic Contracts: Contract Law of Thailand, England and UNCITRAL compared *CTLR.* (2003). Retrieved from WESTLAW online database (COMPTLR 9 (1), 16-30).

[64] UNCITRAL 'Recommendation on the Legal Value of Computer Records'. Resolution 40/71 adopted by 40th General Assembly (11th December, 1985) as reproduced in *United Nations Commission on International Trade Law Yearbook, 1985*,Vol. XVI, Part one, D.

In 1996, the United Nations adopted the UNCITRAL Model Law on E–Commerce[65] to assist countries in drafting and enacting laws to give legal recognition to electronic contracts as well as the UNCITRAL Model Law on Electronic Signatures[66] in 2001. The UNCITRAL Model Law on Electronic Commerce[67] was adopted on 12 June, 1996 and aimed to create a more certain legal environment for what had become known as 'electronic commerce' by providing a tool for states to enhance their legislation of paperless communication and storage of information.[68] Its main purpose is to give effect to the Recommendation on the Value of Computer Records as adopted by the UNCITRAL in 1985.[69] The purpose of the Model Law was to offer national legislators a set of internationally acceptable rules for the enhancement of legal certainty.[70] The principles expressed in the Model Law were also intended to be of use to individual users of electronic commerce in drafting solutions for contracts that are concluded electronically.[71]

The UNCITRAL Model Law on E-Commerce provides a functional equivalent for terms like 'writing', 'signature' and 'original' in electronic form. This was followed by the UNCITRAL Model Law on Electronic Signatures and the United Nations Convention on the use of Electronic Communications in International Contracts[72] which sought to harmonise the provisions of the two Model Laws to form an international law instrument regulating international electronic cross-border contracts. One must mention the interesting fact that the UNCITRAL Model Law on E-Commerce, the UNCITRAL Model Law on E-Signatures as well as the United Nations Convention on the use of Electronic Communications in International

[65] UNCITRAL Model Law on E-Commerce op cit note 8.
[66] UNCITRAL Model Law on Electronic Signatures op cit note 10.
[67] Ibid.
[68] T Pistorius, 'Contract Formation: A Comparative Study of Legislative Initiatives on Select Aspects of Electronic Commerce' (2002) 25 *CILSA* at130. Also see C Glatt (1998) 'Comparative Issues in the Formation of Electronic Contracts' (1998) 1 *JLIT* 6 at 57.
[69] See official records of the UN General Assembly, UNCITRAL Supplement No. 17 (A/40/17) Chapter VI section B (1985).
[70] Guide op cit note 8 par 2 at 16.
[71] See also preamble of the Model Law op cit note 6.
[72] UNCITRAL op cit note 70.

Contracts (UNECIC) are not legally binding upon South Africa although the first two instruments have been influential in the drafting of the ECT Act and have formed the legal basis for this Act. Scholars will note that there are remarkable consistencies with what is proposed in the UNCITRAL Model Laws and the ECT Act. The Model Laws have served both to educate lawmakers about the legal ramifications of electronic transactions and to provide a framework for any country wishing to draft electronic commerce legislation.

A comparative study of electronic transactions legislation from different countries shows that there is a close similarity between them and the Model Laws as they are mostly based on the Model Laws.[73] Although our South African courts are not bound to the provisions of the UNCITRAL Model Laws, by virtue of the Constitution,[74] it gives a clear instruction to an adjudicator to interpret legislation in a manner that is consistent with international law[75] such as the UNECIC.[76] It is also interesting to note that the Constitution further provides for consideration of foreign law, which would include foreign case law.[77]

[73] Malaysia enacted the Digital Signature Act in 1997; Singapore passed the Electronic transactions Act in 1998; India passed the Information Technology Act in 2000; the United Kingdom passed the Electronic Communications Act in 2000; the United States of America passed the UCITA and UETA. Also see Baker & McKenzie, 'Singapore E-commerce Legislation and Regulations' *Global E-Commerce Law*, available at *www.bmck.co/ecommerce/malysia.html* (accessed on 1st March 2014).

[74] The Constitution of the Republic of South Africa Act 108 of 1996, s.231 (4) – 'Any international agreement becomes law in the Republic when it is enacted into law by national legislation; but a self-executing provision of an agreement that has been approved by Parliament is law in the Republic unless it is inconsistent with the Constitution or an Act of Parliament.'

[75] The Constitution of the Republic of South Africa Act 108 of 1996 , s.233 – 'When interpreting any legislation, every court must prefer any reasonable interpretation of the legislation that is consistent with international law over any alternative interpretation that is inconsistent with international law.'

[76] UNCITRAL 'Convention on the Use of Electronic Communications in International Contracts' Resolution 60/21 adopted at the 60th session of the General Assembly (December 2005) available at *http://www.uncitral.org/en-index.html*,(accessed on 1 March 2015)

[77] The Constitution of the Republic of South Africa Act 108 of 1996, s.39.

(b) Recommendation on the legal value of computer records by the United Nations Commission on International Trade (UNCITRAL)

In 1985, the eighteenth session of UNCITRAL had before it a report compiled by the secretariat entitled 'Legal value of computer records'.[78] The report's main conclusions were that, on a global level, there were fewer problems than expected with the use of data stored on computers as evidence in criminal prosecutions.[79] It was, however, noted that a more serious legal obstacle was posed by the use of computers and, in particular, computer-to-computer communication in international trade. Most legal difficulties arose out of the legal requirements that documents had to be signed or be in paper form.[80]

After discussion of the report, the Commission adopted a recommendation, which expresses some of the principles on which the

[78] Recommendation on the legal value of computer records by the United Nations Commission on International Trade (UNCITRAL) (A/CN.9/265)
[79] Preface to UNCITRAL Resolution 40/71 op cit note 70 at 1.
[80] Ibid.

model laws are based and founded.[81] These recommendations were accordingly endorsed by the General Assembly[82] and read as follows:

> '…. Calls upon Governments and international organizations to take action, where appropriate, in conformity with the Commission's recommendation so as to ensure legal security in the context of the widest possible use of automated data processing in international trade.'.

As it can be noted from the simple wording of the UNCITRAL'S recommendation, it is clear that as early as 1985 many countries had already found that the use of electronic data as a form of communication in the commercial realm was very popular. The question regarding validity and enforceability of using such electronic communication for legally relevant acts also highlighted the problems it could create as these recommendations failed to address some of the critical legal aspects of electronic communication.

This policy document was instrumental in the development of electronic commerce law. Notwithstanding, the UNCITRAL

[81] The United Nations Commission on International Trade Law, 'Considering at the same that there is no need for a unification of the rules of evidence regarding the use of computer record in international trade, in view of the experience showing that substantial differences in the rules of evidence as they apply to the paper-based system of documentation have caused so far noticeable harm to the development of international trade,
1. Recommends to Governments:
…. (b) to review legal requirements that certain trade transactions or trade related documents be in writing whether the written form is a condition to the enforceability or to the validity of the transaction or document, with a view to permitting, where appropriate, the use of electronic authentication;
(c) to review legal requirements of handwritten signature or other paper-based method of authentication on trade related documents with view to permitting, where appropriate, the use of electronic means authentication;
(d) to review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services which acquired and established the necessary procedures.
2. Recommends to international organizations elaborating legal text related to trade to take account of the present Recommendation in adopting such text and, where appropriate, to consider modifying existing legal texts in line with the present Recommendation'

[82] UNCITRAL Resolution 40/71 op cit note 70, para 5(b) of 11 December 1985.

Recommendation on the Legal Value of Computer Records was the first attempt by countries to fill the *lacunae* that were created by the advent of electronic communication in the twentieth century.

It should be noted that the nature, type and magnitude of statutory obstacles to electronic commerce varied greatly in different legal systems. That diversity in itself called for a greater degree of flexibility in introducing the necessary amendments to existing laws.[83] These considerations clearly spoke against the adoption of an international convention at that time; however, it would take another ten years, under pressure of the emerging commercial activity on the internet, for the same body to revisit the said recommendations and to adopt those of the UNCITRAL Model Law on Electronic Commerce.[84]

(c) The United Nations Commission on International Trade's (UNCITRAL) Model Law on Electronic Commerce

(i) Objectives and sphere of application of the Model Law

After the UNCITRAL had made its initial recommendations, it became clear that it would have to go the route of internationally harmonising electronic commerce principles. This was seen as the logical approach for dealing with the legal implications of technological developments as a result of 'markets migrating from geographic space to cyberspace'[85] and the fast pace at which technological changes were occurring. Impetus to this movement was also given by the elevation of electronic commerce to a high position on the

[83] UNCITRAL 'Electronic Commerce and International Legal Harmonisation: Time to go Beyond the Functional Equivalence?' (2003). Paper presented at the *ICT and E-Business Strategies for Development* at the High-level Regional Conference for Transition Economies Geneva, 20-21 October 2003 at 2.
[84] Ibid.
[85] Stephen. Kobrin 'Economic Governance in an Electronically Networked Global Economy' in R Hall & T Biersteker (eds) (2002) *The Emergence of Private Authority: Forms of Private Authority and Their Implications for Global Governance* at 11. (also available at http://www-management.wharton.upenn.edu/kobrin/Research/revision%201.pdf)

domestic policy agendas of many countries. A number of international organisations became concerned with trade facilitation in the online world and how commercial law could be harmonised or unified to deal with e-commerce.[86]

It is against this background of increasing legal uncertainty and the exponential increase in international e-trade that the UNCITRAL established a Working Group to draft legal rules on electronic commerce.[87]

The other objectives of the Model Law were to facilitate, rather than regulate,[88] the use of electronic communication and to provide equal treatment to users of paper-based documentation (also known as the functional equivalent approach) and also users of electronic-based documentation or alternative methods of communication to foster economic growth and efficiency of international trade.

The UNCITRAL Model Law provides a basic legal framework for electronic commerce enablement and regulation. Its focus was to facilitate rather than regulate electronic commerce and it was needed at the time to help with the interpretation of existing international law, conventions and other instruments as far as they impeded on e-commerce at that time.[89] Through the application of the principle of functional equivalence, the UNCITRAL Model Law advocated, as a first step, the adaptation of existing legal principles to the electronic commerce environment. [90]

---

[86] G Hermann 'Establishing a Legal Framework for Electronic Commerce: The work of the United Nations Commission on International trade (UNCITRAL)' (1999) Presented at WIPO International Conference on *Electronic Commerce and Intellectual Property* 14th – 16th September 1999, Geneva at 2.

[87] Glatt op cit note 69 at 57.

[88] Hermann op cit note 87 at 3.

[89] Glatt (1998) op cit note 69 at 58.

[90] For some perspective it is necessary to cite from the UNCITRAL Resolution 51/162 at op cit note 5 which states:

'1.Believing that the adoption of the Model Law on Electronic Commerce by the Commission will assist all States significantly in enhancing their legislation governing the use of alternatives to paper-based methods of communication and storage of information and in formulating such legislation where none currently exists, ;

The decision to draft the Model Law not only intended to remedy the disadvantages posed by the lack of uniformity of domestic legislation of the different member states, but it also intended to remedy international trade and the interpretation of international legal instruments that enhanced the disparities of the modem communication techniques between first world and third world countries.[91] It was also a response to the fact that much of the existing legislation governing the communication and storage of information did not contemplate the use of electronic commerce and imposed, or implied, restrictions on the use of modern means of communication by prescribing the use of 'written', 'signed' or 'original document'. [92]

In May 1997 the Guide to Enactment was published.[93] The aim of publishing the Guide to Enactment (hereafter referred to as the Guide) was to summarise the consensus of the discussion by the commission and the working group and to provide explanatory notes to assist governments who wanted to follow the Model Law when enacting their own electronic communication legislation.[94] The Guide was also vital to states that had a limited or no familiarity with the type of communications technique considered in the Model Law.[95]

In preparing and adopting the Model Law, the UNCITRAL was mindful of the fact that such a Guide would be necessary to deal with some of the aspects that could not be addressed adequately due to conflicting legal

---

2. Expresses its appreciation to the United Nations Commission on International Trade Law for completing and adopting the Model Law on Electronic Commerce contained in the annex to the present resolution and for preparing the Guide to Enactment of the Model Law;

3. Recommends that all States give favourable consideration to the Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;'

[91] UNCITRAL Resolution 40/71 op cit note 70 at 17.
[92] Davies op cit note at 63 at 2.
[93] Ibid.
[94] Pistorius op cit note 3 at 180.
[95] Guide op cit note 8 at 15.

rules of different states that could only be explained by means of a guide. Therefore, it is important to note that the Guide has been drafted from the 'travaux preparatoires' with the idea of being helpful to users of electronic communications as well as scholars in the field.[96]

In the Guide, the Model Law is divided into two parts namely, Part 1 (one) that deals with the general 'electronic commerce' provisions.[97] It is the most important part in relation to this treatment. Part 2 (two) briefly deals with 'electronic commerce in specific areas' and it has an open-ended structure to allow for future additions.[98]

The focus of the Model Law is on 'paperless' or 'electronic' means of communication and except for the extent expressly provided it is not intended to alter traditional rules for paper-based communications.[99] Instead, it is intended to provide essential procedures and principles for facilitating the use of modern techniques for recording and communicating information in various types of situations.[100] The term 'electronic contracting' has been used to refer to the formation of contracts by means of electronic communications (or 'data messages')[101] to use the terminology of the UNCITRAL.[102] As such, electronic contracting is a 'method for forming agreements, not a subset based upon any specialised subject matter' [103] of contract law. In fact, the legal principles are the same, the only difference being that the one is concluded on paper or orally, and the other is concluded in electronic form in cyberspace.

---

[96] Ibid.
[97] Glatt op cit note 69 at 58.
[98] Ibid.
[99] Pistorius op cit note 3 at 131.
[100] Blyth op cit note 30 at 5.
[101] 'Data message' as contained in article 2 (a) , is defined message' as:'[a] means [of] information generated, sent , received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail , telegram, telex or telecopy … '
[102] UNCITRAL op cit note 81 at 8.
[103] Kidd & Daughtery op cit note 51 at 215-16.

The Model Law adopts a 'functional equivalence approach' in dealing with electronic commerce. This approach is based on analysing the purposes and functions of paper-based requirements and to determine how these purposes and functions can be fulfilled through electronic commerce techniques.[104]

Article 3, in its interpretation clause, is intended to provide guidance for interpretation by courts and national legislative authorities when drafting and interpreting their own electronic communications law. Paragraph (1) makes it clear that the international origins of the Model Law must not be ignored. In giving effect to the provisions of the Model Law or when interpreting local law with reference to the Model Law, a court should interpret provisions in line with the uniform standards as proposed by the Model Law to enhance uniformity on an international level.[105]

The Model Law lists five non-exhaustive main objectives. First, to facilitate electronic commerce among and within nations; secondly, to validate transactions that have been concluded by new means of technology; thirdly, to promote new technology and encourage the implementation of such technology in trade transactions by facilitating and enabling them; fourthly, to create and promote uniformity and support electronic commerce practices;[106] and fifthly, Article 5 sets out the fundamental principle that electronic communications should not be discriminated against or denied legal effect simply because they are in electronic form.[107] Article 6 sets the basic standard for an electronic document where it is a legal requirement that a document be in writing.[108]

Article 7 of the Model Law acknowledges that a signature is used in the real world to indicate one's approval or verify the contents of the

[104] Davies op cit note 63 at 2.
[105] Guide op cit note 8 para 42 at 30.
[106] Ibid.
[107] Davies op cit note 63 at 3.
[108] Ibid.

document. The article also emphasises that this requirement will be met by an electronic signature if it is a reliable method used to identify the person. Article 7, therefore, gives an electronic signature the same legal effect as an ink signature even if it was not authenticated in a manner peculiar to a paper document.[109] Article 7 also provides broad guidelines instead of specific prescriptions to avoid the risk of tying the legal framework of the Model Law to a given state of technological development.

It is for that reason that the Model Law is called 'technologically neutral'.[110] Article 6 and 7 are intended to take the focus off the mode of communication and place it on the fulfilment of traditional functions and therefore it is 'functionally' equivalent.[111] Gregory supports this approach and states that it is of great significance that the Model Law recognises future developments and applications which are unforeseeable.[112]

While facilitation and promotion of uniformity is a key objective it does not impose any duty on any party to either use, send or receive an electronic data communication.[113] As a result of the 'instrumental approach' [114] adopted by the drafters of the Model Law, important substantive issues such as jurisdiction, aspects of contract formation and performance were not addressed.[115]

The Model Law, however, does not comprehensively address all legal problems created by e-commerce. Issues not addressed adequately were: (a) whether a contract formed between an automated process and a

[109] Blyth op cit note 30 at 6.
[110] Ibid.
[111] W H Thurlow 'Electronic contracts in the United States and the European Union' (2001) *EJCL* (2001, Nov) at 2 available at *http://wwe.ejcl.org/53/art53-1.html* (accessed on the 7 July 2010).
[112] J D Gregory 'Solving legal issues in electronic commerce' (1999) 32 *CBLJ* at 84-104.
[113] Guide op cit note 8 para 43 at 30 as well as Article 4 emphasises party autonomy.
[114] Ibid.
[115] A Phang & D Seng 'The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code' (1999) 7 *IJLIT* 2 at 106. Also UNCITRAL op cit note 81at.6.

natural person has any specific bearing on the rules of contract formation; (b) how the law must deal with data errors and data input errors; and (c) how the law must deal with mistakes and misrepresentations. The legal challenge of creating an internationally acceptable standard for e-commerce, it is submitted here, was in part overcome. This can be evaluated from the influence of the Model Law on laws adopted world-wide for e-commerce on legislation already adopted or being developed.[116]

(ii) Key terms used in the Model Law

Article 2 of the Model Law includes definitions of the key terms namely: 'data message', 'originator', 'addressee', 'intermediary', and 'information system'. These definitions are explained in the Guide. [117]

The definition of a 'data message' includes all types of messages that are generated, stored or communicated in an electronic, optical or digital form. It is notable that the notion of a data message is not limited to communication but is also intended to encompass computer-generated records that are not intended for communication.[118] Therefore, the notion of a message includes a record. The definition of a record must, however, be read together with the term 'writing' as prescribed by Article 6. The Model Law, is cognizant of the fact that there might be future developments in communication techniques, and went a step further in the definition of a data message by adding the words 'or similar means'.[119]

[116] See footnote 10 in the article by J Faria 'E-commerce and international legal harmonisation: Time to go beyond the functional equivalence?' (2004) *SAMLJ* at 532, where he lists countries and their various national codes which in 2003 enacted legislation in line with the objectives of the Model Law. Among them are: Australia, Bermuda, Colombia, Ecuador, India, Ireland, Jordan , Mexico, Pakistan, Philippines, Korea, Singapore, Slovenia, New Zealand Thailand, Venezuela, Jersey, Isle of Man, Hong Kong, some states of the USA, Canada and South Africa.
[117],Guide op cit note 8 par 30 – 40 at 26 – 9.
[118] Ibid para 30 at 26.
[119] Ibid para 31 at 26.

The 'originator', sometimes called 'sender', means the person from whom the data message has been sent and/or the creator thereof. The 'addressee' is the person or the intended recipient of the data message as opposed to the person who might coincidentally come into contact with the message or may unlawfully intercept data message in the course of the communication and re-route it to himself.[120]

Pistorius argued that the 'addressee' may in certain instances also be the 'originator' of data message, for example where the intention was to store the message for future transmission or production or where the originator sent a message to himself for storage.[121]

An 'intermediary' on the other hand, is neither an 'originator' nor an 'addressee'. It is important to note the limited role played by the 'intermediary' and to make a clear distinction between the originator, the addressee and other third parties.[122] The 'intermediary' can be a professional or non-professional party and the intermediaries' duties and relevance is limited to receiving, transmitting or storing data messages on behalf of another person.

The definition of 'information system' is intended to cover the entire data communication infrastructure used for sending, transmitting and receiving data messages. As to what the information system really is, is a factual question. The Model Law does not go in-depth into the matter but an information system may include an electronic mail box or even a telecopier.[123]

[120] Ibid para 36 at 28.
[121] Pistorius op cit note 69 at 131.
[122] Guide op cit note 8 para 39 at 28.
[123] Ibid para 40 at 40.

(iii) Formation and validity of electronic contracts

Article 5 provides for the legal recognition of data messages with emphasis on the principles of non-discrimination of data or media neutrality.[124] To put it differently, it embodies the fundamental principle of 'functional equivalence'.[125] Eiselen describes the functional equivalence approach contained in the Model Law as:

> 'The law has been formed and developed from the point of view of paper-based applications. In order to afford electronic communications the same legal effect and protection as paper based communications, solutions that are functionally equivalent to paper need to be found without trying to imitate paper. This is of relevance especially in respect of formalities and specifically signature.'[126]

Article 5 clearly entrenches the principle that there should be no disparity between data messages and paper-based documents.[127] It should, however, be noted that Article 5 is not intended to override any of the provisions of Articles 6 to 10. It merely indicates that the form in which certain information is presented or retained cannot be given as the only reason for information being denied legal effectiveness, validity or enforceability.[128] The point of departure is that unless there are other legislative stumbling blocks, all electronic communications will be accorded their normal legal consequence depending on the intentions of the parties

[124] Hermann op cit note 87 at 5 .
[125] See also the definition of 'functional equivalent' defined as 'the basic underlying principle of the Model Law'. It involves an examination of the function fulfilled by traditional form requirements (writing, signature, original, dispatch, receipt) and a determination as to how the same function could be 'transposed, reproduced or imitated in a dematerialized environment', op cit note 81at 3.
[126] S Eiselen 'E-commerce and the GISG Formation , formalities and validity' (2002) 6 *Vindobona Journal of International Commercial Law and Arbitration* at 306.
[127] 'Information shall not be denied legal effect, validity or enforce-ability solely on the grounds that it is in the form of a data message'
[128] Guide para 46 at 32.

making said communication.[129] Therefore, if an offer is made with the necessary contractual intent, the offeree can rely on that offer even though it may only be in electronic form.[130]

Article 11, is similar to an entrenchment clause contained in a country's constitution, which makes a clear statement on the value of electronic data messages and the fact that they can be used for valid contract formation.[131] Article 11(1) of the Model Law confirms that unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, the contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.[132] The Guide explains that Article 11 is not intended to interfere with national principles of contract formation but rather to promote international electronic trade by increasing the legal certainty provided for by data messages in Articles 6 to Article 10 and to give legal effect to data messages.[133]

Article 11 goes a step further and also explains the form in which an electronic offer and acceptance may be executed.[134] It allows for the making of an offer in paper-based form with subsequent acceptance in electronic format and vice versa. This is also applicable in instances where both the offer and acceptance are expressed electronically.[135]

One may be of the view that Article 11 is a superfluous duplication of the provisions of Article 5, merely worded differently.

[129] Eiselen op cit 127 at 306.
[130] Ibid.
[131] This Article states that electronic data, in whatever format, will always be of legal value.
[132] See the views of F Ahmad 'Electronic commerce: An Indian perspective' (2001) *International Journal and Information Technology* (9) 2, at 139 as well as Glatt op cit note 69 at 58.
[133] Ibid.
[134] Ahmad op cit note 133 at 139.
[135] Pistorius op cit note 69 at 186.

However, Pistorius[136] is of the view that the said provision is relevant and necessary due to some remaining uncertainties in various countries regarding the validity and enforceability of expressing one's intent (animus) to be contractually bound by means of an electronic data message. This is mainly due to the fact that some offers are expressed and accepted by computers without human intervention, which could cause doubt as to the intent of the parties.[137]

(iv) Electronic writing

Article 6 is intended to define the basic standard to be met by a data message to comply with the statutory requirement that information is retained in writing. Article 6(1) of the Model Law provides that where a law requires information to be in writing, such requirement will be satisfied if it is contained in a data message which is accessible and usable data message for subsequent reference. The requirement that information is retained or presented 'in writing' (or that the information is contained in a 'document' or other paper-based instrument)[138] may be a result of a statute, regulation or common law.

As noted infra the Model Law relies on the functional-equivalence approach which is based on an analysis of the purpose and functions of the traditional paper-based requirements to determine how those purposes or functions could be fulfilled through electronic commerce techniques.[139] Pistorius correctly points out that as stated in Article 6(2), this provision is applicable whether the requirement therein is in the form of an

[136] Ahmad op cit note 133 at 139.
[137] Ibid.
[138] Guide op cit note 8 para 47 at 35.
[139] A Lodder 'Electronic contract and signatures: National Civil Law in the EU will change drastically soon' (2000), Paper presented at the 15th BILETA Conference on 'Electronic Datasets and Access to Legal Information' 14 April 2000, University of Warwick, England at 4.

obligation or whether the law simply provides consequences for the information not being in writing.[140]

In preparation of the Model Law, particular attention was paid to the functions traditionally performed by various kinds of 'writing' in the traditional paper-based environment. Such functions indicate reasons as to why national law may require the use of 'writing'.[141] The Guide gives a list, which does not form a 'numerus clausus', to clarify the reasons why national law requires parties to reduce their actions in writing for legal efficacy.[142]

There are important reasons why writing is required. First, it is mainly to ensure that there is tangible evidence of the existence and nature of the agreement; secondly, to identify the parties who have intent to bind themselves; and thirdly, to assist the parties to be aware of the consequences of entering into a contract. Other reasons are to provide a legible document for all parties involved and to ensure that a document remains unaltered over time and provides a permanent record of a transaction. A further valid reason is to allow for the reproduction of a document so that each party can retain a copy of the same data. Since it is in digital form, it is important that it can allow authentication of the data by means of a signature. The Guide also notes that in certain instances, acceptability of the document by public authorities and courts would be important to: (a) record the intent of the author by means of 'writing'; (b) provide a record of that intent, and; (c) bring legal rights and obligations into existence in instances where 'writing' was required for validity purposes.[143]

However, in the preparation of the Model Law, it was found that it would be inappropriate to emphasise the writing requirement alone as many national laws also require parties to 'sign' a document and in some

[140] Pistorius op cit note 69 at 11.
[141] Guide op cit note 8 para 48 at 35.
[142] Ibid.
[143] Ibid.

instances also retain and/or produce original documents.[144] Thus, the requirement that data be presented in written form (which can be described as a 'threshold requirement') should thus not be confused with the more stringent requirements such as signature and originality.[145]

While a number of functions are traditionally performed by 'writing', the Model Law focuses on the notion that information should be capable of being reproduced and read. Both notions are expressed in Article 6 in an objective test that information be 'accessible so as to be usable for subsequent reference'.[146] The purpose of Articles 6 is to primarily focus on the reproduction and readability of a data message. Pistorius[147] is of the view that this is an objective criterion, namely, that the information in the data messages must be accessible so as to be usable for subsequent reference. This is confirmed in paragraph 50 of the Guide.[148]

With regard to the term 'usable', the Model Law states that data messages should not only be limited to human usability and accessibility but should also include computer use as software might be necessary to render such electronic data in a readable form. It was found that the phrase 'subsequent use' is preferred to 'durability' or 'non-alterability' as these requirements would have been too harsh a standard and the requirements of 'readability' or 'intelligibility' might be too subjective.[149]

In terms of Article 6(3) a member state may exclude certain matters or legally relevant Acts if it deems fit. The writing requirement may not be applicable to certain kinds of information, for example, where the legal requirements include the warnings or legal risks that may be embodied in the conclusion of an electronic contract. The purpose of Article 6(3) is not

[144] Guide op cit note 8 para 49 at 35.
[145] Pistorius op cit note 69 at 144.
[146] Hermann op cit note 87 at 5.
[147] Pistorius op cit note 69 at 144
[148] Guide op cit note 8 para 50 at 36.
[149] Ibid.

to create a blanket exception to the legal recognition of data messages being equivalent to a paper-based document. Rather, member states are encouraged to incorporate the objectives of the Model Law to try and achieve some form of legal uniformity for electronic data messages to gradually overcome the obstacles created by electronic data communication.[150]

(v) Electronic signatures

The Electronic signature issue gave rise to lengthy discussions in the working group during the preparation of the Model Law. While traditional signatures perform many functions, all legal systems recognise that a signature serves, at the very least, to: (a) identify a person, (b) provide certainty of that person's signature and (c) to associate that person with the content of a document. The Model Law concentrates on these functions.[151] To explain the proposition that the electronic signature has its origins in the paper-based methods of signing, it is important to look again at the Guide which is substantial based on the 'travaux préparatoires' of the Model Law.

The Guide notes that in addition to the above factors, a signature may attest to: (a) the intent of a party to be bound by the contents of a signed document; (b) a person's intent to endorse authorship of a text; (c) the intent to associate oneself with a document written by another person; and (d) the time and place that a document was signed or that a person was at a particular place.[152] In some countries a signature has the purpose of fulfilling an 'ex lege' formality in the conclusion of certain contracts and failure to adhere to such formality may render a contract void and/or voidable. A traditional signature can also become subject to additional security procedures such as verification by a witness or a notary.[153]

[150] Also see Guide op cit note 8 para 52 at 37.
[151] Hermann op cit note 87 at 5.
[152] Guide op cit note 8 para 54 at 38.
[153] Ibid.

The drafters of the Model Law were of the view that they had to develop various functional equivalents for the different types of signatures and levels that exist for traditional signatures. This was done to ensure that various means of electronic authentication could be used in electronic commerce practices as a substitute to create legal certainty.[154] Therefore, Article 7 adopts a comprehensive and flexible approach which leaves the question open as to which technologies should be used for such purpose.[155] Article 7 of the Model Law considers the form of an electronic signature and whether it is appropriate in the circumstances.[156]

It establishes the general conditions under which data messages would be regarded as authenticated, sufficiently credible and enforceable in the face of signature requirements which currently present barriers to electronic commerce.[157] Such trust and confidence is indeed a prerequisite to encourage e-commerce for business and consumers. By implication, this means that it will be necessary to deploy secure technologies such as digital signatures, digital certificates and secure electronic payment systems.[158]

Pistorius, affirms that a signature, be it in electronic or hand-written form, fulfils a dual function.[159] On the one hand, it identifies the signatory to a specific agreement or legally relevant act; and on the other, the intention to be contractually bound. Pistorius[160] adds that an additional function of the signature may be to acknowledge the true content of the agreement.[161] It is submitted here, that the correctness of an agreement could also be added to this list, which in legal terms would be extremely close to the true content.

---

[154] Guide op cit note 8 para 55 at 38.
[155] Hermann op cit note 87 at 5.
[156] Mason op cit note 32 at 154.
[157] Guide op cit note 8 para 56 at 38.
[158] J Angel 'Why use Digital Signatures for Electronic Commerce?'(1999) *JILT*(2), at 2-4.
[159] Pistorius op cit note 69 at 13.
[160] Ibid.
[161] Also see Coetzee op cit note 45 at 513 where he successfully sums up all the functions of an electronic signature as stated by the other authorities.

Article 7 is based on the recognition of the functions of signatures in paper-based environments. It is stated that legal requirements for signatures are met in a digital environment if a method is used to identify the signatory in the data message to indicate reliable and appropriate approval of the data's purpose for being generated or communicated.[162] Article 7 of the Model Law states the requirements for the recognition of a valid electronic signature are primarily based on the functions that a signature has in the paper-based environment. Article 7(1) states 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.'

Article 7, thus further focuses 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 the document.[163] The Guide suggests that a flexible approach is applied to achieve the level of security by the method of identification used in paragraph 7(1)(a).[164] In addition, the method used under paragraph (7)(1)(b) should be reliable and appropriate for the purpose which the data message is generated or communicated.[165]

In other words, a particular standard and/or minimum subset of requirements for a particular transaction may or may not be satisfactory in establishing the authenticity of one signature over another. However, the

[162] Lodder op cit note 140 at 4.
[163] Pistorius op cit note 69 at 15.
[164] Guide op cit note 8para 57 (1)(a) at 39.
[165] Ibid.

article relies on the reasonableness of the parties and the need to strike a balance between the method used and the purpose for which it was used and leaves it in the hands of judicial interpretation.[166] As this definition (being technologically neutral) does not mention any particular kind of signature, it should be understood that as long as an electronic signature meets the test of identification, authenticity and reliability, it is a valid signature.[167]

Mason[168] stated that the elements of an electronic signature can create difficulties for the international acceptance of a particular form of a signature. He used Article 7(1)(a) as an example which provides for methods used to identify a person, and to indicate their approval of the message's information. He suggested that although these elements do not preclude any form of electronic signature, the said definition presupposes that only a digital signature will suffice. Furthermore, Mason goes on to say that this is further reinforced by Article 7(1)(b) which discusses issues of reliability and whether the form of a signature used is appropriate in the circumstances.[169]

The Guide goes on to explain the differences that may be apparent in an array of legally relevant acts and it suggests legal, technical and commercial factors that may be taken into account in recognising and or accepting the value of an electronic signature. This particular interpretation should be seen in the light of all the circumstances of a particular legally relevant Act. Some of the important factors used in determining the appropriateness of an electronic signature are: (a) the sophistication of the equipment used by each of the parties; (b) the nature of their trade activity; (c) the kind and size of the transaction; (d) compliance with authentication procedures set forth by intermediaries; (e) the range of authentication procedures made available by any intermediary; (f) the function of signature

[166] Hermann op cit note 87 at 6.
[167] C M Abhilash 'E-commerce Law in developing countries : An Indian perspective' (2002) 11 *ICTL* 3 at 272.
[168] Mason op cit note 32 at 159.
[169] Ibid.

requirements in a given statutory and regulatory environment; and (g) any other relevant factor.[170]

Article 7(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.[171] Article 7(3) gives each state that intends to adopt the provisions of Article 7 the discretion to decide which types of transactions or legally relevant Acts should be expressly excluded from legal recognition in the online environment.[172]

Pistorius confirms[173] that the Model Law in Article 7 does not place any particular duty on any party or state to recognise a particular set of rules or standards regarding electronic signatures, but it rather provides guidance as to what might constitute an appropriate substitute for a signature if the parties used electronic communication in the context of an electronic contract.[174]

The nature, type and magnitude of statutory obstacles and the necessity to apply the authentication of e-commerce transactions in different legal systems placed so much pressure on nations and the international community as a whole[175] that the Model Law was followed by another Model Law in 2001 dealing specifically with issues related to electronic signatures. The UNCITRAL Model Law on E-Signatures is dealt with in detail in this dissertation further on .

---

[170] Such as the frequency at which commercial transactions take place between the parties; the capability of communication systems; compliance with trade customs and practice; the existence of insurance coverage mechanisms against unauthorized messages; the importance and the value of the information contained in the data message; the availability of alternative methods of identification and the cost of implementation; 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.
[171] Article 7 (2).
[172] Article 7 (3) reads: 'The provisions of this article do not apply to the following: [...]'.
[173] Pistorius op cit note 69 at 15.
[174] Guide op cit note 8 para 59 at 40.
[175] Faria op cit note 117 at 530.

(vi) *Attribution of data messages*

In the faceless and quite different regions of cyberspace, one of the most significant issues that need to be resolved is that of attribution.[176] Article 13 has its origins in Article 5 of the UNCITRAL Model Law on International Credit Transfers, which defines the obligations of the sender of a payment order.[177] Article 13 of the Model Law comes closest to establishing a rule of liability. The intention is to give maximum legal weight to the authentication procedures created by the parties.[178]

The purpose of Article 13(1) and 13(2) is to demystify whether a data message has really been sent by the person cited as the originator of the data message, and to create a simple rule to determine when a message may be deemed to be that of the purported sender.[179]

In a paper-based environment, the issue of attribution would arise due to a forged signature of the originator. In the electronic environment, it would be due to sending a data message by way of the unauthorized access to the originator's informations system, notwithstanding the fact that the originator's code, encryption or the like would be accurate. [180]

Article 13(1) entrenches the rebuttable presumption that an originator is bound to a data message if the said message has been

[176] Phang & Seng op cit note 116 at 109.
[177] Guide op cit note 8 para 83 at 49.
[178] Hermann op cit note 87 at.7
[179] Article 13(1) and 13(2) provide that , '(1) A data message is that of the originator if it was sent by the originator itself. (2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
(b) by an information system programmed by, or on behalf of the originator to operate automatically.'
[180] Guide op cit note 8 para 83 at 49.

effectively sent.[181] Paragraph (2) deals with the scenario where the message is sent by person other than the originator who had express and/or implied authority to act on behalf of the originator. Article 13(2)(a) creates a rule that an e-mail will be deemed to be that of the sender even if an agent was the effective sender of the message and the agent purports to have had the authorization to do so. Article 13(2)(b) creates a rule that the recipient of a data message sent by an 'electronic third party agent' programmed by the sender would also be deemed to be that of the sender.[182]

However, the Guide affirms that the Model Law specifically states that the said provision is not intended to alter or to impose any obligations on an enacting state to change its domestic laws of agency. The appropriate domestic laws will determine whether the person in question acted within the scope of their authority or 'ultra vires'.[183]

Article 13(3)[184] deals with two different types of scenarios where an addressee may presume that a data message is that of the originator. In the first scenario as per Article 13(3)(a), the addressee may still hold the originator liable or responsible in the case where the addressee followed the authentication procedures as previously agreed to with the originator.[185] The second scenario as per Article 13(3)(b), is a form of 'estoppel' in that the originator is 'estopped' from relying on the fact that he did not send the data message due to the relationship he had with the sender of the data

[181] See Phang & Seng op cit note 116 at 110 who confirm that a rebuttable presumption is created by Article 13 (1). Also see the Guide para 84 at 49.
[182] Phang & Seng op cit note 116 at 110.
[183] Ibid.
[184] '(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.'
[185] Phang & Seng op cit note 116 at 110.

message.[186]Article 13(4) [187] sets out the exceptions to the rebuttable presumption created by paragraph (3).

Article 13(5)[188] deals with the preclusion that the addressee is entitled to regard the data message as being what the originator intended to send and to act on this assumption unless the addressee knows or should have known that errors have been made in a sent data message. Article 13(6)[189] deals with the practical problem of having erroneously sent duplication of data messages well as the standard of care that should be observed in distinguishing an erroneously duplicated message from a separate data message. The addressee can regard each separate message as valid unless he knew otherwise or whether he ought to have known. [190]

In the early draft stages of Article 13 the drafters wanted to add a paragraph dealing with the attribution of authorships of a data message. This paragraph was not added and it was agreed that mention thereof should be made in the Guide.[191]

[186] Guide op cit note 8 para 85 at 49.
[187] '(4) Paragraph (3) does not apply:
(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or (b) in a case within paragraph (3) (b), at any time when the addressee knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.'
[188] '(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.'
[189] (6) 'The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.'
[190] Guide op cit note 8 para 90-1 at 51.
[191] Ibid para 92 at 49.

(vii) Time, place of dispatch and receipt of data message

In the instance where contracting parties are not in each other's presence, it becomes imperative to establish the time and place or when and where the contract was formed.[192] The time and place of contract conclusion is crucial to determine when the parties are bound to an agreement and will have bearing on legal actions should a dispute arise. The method of acceptance has legal consequences which are more complex to determine in the electronic environment.[193] Rules on contract formation often distinguish between 'instantaneous' and 'non-instantaneous' methods of communicating offers and acceptances. A distinction is also drawn between communications exchanged among parties present at the same place at the same time ('inter praesents') and communications exchanged at a distance ('inter absents').[194] In the ordinary course of business, parties agree on contracts 'inter praesents' or during face-to-face negotiations, leaving aside the possibility of contract formation through performance or other forms of implied acceptance.[195]

Faria states, that there are mainly four theories for determining the moment at which an acceptance becomes effective under general contract law, although they are rarely applied in pure form for all situations. First, in terms of the 'declaration theory'[196] a contract is formed when the offeree produces some external manifestation of his intention to be contractually bound notwithstanding the fact that the offeror may not be fully aware of the offeree's acceptance.[197] Secondly, in terms of the

[192] Hermann op cit note 87 at 7.
[193] Pistorius op cit note 69 at 18.
[194] Faria op cit note 117 at 544.
[195] Ibid.
[196] Which seems to be the default rule for Switzerland. In this case the contract is formed when '*lorsque les partes ont, reciproquement et dune maniere concordante, manisfeste leur volone*'(Part 1 of the *Code des obligations*) as cited by Faria in fn 57. Faria op cit note 117.
[197] Ibid.

'information theory' a contract only becomes effective once the offeror becomes aware of the acceptance. This is usually the default rule and also applies to most forms of communication such as telephone communication and fax.[198]

Thirdly, according to the 'mail box rule' also known as the 'postal, dispatch or expedition theory', the communication of the acceptance is effective once it has been posted or sent by the offeree (e.g., by placing the letter in a mail box). It is usually used in the case of indirect communications and has its origins in the issue of revocability of offers.[199]

Fourthly, the 'reception theory' which determines that a communication of an acceptance only becomes effective on receipt, or when it is possible to access it or when the offeror is made aware of it. In terms of the this so-called '*Zugangsthoerie'*,[200] the deciding moment is dependent upon the communication being available to the relevant recipient in the sense that it is placed at his/her disposal at a place where he/she in the ordinary course of business would be reasonably expected to receive it. Eiselen notes that objectively speaking, this theory would be most suitable for indirect forms of communication such as the internet, EDI and e-mail. [201]

Article 15 (1) of the Model Law defines the time of dispatch of a data message[202] as the time when the data message enters an information system placed outside the control of the originator.[203] Information system must be interpreted broadly and would therefore include the communication link between the sender and, for instance, the service provider.[204] Thus, it is

[198] S Eiselen op cit 127 at 308.
[199] Ibid at 309.
[200] The German term 'for upon receipt'.
[201] S Eiselen op cit 127 at 308.
[202] (1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator
[203] Guide op cit note 8 para 101at 55.
[204] Pistorius op cit note 69 at 19.

suggested that under the Model Law, offer and acceptance are dispatched when the enter button on the sender's computer is pressed.[205]

Ahmad notes that Article 15(1) attempts to change the substantive law relating to the communication of offer and acceptance where electronic means have been used.[206] Abhilash disagrees with this view and emphatically states that this is unfounded as Article 15 only explains and clarifies, inter alia, when dispatch and receipt of records take place, which is important purely for time of dispatch and receipt.[207] In terms of the concept of having dispatched a message, a message should not be deemed dispatched if it merely reaches the information system of the addressee but fails to enter it.[208]

For the time of receipt, Article 15(2)[209] distinguishes between a few factual situations: (a) where the addressee designates a specific information system, which may or may not be his own, for the receipt of a message, the data message is deemed to have been received when it enters the designated system; (b) if the data message is sent to an information of the addressee that is not the designated system, receipt occurs when the data message is retrieved by the addressee; and (c) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.[210]

---

[205] Glatt op cit note 69 at 59.
[206] Ahmad. op cit note 131 at 139.
[207] Abhilash op cit note 168 at 274.
[208] Guide op cit note 8 para 104 at 56.
[209] '(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:
(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:
(i) at the time when the data message enters the designated information system; or
(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
[210] J Faria op cit note 115 at 547. Also see the views of C Glatt op cit note 69 at 60.

Article 15(3) emphasises that paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

Glatt aptly illustrates the complexity of the problems with the following illustration.[211] A Scottish company accepts an offer from a US company situated in State X. Both use a service provider for internet access.[212] The Scottish company has a German service provider; the US company's service provider has its place of business in State Y. If in this situation the postal rule applies, the contract would be formed in Germany, where the message will be received for transmission to the US. Depending on the further circumstances of the case, the contract might therefore be subject to German law.[213] It is not uncommon, that users of electronic communications link with each other on a cross-border platform without being aware of it. Therefore, the Article 15 attempts to negate the location issue and emphasises a more objective criterion, namely, the place of business.[214] This consequence is avoided by the UNCITRAL Model Law on Electronic Commerce in Article 15(4).[215]

The Model Law reflects the fact that the location of information systems is irrelevant and sets forth a more objective criterion, namely, the place of business of the parties. However, Article 15 is not intended to

[211] Glatt op cit note 69 at 61.
[212] Ibid.
[213] Ibid.
[214] Guide op cit 8 para 100 at 55.
[215] '(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.'

establish a conflict-of-laws rule.[216] Paragraph 78 of the Guide consciously avoids providing a solution to the said conflict of laws. [217]

Article 15(4) provides that a data message is deemed to be dispatched at the place of the originator's place of business, and is deemed to be received at the addressee's place of business. In the instance where the parties have multiple places of business the place closest to the underlying transaction relationship will be deemed the place of business.[218] Where the there is no underlying transaction, the deemed place will be where the parties have their place of business. Where the parties do not have a principle place of business, their habitual place of business will be deemed to be their place of receipt.[219] Thus, Article 15 (4) introduces a distinction between the deemed place of receipt and place actually reached by a data message at the time of its receipt under Article 15 (2).

(viii) Acknowledgement of receipt

The use of the principle of 'functional acknowledgement' is a business decision that can be made by users of electronic commerce. Article 14 establishes a system of acknowledgment of receipt. It focuses upon whether or not a data message was received, but not on whether it has been read.[220] The provision of acknowledgement of receipt does not intend to impose any duty on any user to apply such procedure; however, the commercial world values such a system as highly important and the practice

[216] S Eiselen op cit 127 at 308.
[217] 'As to the time and place of formation of contracts in cases where an offer or the acceptance of an offer is expressed by means of a data message, no specific rule has been included in the Model Law in order not to interfere with national law applicable to contract formation. It was felt that such a provision might exceed the aim of the Model Law, which should be limited to providing that electronic communications would achieve the same degree of legal certainty as paper-based communications. The combination of existing rules on the formation of contracts with the provisions contained in Article 15 is designed to dispel uncertainty as to the time and place of formation of contracts in cases where the offer or the acceptance are exchanged electronically.'
[218] Pistorius op cit 67 at 19.
[219] Ibid.
[220] Hermann op cit note 87 at 7.

is commonly used and applied.[221] Therefore Article 14 (1) specifically states that the provisions of Article 14(2) – (4) are used at the discretion of the contracting parties where an acknowledgment of receipt has been requested.[222]

The purpose of Article 14 (2)[223] is to validate acknowledgement where the originator has not expressly agreed with the addressee as to the method to be used to validate acknowledgement.[224]Article 14(3) deals with the situation where the originator has declared that the data message is subject to acknowledgement of receipt[225] without specifying a specific time in which the said acknowledgement of receipt should be received.[226]

Article 14(4),[227] on the other hand, deals with the factual and more common situation where an acknowledgment of receipt is requested by the originator without adding the condition that failure to acknowledge receipt may result in the data message being deemed not to have been sent. The purpose of this provision is to establish whether the sender of the message would be relieved from any legal consequences due to the failure of

[221] Guide op cit note 8 para 93 at 52.
[222] Article14(1) provides: 'Paragraph (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.'
[223] Article14(2) provides: 'Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by
(a) any communication by the addressee, automated or otherwise, or
(b) any conduct of the addressee sufficient to indicate to the originator that the data message has been received.'
[224] Guide op cit note 8 para 94 at 52.
[225] Article 14(3) provides: 'Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.'
[226] Guide op cit note 8 para 95 at 53.
[227] 'Article 14(4) provides: 'Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and theacknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:
(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and
(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.'

the addressee to acknowledge receipt.[228] On the other hand, for the originator to rely on this provision he/she must: (a) send another message notifying the other party of its default; (b) specify a reasonable time by which such acknowledgment must be received; and (c) specify the effect of such default before relying on the consequences of this provision.[229]

Article 14(5) creates a rebuttable presumption that when the addressee sends an acknowledgment of receipt that he has actually received the message sent by the addressee. [230] The second part of Paragraph (5) echoes paragraph (5) of Article 13, which states where there is a conflict between the text sent and the text received, the received text prevails.[231]

(ix) Automated transactions

According to Pistorius, the UNCITRAL Model Law indirectly addresses automated transactions.[232] Article 11 provides that, unless agreed otherwise, 'a contract may be formed by an offer and the acceptance of an offer by means of data messages'. The Guide notes that the provision was deemed necessary in view of remaining uncertainties in many countries as to the validity of electronic contract formation where data messages expressing the offer and acceptance are generated by computers without immediate human intervention.[233] It is submitted that this is the correct approach as the wording of Article 11 was structured to encompass all forms of e-commerce at the time.

[228] Guide op cit note 8 para 96 at 53.
[229] Ibid.
[230] '(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.'
[231] Guide op cit note 8 para 97 at 53.
[232] T Pistorius 'The Legal Effect of Input Errors in Automated Transactions: The South African Matrix' (2008) *JILT* available at http://go.warwick.ac.za/jilt/2008_2/pistorius2 (accessed on 14 February 2012)
[233] Guide op cit note 8 para 76 at 46.

(x) The impact of the Model Law

Notwithstanding the fact that many countries widely accepted the principles contained in the UNCITRAL Model Law on E-Commerce, it could not simply be assumed that its principles achieved the goal of world-wide harmonization.[234] The fact that technology is rapidly changing poses several challenges to the framework of the Model Law. It became evident that electronic signatures would definitely be a problem owing to the different signing techniques that were being developed. The provisions of the Model Law soon proved inadequate to deal with all the issues raised by the creation and use of electronic signatures.[235] The pioneering work of the UNCITRAL Model Law has recently[236] led to the adoption of a treaty on Electronic Contractors. It has also formed the basis for most universal e-commerce domestic legislation around the world namely e-commerce legislation

(d) United Nations Commission on International Trade (UNCITRAL) Model Law on Electronic Signatures

(i) Objectives and scope

Adopted by UNCITRAL on 5 July 2001, the Model Law on Electronic Signatures creates a legal framework for electronic signatures. Building on the flexible principle contained in Article 7 of the UNCITRAL Model Law on E-Commerce, it establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures.[237]

[234] Faria op cit note 115 at 533.
[235] Eiselen op cit 127 at 314.
[236] UNCITRAL. The UNECIC in 'International Contracts Entered (2005) into Force on 1 March 2013' – UNCITRAL press statement available at http://www.uncitral.org (accessed on 9 April 2013.)
[237] Summary regarding the contents of UNCITRAL Model Law on Electronic Signatures can be found at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html (accessed 9 April 2013)

The Model Law follows a technology-neutral approach, which avoids favouring the use of any specific technical process or technology.[238] To place the matter in context before examining : (a) the provision relating to the meaning of electronic signatures; (b) the treatment of signature technologies; and (c) the compliance with requirements for electronic signatures, this research would like to refer to the Resolution[239] adopted by the UNCITRAL General Assembly.

UNCITRAL, in drafting the new Model Law had to give further effect to the Model Law on Electronic Commerce adopted by the Commission at its 29th session, in 1996 as complemented by the additional Article 5 adopted by the Commission at its 31st session in 1998. This was in addition to paragraph 2 of General Assembly Resolution 51/162 of 16 December 1996 in which the Assembly recommended that all states should give favourable consideration to the Model Law when enacting or revising their laws. [240]

The Model Law on E-Signatures provides a link between technical reliability and legal effectiveness of an electronic signature by adopting an approach according to which the legal effectiveness of an electronic signature is predetermined.[241] It sets out the presumption that where e-signatures meet certain criteria of technical reliability, they should be treated as equivalent to hand-written signatures. In establishing that presumption, the Model Law on E-Signatures follows a 'technologically neutral approach'.[242]

[238] Ibid.
[239] Resolution adopted by the General Assembly [on the report of the Sixth Committee (A/56/588)]56/80 Model Law on Electronic Signatures op cit note 10 at *vii*.
[240] Ibid.
[241] Ibid.
[242] F Morel & R Jones 'De-mystifying Electronic Signature and Electronic Signature Law from a European Union Perspective' (2002) 7 *Communication Law* 6 at175.

In addition, the Model Law on E-Signatures establishes basic rules of conduct that may serve as guidelines for assessing the responsibilities and liabilities of the various parties involved in the signatures process. These are: (a) the signatory; (b) the relying party ; and (c) the trusted third party (where applicable).[243] The instrument was conceived as an addition to the UNCITRAL Model Law on E-Commerce, which should be dealt with on an equal footing and share the legal nature of its forerunner.[244]

The drafters of the Model Law on E-Signatures took the view that if they wanted to draft a law that advocated 'media-neutrality' and the 'technology-neutral' rules, it would be nonsensical to exclude or limit the scope of application of the Model Law on Electronic Signatures to any specific form or medium of electronic signature.[245] In addition, the Electronic Signature Model seeks to establish both a national and an international standard for electronic signatures.

The non-standardisation of local and international e-signature laws may also create a duality of regimes, so creating a serious obstacle in the uniform standard as sought by the Model Law on Electronic Signatures.[246] It is important to note that the provisions of the E-Signatures Model Law are to be interpreted with 'regard to its international origin and the need to promote uniformity in its application and the observance of good faith.'[247] Questions concerning matters governed by the Model Law on Electronic Signatures, which are not expressly settled in it, are to be settled in conformity with the general principles on which it is based.[248] Article 2, defines an 'electronic signature' as:

[243] Ibid.
[244] Guide op cit note 8 para 87 at 40.
[245] Ibid at 40.
[246] Guide op cit note 8 para 91 at 42.
[247] Article 4(1).
[248] Article 4(2).

'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.'

This again confirms the functions of the signature in accordance with the traditional purpose that it has. It adds that the e-signatures may have other functional uses in the electronic world. Eiselen explains that Article 2 deals specifically with issues of identification, attribution and assent and that it aims to create a functional equivalent for an electronic signature without trying to mimic the physical attributes of a paper-based signature.[249] Once again, the principle of 'functional equivalence' appears in the E-Signatures Model Law.

In addition, a new standard of flexibility has been achieved in the definition of an electronic signature that is embodied in the 'technological neutrality' principle. It is also important to give the definition of a 'certificate', which is defined as 'a data message or other record confirming the link between a signatory and signature creation data'.[250]

(ii) Equal treatment of signatures

Wang explains that there are three different approaches when dealing with the various electronic signature legislations that have been enacted world-wide, namely the 'minimalist approach', the 'prescriptive approach' (also known as the technology-specific approach) and the 'two-tiered approach'.[251] Some jurisdictions that follow a technological neutrality approach recognise all technologies for electronic signatures. This approach is called the minimalist approach as it is non-prescriptive.

[249] Eiselen op cit 127 at 315.
[250] Ibid.
[251] M Wang 'Review of the signature regulations: Do they Facilitate or Impede Intentional Electronic Commerce?' (2006) Paper presented at ICEC 6 August 14-16 2006, Fredericton, Canada at 549.

The Technological approach is seen as a light approach as it recognizes all forms of electronic signatures as functional equivalent of handwritten signatures provided that they fulfil certain specified functions and meet the technology-neutral reliability requirement.[252]

When applying the prescriptive approach, legislators looked at the highest level of security offered by existing technology to avoid unauthorized access and to promote data security. However, by favouring particular signatures types, this approach is seen as inhibiting the development of new signature techniques as it excludes a number of futuristic electronic signatures.

On the other hand, the two-tier approach recognizes: (a) self-regulation; (b) limited government involvement ; and (c) government-led processes in achieving its goal.[253] The two-tiered approach is also known as the two-pronged legislative approach. The first tier of regulation sets very low thresholds of requirements for electronic authentication methods to receive a certain minimum legal status. The second tier of regulation assigns a greater legal effect to certain authentication methods known as secure, advanced, or enhanced electronic signatures.[254]

Article 3 of the Model Law on E-Signatures contains the fundamental principle that all digital signature methods, irrespective of the technology used, should be treated equally and should be given legal recognition as explained in Article 6.[255] This, however, should not be

[252] UNCITRAL. 'Promoting Confidence in Electronic Commerce: Legal issues on International Use of Electronic Authentication and Signature methods' (2009) para 83 at 36, available at http://www.uncitral.org/uncitral (accessed on 7 March 2011).
[253] Ibid para 90-9 at 39-40.
[254] Ibid para 93 at 41-3.
[255] UNCITRAL Model Law on Electronic Signatures op cit note 10 para 107 at 48.

construed as overriding the provisions of Article 5[256] that allow freedom of contracting between contracting parties using inter alia whatever digital signature method has been agreed to by the parties.[257] This is in line with the minimalist approach supported by Wang, which does not accord preferable assumptions to any particular technology. The parties can choose their preferred e-signature at their own discretion.[258]

(iii) Compliance with a requirement for a signature

Article 6, is one of the core provisions of Model Law.[259] Article 6 deals with the liability and recognition of electronic signatures and states:

> '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.'

As stated above, the idea underlying Article 6 is to build upon the principle as laid down in Article 7 of the UNCITRAL Model Law on E-Commerce. Article 6 also gives guidance to the fulfilment of the test of reliability as Article 7(1)(b). During preparation of the Model Law on E-Signatures, the view was expressed that one should rather refer to an 'enhanced electronic signature' as this would have a dual function: (a) legal consequences would arise from signature techniques that would be deemed

[256] Ibid Article 5 states that: 'The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law'.
[257] Ibid at 42.
[258] Wang op cit note 247 at 252.
[259] Guide op cit note 8 para 115 at 52.

reliable, and (b) no legal consequence would arise from the use of a less reliable signature.[260] Another reason for this new e-signature standard was to do away with the ex post facto necessity, as per Article 7 of the Model Law of analysing as to whether a signature is recognised or not.[261] According to the Guide, states are free to insert this provision into their law, either as a substantive rule, or as a legal presumption pertaining to reliability of an electronic signature as dealt with by the insertion of Article 6(3).[262]

The main focus of this provision is to ensure that where a reliable e-signature has been used it should have legal consequence.[263] It must also be noted that the meaning of identification as contained in the Model Law on E-Signatures is intended to have a broader meaning than that of just identifying names, but it may also refer to their position or authority in combination with the said name.[264]

Subparagraphs (a) – (d) are intended to express the objective criteria of the technical reliability of an electronic signature. In subparagraph (b) there is reference to the signatory's control over the signature creation data of an e-signature, and it is submitted that an authorized person has used it. In the case of a 'split-key' the signature will be attributed to the person

---

[260] Guide op cit note 8 para 118 at 53.
[261] Ibid.
[262] Article 6(3) provides : '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.'
[263] Ibid para 116. Also note that paragraphs 1, 2 and 5 of Article 6 introduce provisions drawn from Article 7, paragraph 1(b), 2 and 3 of the UNCITRAL Model Law on E-Commerce. Wording of para1(a) of Article 7 of the UNCITRAL Model Law on E-Commerce dealing with the meaning of an electronic signature has already been drawn into Article 2 (a) of the Model Law of E-Signatures.
[264] Guide op cit note 8 para 117 at 52.

using the said key.[265] In terms of principles of subparagraph (a) and (b) there may be no agency or transmissibility of an e-signature. Regarding the integrity of the e-signature, subparagraph (c) deals with the criterion to be applied when establishing the reliability of an electronic signature. Subparagraph (d) makes it clear that the said provision would apply only to those countries where no distinction could be made between the signature's integrity and the integrity of the information.[266] Subparagraph (d) also eliminates the notion that an e-signature may not be separated from the entire data message. Paragraph 4[267] and 5[268] has also been included to deal with a few outstanding issues.

Paragraph 4(a) is intended to provide a legal basis for contracting parties in commercial practice. Paragraph 4(b) also re-affirms that the presumptions made in paragraph 3 may be rebutted.[269] This is also not to specifically exclude any certain acts or transactions. Paragraph 5 has been inserted to allow a flexible inclusion of the provisions of Article 6 so that they can find general acceptance by contracting states, and in some instances, may increase the criteria as required by Article 6 or, in exceptional cases, even reduce the standard as required.[270]

[265] Ibid para at 55.
[266] Ibid paras 124-125 at 55 - 56.
[267] Paragrpaph (4) provides: 'Para 3 does not limit the ability of any person:
(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.'
[268] Paragraph (5) provides:'The provisions of this article do not apply to the following: [...]'.
[269] Guide op cit note 8 para 128 -129 at 56.
[270] Guide op cit note 8 para 131 at 57.

iv) Recognition of foreign certificates and e-signatures

Article 12[271] deals with recognition of foreign e-signatures and certificates between two contracting parties in two different states. Article 12 endeavours to solve the problem. The purpose of paragraph 1 is to introduce the general rule of 'non-discrimination' between foreign signatures and certificates on the basis of their origin.[272] The fact that a signature is from a particular jurisdiction should have no bearing on the effectiveness and legal recognition of that electronic signature.[273] Instead, the adequate test in establishing the recognition of a foreign signature should be that of reliability and not origin. Article 12(2)[274] lays down the general criterion to be applied in establishing 'technical equivalence' known as the 'substantial equivalence reliability test.'[275]

The test as stated does not require a signature to be the exact equivalent but substantial equivalence is required.[276] This means that the similarity test must be satisfied and that the differences in reliability must be minimal (if any). It must be noted that the test as applied for e-signatures is the same for certificates as per sub-paragraph 12(3).[277]

Paragraph 4 deals with any other factors that may be relevant in establishing the substantial equivalence of the two foreign signatures and

[271] Article 12(1) provides: 'In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:
(a) To the geographic location where the certificate is issued or the electronic signature created or used; or
(b) To the geographic location of the place of business of the issuer or signatory.'
[272] UNCITRAL op cit note 253 para 159 at 75-6.
[273] Guide op cit note 8 para at 69.
[274] Article 12(2) provides: 'A certificate issued outside [the enacting State] shall have the same legal effect in [the enacting State] as a certificate issued in [the enacting State] if it offers a substantially equivalent level of reliability.'
[275] Guide op cit note 8 para 153 - 5 at 70.
[276] Ibid.
[277] Article 12(3) provides: 'An electronic signature created or used outside [the enacting State] shall have the same legal effect in [the enacting State] as an electronic signature created or used in [the enacting State] if it offers a substantially equivalent level of reliability.'

certificates.[278] Further, when carrying out such analyses, the parties must also take cognizance of the recognised international standards. Paragraph 5[279] re-iterates the principle of party autonomy but discourages steering away from the substantial equivalence test as suggested by paragraphs 2, 3 and 4.[280] The Model Law on E-Signatures does not require or promote a reciprocity arrangement for the recognition of foreign electronic signatures between countries as it steers away from any geographical factors for legal effectiveness. It aims, instead, to enhance a multinational acceptance of different nations' e-signatures.[281]

In short, the Model Law on E-Signatures has gone a long way to re-entrench the principle as established by the Model Law of E-Commerce and has clarified some key aspects that either were not adequately addressed in the latter, or were issues of contention. Eiselen stated that the creation of the 'technology neutrality' principle has gone a long way towards embracing different authentication methods, such as digital certificates and biometrics.[282]

It is submitted here that although there is very little case law that deals with the ability of an e-signature to meet the legal signature requirement, the Model Law on E-Signatures has nevertheless influenced the courts of various countries (in particular in the United States and Germany) to start recognising them.[283] Therefore, the Model Law of E-Signatures has fulfilled its purpose and will apparently continue to do so in the future. This is definitely a step in the right direction.

---

[278] Article 12(4) provides, 'In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of paragraph 2 or 3, regard shall be had to recognized international standards and to any other relevant factors.'
[279] Article 12(5) provides, ' Where, notwithstanding paragraphs 2, 3 and 4, parties agree, as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.'
[280] Guide op cit note 8 par 158 -160 at 71-7 2.
[281] UNCITRAL op cit note 253 para 160 at 76.
[282] Eiselen op cit 127 at 316.
[283] UNCITRAL op cit note 253 para 107 at 48-51.

(e) United Nations Convention on the use of Electronic Communications in International Contracts (UNECIC)

(i) Objectives and scope of the treaty

After the creation of the two Model Laws on E-commerce and E-signatures it became apparent that issues relating to the formation of international contracts required further redress. Faria divides them into two broad categories: (a) general issues of contract formation as provided for in contract law (which will be of interest in this dissertation); and ;(b) issues specific to contracting by electronic means, or those that may be rendered particularly conspicuous by the use of modern-day technology.[284]

The issues raised in the first category deal with the central question of whether traditional notions, such as offer and acceptance and the time of receipt and dispatch of offer and acceptance may be transposed into an electronic environment.[285] The legal uncertainty of the issues raised above, especially their application to international contracts, led to the drafting of the UNECIC (2005).[286]

The Convention entered into force on 1 March 2013, after the minimum number of member states ratified it.[287] It is an interpretive legal instrument with minimum substantive provisions. The UNECIC promotes the use of electronic communication in international contracting by providing for the functional equivalence of e-communications whilst preserving and observing the principle of technological neutrality.[288] Taking the form of a Convention is a landmark legal instrument that promises to harmonise basic electronic commerce legislations amongst contracting member states.

[284] Faria op cit note 115 at 541.
[285] Ibid.
[286] UNCITRAL Resolution 60/21 op cit note 75.
[287] UNCITRAL press statement op cit note 238.
[288] K W Chong & J Chao 'United Nations Convention on the use of Electronic Communications in International contracts – a new global standard' (2006) 18 *SALJ* at 119.

The Convention builds upon both UNCITRAL's Model Laws on E-Commerce and E-Signatures but its provisions have been improved and updated to take into account technological development since 1996 – most notably the growth of the internet.[289] The two Model Laws were aimed at standardising and facilitating the response of domestic legal systems to the challenges of e-commerce. They have subsequently been used in drafting the domestic legislation of a fairly large number of countries.[290]

The UNECIC, in turn, aims at establishing legal certainty in international trade by providing solutions and harmonising rules on e-communication for international transactions[291] and also to offer practical solutions for issues related to the use of e-communication in international contracts.[292] In addition, it introduces two ancillary principles that were not contained in the previously mentioned UNCITRAL Model Laws, namely: (a) freedom of form and ;(b) the principle of combined technological neutrality with the functional equivalence approach.[293]

The UNECIC is not intended to establish uniform rules for substantive contractual issues. Instead, it is argued that the enabling provisions in the UNECIC are dealt with in a completely different manner than its Model Law predecessors. While the Model Law on E-Commerce contains a number of separate articles for creating electronic equivalents for the requirements of 'writing', 'signature', 'original', and 'retention of electronic messages', all enabling provisions in the UNECIC are in the same article.[294] The UNECIC does not cover 'record retention' as it was felt that this deals more with evidential issues than contract formation. Connolly and

[289] Ibid.
[290] S Eiselen 'The UNECIC: International Trade in the digital era'(2007) in *PER* at 4-49.
[291] See preamble of UNECIC as referred to by Eiselen op cit note 291.
[292] UNCITRAL. United Nations Resolution 51/162 op cit note 5 para 3 at 13.
[293] F G Mazotta 'Notes on the United Nations Conventions on the effect of Electronic Communications of International Contracts and its effects on the United Nations Conventions on Contracts for the International Sale of Goods'(2007) *RCTLJ*.2.
[294] C Connolly & P Ravindra 'First UN Convention on e-commerce finalised' (2006) 22 *Computer and Security Report* at 35.

Ravindra have levelled the same argument against the article dealing with electronic signatures in the UNECIC.[295] Pistorius, however, disagrees and states the writing and signatures provisions are central to contract formation.

However, the convention contains a few substantive rules that do not just reiterate the principal of functional equivalence but actually put into place some new substantive rules necessary to ensure effectiveness in e-communications. Article 1 of UNECIC deals with the scope of the application of the convention[296] and provides the UNECIC applies to e-contracts entered into by parties who have their places of business in different states.[297]

The UNECIC does not specifically prescribe that both parties must have their business in a contracting state and thus does not have a narrow application, such as the Convention on Contracts for International Sale of Goods (CISG) [298], which requires that before the convention may apply, it must have been adopted by the state in which protection is being claimed.[299] However, as the UNECIC does not apply automatically to all international transactions. It will not apply automatically as public international law, but only according to the rules of international law - if the transaction is made subject to a legal system where the UNECIC applies.[300]

---

[295] Ibid.

[296] Article 1(1) provides that:'This Convention applies to the use of electronic communications in connection with the formation or performance of a contract between parties whose places of business are in different States'.

Article 1(2) provides that: 'The fact that the parties have their places of business in different States is to be disregarded whenever this fact does not appear either from the contract or from any dealings between the parties or from information disclosed by the parties at any time before or at the conclusion of the contract.

Article 1(3) provides that:'Neither the nationality of the parties nor the civil or commercial character of the parties or of the contract is to be taken into consideration in determining the application of this Convention.'

[297] Ibid.

[298] J Coetzee 'The Convention on the use of Electronic Communications in International : Creating an International Legal Framework for Electronic Contracting' (2008) 18 *SAMLJ* at 249.

[299] Ibid .

[300] Eiselen op cit note 291 at 11- 49.

The convention will also apply to the agreement if formed and executed in the same state but where the two contracting parties have their places of business in different jurisdictions at the time the agreement was concluded.[301] Notwithstanding the fact that there is no need for the parties to have their place of business in the contracting state, it is nevertheless important that the law of a contracting state apply to the parties' dealings. In the instance where the parties have not agreed on a particular law to govern the relationship, the law will be determined in terms of the rules of private international law of the forum state, that is, the law will apply as the domestic governing law of the agreement.[302]

Article 4 deals with definitions as presented in the text of the Convention. It is worth mentioning that most of the definitions are based on the definition in the UNCITRAL Model Law on E-Commerce.[303] The UNECIC defines a 'communication' as 'any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer that the parties are required to make or choose to make in connection with the formation or performance of a contract'. The definition of 'electronic communication' has been kept broad enough to be defined as 'any communication that the parties make by means of data messages'.

It is also noteworthy that the definition of 'message' has been extended from the Model Law definition of data message, including previously excluded formats, and is now defined as:

> '….information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic mail, telegram, telex or telecopy…'

[301] Coetzee op cit note at 299.
[302] Ibid.
[303] A Kuczerawy & W Killian 'United Nations Convention on the Use Communications in International Contracts' (2007) 1 *CBKE – e – Biuletyn* 7 at 10.

Article 4(h) has also extended the meaning of the 'place of business' which has now also been given a more liberal and realistic approach to e-commerce and is defined as:

> ' [A]ny place where a party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location.'

Eiselen[304] illustrated the application of the Convention in the following manner. Trader A, which has its place of business in Senegal, has concluded a transaction with trader B, who has its place in business in South Africa. For the purposes of illustration, Eiselen suggested that Senegal has adopted the UNECIC and that South Africa has not. The first question to ask is: Should there be any dispute regarding the validity and formation of the agreement, which law will apply?

Eiselen suggests that this can be resolved by using the rules of private international law of the 'lex fori', that is, the court adjudicating over the dispute. In other words, if the rules of private law should determine that Senegalese law should be applied then, the UNECIC will be applicable, if not and South Africa is determined to be the governing law, then the UNECIC will not have application.[305] However, an agreement would not be regarded as international unless the parties were both aware of this fact before the time of the conclusion of the agreement.[306] If a government, a parastatal or similar body should make use of electronic communication in dealing with a party in another state, the Convention will apply.

This seemingly straightforward position is equally complicated by Article 19 and Article 20 which deal with the exclusion of the application of the Convention in instances where a state makes certain declarations.

[304] Eiselen op cit note 291 at 11 – 50.
[305] Eiselen op cit note 291 at 11-12, 49.
[306] Eiselen op cit note 291 at 14, 49.

Article 2 provides for the exclusion of the UNECIC's scope of application.[307] The UNECIC is aimed solely at commercial contracts and consumer contracts are specifically excluded in Article 2(a). Article 2(1) and Article 2(2) also list excluded transactions that do not fall within the scope of the convention, such as contracts concluded for personal, family or household purposes,[308] foreign exchange transactions, negotiable instruments and interbank payment systems.[309]

The scope of application may also be restricted by means of declarations made in terms of Article 19. The effect and procedures for making such declarations are stated in Article 20 of the UNECIC. Article 19 provides states with two choices as to how they would like to make declarations in terms of the UNECIC.[310]

In the first instance, the Convention may apply only if both parties have their place of business in a contracting state, but on the other hand, the parties can agree that the Convention will apply where and if the parties have expressly agreed to do so.[311] Connolly and Ravindra state that the non-binding character of these instruments gives states a method to choose provisions to implement into domestic law and how to implement them. However, this approach has the same shortcomings of the UNICTRAL Model Laws in that: (a) international uniformity is reduced; (b)

---

[307] '1. This Convention does not apply to electronic communications relating to any of the following:
(a) Contracts concluded for personal, family or household purposes;
(b) (i) Transactions on a regulated exchange; (ii) foreign exchange transactions; (iii) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; (iv) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary.
2. This Convention does not apply to bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.'

[308] Kuczerawy & Killian op cit note 304 at 7-9.

[309] Chong & Chao op cit note 289 at 122.

[310] Coetzee op cit note 299 at 253.

[311] UNCITRAL Resolution 60/21 op cit 75 paras 278 – 281 at 88-89.

there is less legal certainty; and (c) harmonization of the domestic laws cannot be achieved.[312]

Article 3 embraces the 'party autonomy' principle and provides that it may vary from their domestic laws, principles of international law and the UNECIC.[313] Article 3 of the Convention allows parties to exclude the application of the Convention or derogate from or vary the effect of any of its provisions, which means that unless 'opted out', the Convention will govern any international contract that meets its jurisdictional requirement.[314]

Article 19(2) authorises a state to exclude any matter it may specify in terms of an Article 20 declaration. Coetzee is of the view that where the provisions of the UNECIC do not apply by virtue of the Convention being applicable, the parties may still agree to be bound by the provisions of the Convention. In such instances the Convention will be dealt with as if it were a contractual term of the agreement.[315]

(ii) Location of parties

The purpose of Article 6is to offer elements that allow the parties to ascertain the location of the parties' place of business,[316] thus assisting in the determination of, amongst other relevant factors, the international or domestic character of a transaction and the place of contract

[312] Connolly & Ravindra op cit note 295 at 32.
[313] Coetzee op cit note 299 at 253.
[314] Kuczerawy & Killian op cit note 304 at 10.
[315] J Coetzee op cit note 299 at 254.
[316] Article 6 (1) states that: 'For the purposes of this Convention, a party's place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

Article 6(2) states that: 'If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this Convention is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract.'

formation.[317] Article 6(1) creates a rebuttable presumption in favour of a party's indication of its place of business accompanied by the condition that such indication may be rebutted if the other party can show that the party claiming its 'place of business' in a specific location is, in fact, not giving the correct information.

Article 6(2) will come into play in the instance such as where no place of business has been specified[318] and it provides that if a party has not indicated a place of business, and has more than one place of business, the place of business for the purpose of the contract is that which has the closest relationship to the relevant contract, with regard to the circumstances known to or contemplated by the parties at or before the conclusion of the contract. If there is no indication by a party to the contract of the exact place of business and it only has one place of business, that sole place of business falling within the definition in terms of Article 4(h) of the UNECIC would be the place of business for the purposes of the contract.[319]

The provision allowing a party the opportunity to prove that its place of business at another location is important in that a party may want to deceptively indicate a place of business where no assets are located and thus may not be subject to some form of legal restraint. The innocent party is then given the option to choose as to where the place of business should be, and that alone can be crucial for purposes of jurisdiction and legal proceedings.[320]

Article 6(3) to Article 6(5) deal with other factual situations such as in the case of a naturalised person who claims to have a place of business and the situation where a party may want to rely on the presence of its

[317] UNCITRAL United Nations Convention 60/21 para 108 at 42.
[318] UNCITRAL United Nations Convention , Resolution 60/21paras 110 - 12 at 42.
[319] Chong & Chao op cit note 289 at 124.
[320] Eiselen op cit note 291 at 28- 49.

domain in another state. [321] Where a party has no place of business, his/her habitual place of residence will be deemed to be his place of business. It is also important to note that the location of a server is not indicative of a business's place of business. This also relates to the use of foreign domain names instead of the domain names within one's jurisdiction.[322]

While Article 6(4) and Article 6(5) seek to clarify that certain presumptions should not be made based on the location of any supporting technology or virtual address, this does not preclude a court or an arbitrator, from taking these matters into consideration when determining the location of a party, where deemed appropriate.[323]

[321] '6(3). If a natural person does not have a place of business, reference is to be made to the person's habitual residence.

6(4) A location is not a place of business merely because that is:

(a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(b) where the information system may be accessed by other parties.

6(5). The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.'

[322] Eiselen op cit note 291 at 8-49.

[323] Connolly & Ravindra op cit note 295 at 34.

(iii) Treatment of electronic communications and legal recognition of electronic contracts

This Article has its origins in Article 8 of the UNCITRAL Model Law on E-Commerce and embodies the principle of party autonomy. Article 8 of the UNECIC confers validity and enforceability on e-communications. As Eiselen correctly pointed out, Article 8 aims at establishing technological neutrality as far as the form or method of business communication are concerned.

Article 8(1) stipulates that e-communications will be given legal effect on par with other traditional paper-based forms as required by the functional equivalence approach. The mere fact that a statement is sent as a data message cannot serve as grounds for its non-recognition.[324] Article 8 (1) of the UNECIC provides that:,

> '[A] communication or a contract shall not be denied legal validity and enforceability solely on the grounds that it is in the form of an electronic communication. '

Furthermore Article 8(2) provides that:

> '[N]othing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct. '

Article 8(2) embodies the principle of part autonomy and clarifies that the Convention does not require a party to use or accept electronic communications.[325] Article 11 states that e-communications that are not addressed to a specific party but are accessible by a number of

[324] Chong & Chao note 289 at 125.
[325] *Ibid* at 126.

parties using an information system are to be considered an invitation to offer (or invitation to treat) unless a contrary intention is clearly expressed.[326] Article 12 goes further and states that a contract is not invalid simply because one or both parties use automated message services (such as websites or software programmes) to communicate on their behalf, without human attention at the time of the contract.[327]

Mindful of Conventions such as the CISG, the UNCITRAL working group decided not to include rules determining place and time of the formation of contracts.[328] The combination of existing rules on the formation of contracts is designed to dispel uncertainty as to the time and place of formation of contracts in cases where the offer or acceptances are exchanged electronically.[329] Mazotta supports this view[330] which this writer submits is the correct one as the UNECIC never intended to change any preceding Conventions but was designed to enhance and take further what the Model Laws had begun.

(iv) Form

Like the UNCITRAL Model Law on E-Commerce, the UNECIC also continues in the spirit of functional equivalence with the view of fulfilling the requirement of issuing paper-based documents in electronic form.[331] Although the principles of functional equivalence and technological neutrality may be relatively easy to state, their actual application is easier said than done. Article 9(1) makes it clear that the UNECIC does not require a communication or a contract to be made or evidenced in any particular

[326] Connolly & Ravindra op cit note 295 at 35.
[327] Gregory op cit note 113 at 9.
[328] UNCITRAL Resolution 60/21 op cit note 87 para 130 at 47.
[329] Ibid.
[330] Mazotta op cit 294 note at 28.
[331] UNCITRAL United Nations Convention with explanatory note para 133 at 48.

form (which also includes electronic form) thereby confirming the principle of freedom of form.[332]

Articles 9(2) to Article 9(4) contain a number of default minimum standards for enabling the recognition of electronic equivalents to traditional paper-based form requirements.[333] As to how the issues of technological neutrality and functional equivalence can be tackled effectively with regard to 'writing', 'signature' and 'originality' is comprehensively dealt with in Article 9(2)[334] to Article 9 (5)[335] as mentioned below. Therefore, the UNECIC focuses on the minimum requirement that information must be capable of being reproduced and read, rather than a standard to determine whether an electronic communication has fulfilled the requirement of a paper-based document as contained in Article 9(2).[336]

In drafting Article 9(3) the working group took cognizance of the value and functions of both paper-based and electronic signatures[337] as previously discussed in this treatment. Article 9(3), deals with the value of electronic signatures, and concerns itself more with the authenticity requirement by adding additional measures in evaluating the validity of an electronic signature.[338] Significantly, Article 9(3) of the Convention contains a new rule for the electronic functional equivalent of handwritten signatures.[339] Article 9(3)(a) provides a definition of functional equivalent electronic signature as:

'Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of a writing, that requirement is met by an electronic communication if the information

[332] Ibid para 136 at 49.
[333] Connolly & Ravindra op cit note 295 at 35.
[334] Mazotta op cit note 294 at 8.
[335] Ibid at 8.
[336] Ibid.
[337] UNCITRAL United Nations 60/21 para 151 at 53.
[338] Mazotta op cit note 294 at 8.
[339] Chong & J Chao op cit note 289 at 128.

contained therein is accessible so as to be usable for subsequent reference. [Two methods can be] used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication; and 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 [9(3)(a)] above, by itself or together with further evidence.'

Chong and Chao state that a legal requirement for a signature will be met if Article 9(3)(a) and Article 9(3)(b)(i) (which they term 'the reliability in theory') or Article 9(3)(b)(ii) ('the reliability in fact') is proven.[340] The 'reliability in theory' also called 'reliability in principle' involves a more theoretical determination of reliability. The circumstances surrounding the use of the electronic signature, including any relevant agreement, is also to be considered in determining reliability.[341] The 'reliability in fact' allows evidence to be adduced to prove the signature used fulfilled the function described in Article 9(3)(a).[342]

Article 9(4) deals with the requirements for the integrity and reliability of an electronic communication. Article 9(5) states that:

'Where the law requires that a communication or a contract should be made available or retained in its original form or provides consequences for the absence of an original, that requirement is met in relation to an electronic communication if:

[340] Ibid.
[341] Connolly & Ravindra op cit note 295 at 36.
[342] Ibid.

(a) there exists a reliable assurance as to the integrity of the information it contains from the time when it was first generated in its final form, as an electronic communication or otherwise; and

(b) where it is required that the information it contains be made available, that information is capable of being displayed to the person to whom it is to be made available.'

It states that where domestic law requires a document to be retained in its original form, that requirement is deemed met if a reliable assurance exists as to the integrity of the information as first generated in its final form.

Article 9(5) sets out the material requirements for judging the integrity of such information by emphasising that the information has to remain complete and unaltered.[343] Article 9(5) contains further provisions on assessing the integrity of a communication namely, Article 9(5)(a) which states that the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the additions of any endorsement and any change which arises in the normal course of communication, storage and display.[344] Article 9(5)(b) also states that the standard of reliability shall be assessed in the light of the purpose for which the information was generated and in light of all relevant circumstances.

The manner in which electronic information is handled within any business will depend on the nature and importance of such information. Eiselen suggests that to fulfil the above requirements and to satisfy the various standards of authentication and integrity, companies must develop protocols that deal with the information in a way that is compliant with the UNECIC. [345]

[343] Gregory op cit note 113 at 7.
[344] Connolly & Ravindra op cit note 295 at 35.
[345] Eiselen op cit note 291 at 33 - 49.

(v) Time and place of dispatch and receipt of communication

Article 10 of the Convention contains the rules on the time and place of dispatch of electronic communications. Significantly, both these rules are different from the equivalent rules in the UNCITRAL Model law on E-Commerce.[346] Article 10 of the UNECIC which deals with the determination of the determination of the time and place of communications is important for a number of reasons, including the time that an acceptance becomes effective, or some other time limit such as when a performance was rendered.[347] Article 10 reads as follows:

> 'The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.'

In terms of Article 10(1), a message is deemed to have been sent (dispatched)[348] if it leaves the information system used by the originator, that is, when the message is beyond the control of the originator. In the instance where the originator and addressee are in the same information system, the message is deemed to have been sent when it is received by the addressee.[349] Article 10(2) states the following on the issue of 'receipt':

[346] Chong & Chao op cit note 289 at131.
[347] Eiselen op cit note 291 at 29 - 49.
[348] Ibid.
[348] Ibid.

> 'The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.'

During the drafting of this article, the UNCITRAL noted that it was of the view that that the test for the capability of retrieval is not intended to be subjective but objective.[350] The 'receipt' is linked to the time when the e-communication becomes capable of being retrieved, which is presumed to be at the time when it has reached the addressee's designated electronic address and is capable of being retrieved. Conversely in terms of Article 10(2), an e-communication is deemed to be received when the addressee becomes aware of the fact that the massage has been sent to the address as designated by the addressee[351] and such e-communication must be capable of being retrieved at electronic address of the addressee.

Article 10(2) seeks to distinguish between a designated and a non-designated electronic address to create a fair allocation of risks for the originator and addressee. The issue becomes even more complex when a party has multiple e-mail addresses, which might not be checked on as frequently as the primary address.

The notion that a party 'ought to have known' that an e-mail could be sent to a different e-mail address is dispensed with and a party is

[350] Ibid.
[351] Eiselen op cit note 291 at 30- 49.

not penalised for not having checked another business e-mail address.[352] The issue of awareness seems to be a factual issue and could be proved by means of showing that, for example, a message was indeed received because it was opened on the addressee's computer. The UNECIC, therefore, applies an objective test.[353]

Article 10(3) and Article 10(4) address the situation where the place of receipt of electronic communications is in another location than that of the addressee. The principal reason for including these rules is to address a characteristic of e-commerce that may not be treated adequately under existing law in that the information system of the addressee where the e-communication is received, or from which the e-communication is retrieved, is located in a jurisdiction other than that in which the addressee itself is located.[354]

Article 10(3) contains a firm rule and not merely a presumption. Consistent with its objective of avoiding a duality of regimes for online and offline transactions, it specifically places its focus on the actual place of business of the party. Article 10(3) reads as follows:

> 'An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business, as determined in accordance with Article 6.'

The phrase 'deemed to be' has been chosen deliberately to avoid attaching legal significance to the use of a server in a particular jurisdiction other than the jurisdiction where the place of business is located simply because that was the place where an electronic communication had reached the information system where the addressee's electronic address is

[352] UNCITRAL Resolution 60/21 op cit note 75 para 191.
[353] Connolly & Ravindra op cit note 295 at 36.
[354] UNCITRAL Resolution 60/21 op cit note 75 para 194.

located.[355] Article 10(4), once again re-confirms the position that the location of the information system (server) receiving the information is irrelevant and that the jurisdiction of the relevant place of business or habitual place of business will prevail:

> 'Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.'

The location of the information system supporting the electronic address of the addressee is not relevant provided that there is a reasonable connection between the originator and the information system and therefore it may be different from the place where the e-communication was deemed to have been received.[356]

(vi) Invitations, advertisements and offer

Whether a website, by offering goods or services for sale constitutes an offer, is a question not restricted to e-communication, but is a much older problem. The reason is that most jurisdictions (such as South Africa,[357] Germany[358] and Scotland[359] do not regard an advertisement as an offer but merely an offer to do business (also called *'invitatio ad offerendum'*).[360] Most jurisdictions require that the offer must be a firm statement addressed to the offeror that can allow the offeree to make a firm 'I accept' or 'I do not accept' statement and form the intent to be bound contractually.

[355] Ibid para at 64-5.
[356] Kuczerawy & Killian op cit note 304 at 17.
[357] *Crawley v Rex* 1909 TS 1105.
[358] Also see C Glatt op cit note 69 at 39.
[359] Ibid at 41.
[360] UNCITRAL Resolution 60/21 op cit note 75 para 197 at 65.

The use of the internet has taken this problem a step further as individuals are able to interactively purchase goods or services instantaneously.[361] This general principle that goods or services offered that are accessible to an unlimited number of persons are not binding applies even where the offer is supported by an interactive application.[362] The only remedy here is by way of using the autonomy principle to provide for a term or terms to which the parties will be bound notwithstanding the fact that such offer was not directly sent to him or her. Article 11[363] of the UNECIC deals with the issue of whether an advertisement is an offer in a traditional manner by reaffirming the general norm that an advertisement is merely an invitation to bargain or to do business.

Article 11 states that electronic communications that are not addressed to a specific party but are accessible by a number of parties using an information system are to be considered an invitation to offer (or invitation to treat) unless a contrary intention is clearly expressed.[364] It is submitted that the wording of the website is important to distinguish between an offer and on invitation to do business. The wording will usually be of assistance in establishing the intent of the parties and could indicate a contrary intention.

(vii) Automated transactions

In so far as traditional contracts negotiated and entered into by natural persons have been examined, it is clear with reference to the previously mentioned Model Laws, that the UNECIC has adapted specific

[361] Eiselen op cit note 291 at 3- 49.
[362] UNCITRAL United Nations Convention para 205 at 75,
[363] A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.
[364] Connolly & Ravindra op cit note 295 at 35.

problem-solving provisions.[365] In fact, in the light of technological neutrality and the functional equivalence principles, no discrimination should be made because the means of communication used to enter into the agreement was in an automated form.[366] Article 12 confirms the use of electronic agents for the purposes of automated transactions.[367]

Article 12 of the UNECIC removes the legal uncertainty of automated transactions unlike the UNCITRAL Model Law on E-Commerce which, by implication, simply includes it in Article 11. However, the specifically created Article 12 in the UNECIC expressly deals with automated transactions and, in essence, attributes the actions of the automated system to the party making use of such automated system and seeks reliance on an agreement concluded in such a manner.[368]

Article 12 states that:

> 'a contract is not invalid simply because one or both parties use automated message services such as websites or software programs) to communicate on their behalf, without human attention at the time of the contract'. [369]

(f) African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa [370]

(i) Objectives and scope of convention

The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (AUCLCS) is an

[365] Mazotta op cit note 294 at 12.
[366] Ibid.
[367] Coetzee op cit note 299 at 255.
[368] Eiselen op cit note 291 at 34 – 49.
[369] Article 12 and also see Gregory op cit note 113 at 9.
[370] AUCLCS (version -1/01.2011), available at: *http://www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf* (accessed 22 November 2012)

African legal framework that has been created following the 14th AU 2010 summit which explored the theme 'Information and communication technologies in Africa : Challenges and Prospect for Development'[371] and this was subsequently confirmed by the 'Abuja Declaration'.[372].

The AUCLCS gives effect to a Resolution of the last session of the Assembly of Heads of State of Governments of the African Union, and seeks to harmonise African cyber legislations on e-commerce personal data protection, cyber-security promotion and cyber-crime control. [373] It is, however, clear that its focus is more on cyber-security and cyber-crimes than provisions on enablement and regulation of e-commerce in Africa.

Unlike the UNCITRAL Model Law for E-Commerce, Article I-1 of the AUCLCS has interestingly omitted definitions such as 'data', 'data messages' , 'writing', 'electronic signature' and 'original' but includes wide definitions for the terms such as 'electronic commerce',[374] 'electronic mail'[375] and 'information'.[376] Although Article I–2 re-states that, 'electronic commerce is an economic activity by which a person offers or provides goods and services by electronic means' such as in Article I-1(4), it goes on to define the 'field of electronic commerce' as also comprising:

---

[371] [Assembly/AU/11(XIV)], Addis Ababa, Ethiopia, 31 January - 2 February 2010) also see U J Orji *Cybersecurity Law and Regulation* (2012) at 375.

[372] CITMC-3 ([AU/CITMC/MIN/Decl.(III)], Abuja (Nigeria), 03-07August 2010 and also see A Yankey ,'The AU Draft Convention on Cybersecurity and e-transactions: Cooperation against Cybercrime' presented atCyber Crime Octupus on 6 – 8 June 2012, Strasbourg – France.

[373] Also see summary of the Convention at *http://www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf* (accessed 22 November 2012).

[374] Article I-1(4) states that: 'Electronic commerce means all economic activity by which a person offers or provides goods and services remotely or by electronic means'.

[375] Article I-1(7) states that: 'Electronic mail means any message in the form of text, voice, sound or picture sent by a public communication network, and stored in a server of the network or in a terminal facility belonging to the addressee until it is retrieved'.

[376] Article I-1(9) states that: 'Information refers to any element of knowledge likely to be represented with the aid of devices and to be used, conserved, processed or communicated. Information may be expressed in written, visual, audio, digital and other forms'.

> '[S]ervices such as those providing information on-line, commercial communications, research tools, access, data retrieval and access to communication or information hosting network, even where such services are not remunerated by the recipients.'

Murungi argues that the said definition only includes the seller's economic activity by which a person offers or provides goods and services by electronic means. He states that, 'a better attempt at such provision would have been to use words such as "person who offer or receives offers by electronic means"'.[377]

Article I-3 states that the activities, as stated in Article I-2, be freely exercised in the African Union space, except for gambling (even in legal authorized betting and lotteries), in legal representation and assistance activities and activities of a notary.

(ii) Contracts in Electronic Form

Article I–16 entrenches the 'functional equivalence approach' by giving legal validity to electronic communication(s) in contract formation and states that:

> 'Electronic means may be used to disseminate contractual conditions or information goods or services.'

Furthermore, Article I–17 seems to follow the 'party autonomy principle' giving the parties the right to decide as to whether they want to use electronic communication in their transacting in that it states:

[377] M Murungi 'Comments on The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa (version -1/01.2011) at 4-11. Available at *http:// michaelmurungi.blogspot.com/2012/08/comments-on-draft-african-union.html* (accessed on 22 November 2012).

> 'The information requested for the purpose of concluding a contract or available during contract execution may be transmitted by electronic means addressee of such information has agreed to the use of the said means. '

In addition, Article I-18 further states that information,

> 'meant for a professional may be addressed to him/her by electronic mail provided she/he has communicated his/her personal address. '

Article I-23 confirms the 'party autonomy' principle in that it states that, 'no person shall be compelled to take a legal action by electronic means' as well as the right not to choose technology.[378] Article I-24 furthermore confirms that, 'where a written matter is required to validate a legal act such may be established and conserved in electronic form' under the conditions of the said domestic law applicable.

Article I-25 excludes the following acts from being performed electronically in terms of the AUCLCS, namely, the signature of a private individual relating to family law or law of succession and acts of a civil or commercial nature under the signature of a private individual relating to real security or personal security.

[378] Ibid at 6 -11.

(iii) Electronic Signatures

The convention also guarantees the validity of electronic signatures and gives the definition for electronic signatures in Article I–32 as:

> 'data in electronic form attached to or logically subjoined to a data message and which can be used to identify the data message signatory and indicate consent for the information contained in the said message.'

The above provision seems to be in line with the spirit and purpose of the UNICTRAL Model Law on E-commerce as well as the UNICTRAL Model Law on E-Signatures. Furthermore Article I–36 states that:

> 'A copy or any other reproduction of acts undertaken by electronic means shall have the same weight as the act itself, where the said copy has been certified as a true copy of the said act by bodies duly accredited by a State authority. The certification shall culminate in the issuance of an authenticity certificate, where necessary.'

In addition to the above Article I – 37 states that:

> 'An electronic signature on an electronic written matter shall be admissible on the same terms as a signature in manuscript written on paper based matter.
>
> The signature shall use such reliable identification procedure as guarantees its linkage with the act to which it relates. Such

> procedure shall be presumed to be reliable until proved otherwise, where the electronic signature has been created by a security signature device, and where the procedure guarantees the integrity of the act and the signature thereof has been identified.'

As stated above, it appears as if Article I-37 follows the UNCITRAL Model Law on E-Commerce. The UNCITRAL Model Law on E-signatures is also reflected with regard to the requirements of an e-signature. It is unfortunate that the rest of the AUCLCS, which seems to be in contrast to generally accepted international best practices and guidelines.

(iv) Conclusion on AUCLCS

Although the AUCLCS is an African legal framework designed to streamline African cyber security in the 21st Century, it has yet to be seen if this will become another idealistic legal framework that will not get off the ground. As noted above the AUCLCS also has to overcome the fact that it is not consistent with international consensus on the application and use of the UNCITRAL Model Laws.

The AUCLCS also seems to focus on other aspects of communication regulation such as security and electronic crimes, but it fails to cover core legal issues related to and affected by electronic commerce. It is also no secret that different regional developments have also superseded the effort of the African Union in codifying African cyber law.[379]

[379] For example the efforts of the East African Community (EAC1 and EACII) available at http://www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148 (accessed on 12 March 2013), Southern African Development Community (SADC Model Law of Electronic Commerce), available at http:// http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf. (accessed on 7 March 2013)

(g) Concluding Remarks

In conclusion, it is important to note that the international community has widely, through international responses, dealt with and attempted to resolve the legal problems created by e-commerce both domestically and on an international level. The Model Law deals with the recognition of data messages for purposes of contract formation, e-signatures, the issue of attribution of messages and also created new rules regarding the time and place of the dispatch and receipt of data messages.

This chapter also addresses the value and standards to be applied when using e-signatures which has now been clarified in great detail in the Model Law on E-Signatures with reference to the standard that must be applied in recognising e-signatures both in national and cross-border scenarios.

The issue of a contract formation where either partly or wholly by the actions of electronic agents has not been directly addressed in the Model Law.

The UNECIC now seeks to create uniformity regarding the principles laid down by the Model Laws and demystifies some of the issues regarding the time and place of dispatch and receipt of electronic communications. Although the AUCLCS is a step in the right direction to establish a legal African framework with a uniform approach to e-contract formation it has not achieved all it was intended to do.

The UNECIC also provides clarity and provisions on the issue of website offers as well as the value of automated transactions - a topic which previously was only mentioned in the Model Law by implication .

CHAPTER IV: THE SOUTH AFRICAN COMMON LAW ON CONTRACT FORMATION

(a) Consensus (meeting of minds)

As individuals and businesses interact they may enter into contracts in which rights and obligations are created. In certain instances contracts are breached and a party may want to claim specific performance or cancel the agreement and claim damages. To establish whether a legally binding agreement or a contract exists one looks first for the agreement by consent of the two or more parties involved.[380] A contract is defined as an agreement (arising from either true assent [consensus] or quasi-mutual assent) which is, or is intended to be enforceable at law[381] as a result of a valid offer and acceptance.[382] South African case law suggests that consent is the foundation or basis of a contract.[383]

The South African law of contract requires that the following elements of a contract be present for there to be a legally binding agreement between any parties: (a) capacity to act,[384] (b) consensus,[385] (c) lawfulness,[386] and (d)

[380] RH Christie *The Law of Contract* 4 ed (2001) at 23.
[381] Ibid at 2. Also see the South African case *Wilken v Kohler* 1913 AD 135 at 140 where J Innes referred to the use of the word *consensus* 'in its strict sense as meaning a concluded agreement legally enforceable'.
[382] *Estate Breet v Peri-Urban Areas Health Board* 1955 3 SA523 (A) 532E.
[383] *Greenberg v Washke* 1991 WLD 1 7, *Swart v Vosloo*1965 1SA 100 (A) and *Cinema City (Pty)Ltd v Morgenstern Family Estate (Pty) Ltd* 1980 1 SA 796 (a) 804D.
[384] See Nagel *et al Commercial Law* (2000) at 66. 'The law presumes that every living person and/or juristic person has contractual capacity. This may however be limited or excluded due to age. Only majors over 21 have full contractual capacity. Minors have to be assisted by one or both parents and or/guardian. In the case of *Infans* and intoxicated persons capacity to act is fully excluded'.

[385] A contract is generally concluded when an offer created by one party is unequivocally accepted by another resulting in the creation of consensus amongst the parties. The wills (intentions) of the parties and their intentions with the contract is the basis on which consensus is reached. Also See *Saambou-Nasionale Bouvereining v* Friedman 1979 (3) SA 978 (A), as well as the case of *Allen v Sixteen Stirling Investments (Pty)* 1974 4 SA164 (D) 172.
[386] See *Sierhout v Minister of Justice* 1926 AD 99 109 – where the court held that it is a fundamental principle of our law that 'a thing done contrary to the direct probation of law is void and no effect' as well as *Nino Bonino v De lange* 1906 TS 120 - in which the court

physical possibility.[387] Formalities may be included but are not mandatory.[388]

Accordingly, if any electronic communication between two or more parties (e.g. e-mail or SMS) can be interpreted as having complied with the formal constitutive requirements of a contract, as stated above at common law, it could be inferred without any reference that a valid contract has been concluded.[389] If any of the said requirements is not present, or doubt exists as to the genesis thereof, it may be declared void or voidable by a court of law.

(i) The valid offer

The first question that one needs to ask when examining the validity of an electronic contract is whether the contents of a website can constitute a valid offer at common law.[390] A person is said to make an offer when he puts forward a proposal with the intention that, by its mere acceptance and without more, a contract should be formed.[391] The offer must embody or contain sufficient information to enable the person to whom it is addressed to form a clear idea of exactly what the offeror has in mind.[392] In other words, the offer must set out the exact essential and material terms of the agreement to be unequivocally accepted by the offeree. The South African

---

held that an agreement that was 'contra bonus morales' and held to be invalid and unenforceable.

[387] See the case of *Aird v Hockley* 1936 EDL 117 the Court held that initial physical impossibly renders a contract void as and un-enforceable. Also see the case of *Hirshowitz v Moolman* 1985 3 SA where the court distinguished between a 'pactum de contrahendo' and physical possibility.

[388] See *Conrade v Rossouw* 1919 AD 287 were the Court confirms that no special formalities are required for the making of an enforceable contract unless a specific statute or common law rule requires any particular formatives as confirmed in *Goldblatt v Freemantle* 1920 AD 123.

[389] S Papadopoulus and S Snail (2012) 'Electronic contracts in South Africa (E-contracts)' in *Cyberlaw @ SA III : The law of the Internet in South Africa*, at 44.

[390] Pistorius op cit note 3 at 286. Also see Papadopoulus & Snail op cit note 390 at 45.

[391] Christie op cit note 381 at 32.

[392] *Humphreys v Casells* 1923 TPD 280 and also see Nagel op cit 379 at 18.

courts have been extremely reluctant in declaring agreements that are either vague or incomplete as valid and enforceable contracts .[393]

The offer must be a firm offer which means that the offeror has addressed a specific person or group of persons with the intent to be contractually bound. A tentative statement with a possible agreement in mind is not sufficient.[394] It should also be noted that an advertisement does not generally constitute an offer, it merely amounts to an invitation to do business.[395] It should be noted, however, that an advertisement may, depending on its wording, qualify as an offer.[396] This might be a grey area especially when dealing with website-based advertisements and advertisements by e-mail. Such interactive applications might be regarded as an offer 'open for acceptance, while stocks last', as opposed to an 'invitation to treat'.[397]

In *Bloom v American Swiss,*[398] the court stated and made it clear that an offeree can only accept an offer that he had knowledge of. A person cannot accept an offer made by an offeror if he/she does not understand the terms of and/or the circumstances of the offer, as this would lack the necessary '*animus contrahedi'* (intention to be contractually bound).[399]

Offers once received by the offeree can only lapse in the following circumstances: (a) expiry or lapse of prescribed time[400];(b) in the case of a contract where time is of essence; (c) after a reasonable time;[401] (d) upon the

[393] *Kantor v Kantor* 1962 (3) SA 207; *Murray v Murray* 1959 (3) SA 84 (W).
[394] *Efroiken v Simon* 1927 CPD 367 at 370 for a good illustration of this principle.
[395] *Crawley v Rex* op cit note at 352.
[396] *Carlill v Carbolic Smoke Ball Company* [1893] 1 QB 256 (CA) at 268-269 also see Pistorius op cit note 3 at 286.
[397] Ibid.
[398] *Bloom v American Swiss* 1915 AD 100 at 102 – 107.
[399] Christie op cit note 381 at 33.
[400] *Dietrichsen v Dietrichsen* 1911 TPD 486 at 496.
[401] E Kahn *et al Ellison Kahn Contract and Mercantile Law* 2 ed (1989) at 157. Also see Papadopoulus & Snail op cit 390 at 45

death of either of the parties;(e) upon being rejected ; and ;(f) upon revocation.[402]

(ii) The acceptance

A binding contract is created when there is an acceptance of an offer.[403] The acceptance must be manifested or be indicated by some form of an unequivocal act from which the inference of acceptance can logically be drawn.[404] It stands to reason that consent is possible only where the whole offer and nothing more or less is accepted.[405] When the acceptance is coupled with reservation, it is no acceptance but is in fact a counter-offer, which the offeror may accept or reject. [406]

In a nutshell, the requirements for valid acceptance are that: (a) the acceptance must be unconditional/unequivocal[407];(b) the offer must be accepted by the person to whom it was addressed;[408];(c) acceptance must be in response to an offer and ;(d) acceptance must comply with formalities.[409]

[402] *Laws v Rutherford* 1924 AD at 261 – 262.
[403] Christie op cit note 381 at 65. Also see Pistorius op cit note 3 at 286..
[404] *Reid Bros v Fischer Bearings Ltd* 1943 AD 232 at 241 and *Collen v Rietfontein Engineering Works* 1948 (1) S 413 (A) at 429 – 30.
[405] *Saambou* op cit note 380.
[406] Van Aswegen *et al General Principles of the Law of Contract* (1999) at 27.

[407] Christie op cit note 381 at 67.
[408] *Hersch v Nel* 1948 SA 686 at 693 –695 .
[409] *Brand v Spies* 1960 (4) SA 14 - where a contract of sale of land that failed to satisfy statutory requirements in terms of section 2 (1) of Land Alienation Act was deemed invalid.

(b) Formalities for a valid agreement

There is no specific requirement that an agreement must be in writing, however, the legislator has created laws to ensure that certain agreements, once concluded, will be 'prima facie' evidence of the agreement between the parties. In the matter of *Goldblatt v Freemantle,*[410] the court clearly stated that: 'Subject to certain exceptions, mainly statutory,[411] any contract may be verbally entered into; writing is not essential to contractual liability'.

There are no specific reported cases that specifically deal with the formation of a contract via the interchange of electronic mail. However, the case of *Council for Scientific and Industrial Research v Fijen*[412] gave an indication of how the South African courts viewed the then relatively new technology by stating that an electronic Local Area Network (LAN) message sent to a superior indicating one's intent to resign constituted a valid letter of resignation in the context of a written and signed document.[413]

Section 3 of the Interpretation Act 33 of 1957 states that:

> 'In every law expression relating to writing shall, unless the contrary intention appears, be construed as including also references to typewriting, lithography, photography and all other modes of representing or reproducing words in visible form.'

[410] *Goldblatt* op cit note 389 at 128.
[411] Author's note: In other words there are common law rules that require writing.
[412] *Council for Scientific and Industrial Research v Fijen 1996 17 ILJ 18* (AD).
[413] Ibid.

It is submitted that that a signature amongst other descriptions thereof could be by 'a mark'. It is submitted that this would also include an electronic mark and therefore an electronic signature as well.

It could be deduced from the wording of the above provision that, 'all other modes of representing or reproducing words in visible form',[414] would also include the reproduction of the e-mail; be it in reduced material form (printed) or electronically visible (on an electronic display device) – since there is no 'numerus clausus' (closed number of possibilities) on the various methods anticipated by this particular wording of Section 3 of the Interpretation Act [415]

South African courts have, in the past, followed a similar approach as that suggested by the Interpretation Act, for example, in the case of the alienation of land that was supposed to be reduced in writing, in the case of *Balzan v O'Hara and Others,*[416] where the parties used the antiquated method of sending a telegram. Judge J Coleman held that a telegram constituted written and signed authority within the meaning of written and signed, as contemplated in the Land Alienation Act.[417] The learned judge went on to say that:

> '[T]he fact that the telegram was not personally written, nor signed by the sender, was not sufficient to disqualify the document as being non-compliant with the provision. The sender had obviously written the telegram in his own words by hand and signed the form which authorised the post office to send the telegram himself.'[418]

[414] Papadopolous and Snail op cit note 390 at 44-46.
[415] Ibid.
[416] *Balzan v O'Hara and Others* 1964 (3) SA (T).
[417] Act 68 of 1957.
[418] *Balzan* op cit note 417.

Therefore, the court could only come to the logical conclusion that compliance had been rendered sufficiently. The court also confirmed in the decision of *Yates v Dalton*[419] that an offer and acceptance may be made by telegraph. One could argue that these cases are not persuasive authority as to whether an e-mail may constitute a valid offer. However, it is important to know that in both the *Balzan* and *Yates* cases, a more mechanical device was used called a telegram. The said device encodes the sender's initially written message into an electronic frequency message that is sent via a telephone line and decoded on the receiving side and results in a typed document - the telegram.

The reasoning was that a telegram may meet the requirements of a written and signed document should apply as readily to e-mail messages. E-mail messages are transmitted over long telephone lines and satellite links where the user enters a data massage by pressing his fingers on the keys of the keyboard. Furthermore, such messages can be reduced to tangible form by means of a compact disc, stiffy disc or other reliable form of stored format that can be viewed on a screen display or in the form of printout.[420]

(iv) Time and place that the contract enters into effect

Normally, no difficulties arise when establishing the time and place that acceptance of an offer takes place and the contract becomes effective as the offeree usually makes his acceptance known in the presence of the offeror. Van Aswegen states that the South African law takes cognizance of four possible jurisprudential contract theories:[421] The declaration theory, the expedition theory, the reception theory and the information theory.[422] For

[419] *Yates v Dalton* 1938 EDL 177.
[420] S Edelstein 'Litigation in Cyberspace: Contracts on the internet' (1996) *Commercial Litigation*. Retrieved from University of Pretoria (Legal Track,Trial, Vol32 No10 at 16 (7)).
[421] Van Aswegen op cit note 407 at 30.
[422] For a discussion of these theories see Christie op cit note 381 at 75 - 85; *Cape Explosives Works v SA Oil and Fat Industries* 1921 CPD 244*; Kergeulen Sealing & Whaling v CIR* 1939 D 487*; Jamieson v Sabingo* 2002 (4) SA 49 (SCA).

the purposes of this discussion it is important to look at the information and expedition theories.[423]

In accordance with the information theory, the expression of acceptance and its communication to the offeror occur simultaneously and the agreement is accordingly concluded at that time and place. According to the information theory (which applies to all contracts concluded in the presence of both parties) which seems to be a widely applied theory, contract formation and rights and duties related thereto begin when both parties consciously agree upon the terms of the contract.[424]

Although the information theory rests on the principle that the primary basis for contractual liability is the actual and conscious agreement between the contractors, there are exceptions. The general rule is that an agreement is formed only when the acceptance is communicated to the offeror.[425] The implication of this legal rule is that a legal bond will only be created when the offeror is informed of the acceptance for there to be consensus '*ad idem'*. Difficulties do arise, however, when there is an interval between the expression of the acceptance and its communication to the offeror; as in the case of contracts concluded by post. A distinction is therefore made between direct (instantaneous) communication methods and indirect communication methods (non-instantaneous).[426]

The court decided in the case of *Cape Explosives Works v Lever Brothers SA (Ltd.)*[427] that in the matter referring to previous English decisions such as *Adams v Lindsell*[428] and *Henthorn v Fraser*[429] which stated in its judgment that, 'agreements entered into by letter arise at the place and

[423] Eiselen op cit note 291 at 3-49.
[424] Van Aswegen op cit note 407 at 28.
[425] *Rex v Nel* 1921 AD 339.
[426] Papadopoulus & Snail op cit 390 at 52.
[427] 1921 CPD 244.
[428] *Adams v Lindsell [*1818] EWHC KB J59.
[429] *Henthorn v Fraser* [1892] 2 Ch 27.

at the moment when the letter of acceptance is mailed'.[430] This is known as the expedition theory. One must note that this will only apply in instances where the offer was also mailed. It will not apply where the offer was effected in another form to that of post [431] or where the offeror indicated this form of acceptance in his offer [432] as then the postal rule will apply.

The distinction between direct (instantaneous) communication methods and indirect communication methods is aptly demonstrated in the English court's decision on the issue of where a contract is concluded when parties communicate by telephone, telex or telex transmission. In the often quoted case of *Entores Ltd v Miles Far East Corporation Ltd*[433] the court held that a telex is a 'virtually instantaneous' method of communication.[434] The court applied the 'information theory' as the 'instantaneous communication rule' when it held that a telephone conversation is the same as two people communicating '*inter-partes*' (between parties). Accordingly, the contract is concluded at the time and place at which the offeror is made aware of the offeree's acceptance.[435]

This position was also later confirmed in the case of *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft GmbH.*[436]The court had to decide on the time and place of conclusion of the contract, where a fax was sent from London to Vienna. The court held that the general rule on instantaneous communications was applicable but that the acceptance must come to the attention of the offeror or at least constructively come to his attention.[437] The court held that the contract was formed when the offeror became aware of the acceptance.

---

[430] *Cape Explosives Works* op cit note 420 at 266 and at 276.
[431] *Smeiman v Volkerz* 1954 (4) SA 170 (C) at 179.
[432] *Levben Products v Alexander Films* 1959 (3) SA 208 (SR) at 208 -209. Also see the discussion of Kahn et al op cit note 395 at 142- 144.
[433] *Entores Ltd v Miles Far East Corporation Ltd* [1955] 2 QB327.
[434] Ibid at 332.
[435] Ibid.
[436] *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft GmbH* All ER 293.
[437] Ibid at 296.

Similar reasoning was used by South African jurisprudence prior to the ECT Act coming into effect in respect of when and where a contract is concluded in the case where a fax has been used, namely in the case of *Jamieson v Sabingo*[438] where the court held that:

> 'Parties who communicate by telephone, telex or tele-facsimile transmission are "to all intents and purposes in each other's presence", the ordinary rules applicable to the conclusion of contracts made by parties in each other's presence apply, viz the contract comes into existence when and "where the offeree's acceptance is communicated to and received by the offeror".' [439]

Thus, in general, South African law applies the information theory to contracts, where there is direct communication between the parties, and the expedition theory to 'pure' postal contracts, where there is indirect communication between the parties. The *Brinkibon* decision added a layer of complexity to the application of this rule. After the ECT Act took effect, the situation became somewhat different for contracts concluded electronically.[440]

[438] 2002 (4) SA 49 (SCA).
[439] Ibid at 50.
[440] Papadopoulus & Snail op cit note 390 at 52.

(v) Conclusion

After having examined the common law position in South Africa prior to the enactment of the ECT Act one can safely deduce that prior to this Act our courts used to recognise electronic transactions in the course of a commercial transaction and that the reception theory coupled with the information theory would have been the preferred approach to electronic transactions rather than the widely accepted postal rule - also known as expedition theory.

Due to a great level of uncertainty still exists as to which rules apply for the time and place of contract conclusion. One can also accept that the South African law had already developed, in so far as telex and facsimile transmission, in that our courts were willing to accept that formalities pertaining to writing and signatures would suffice where a facsimile and or telex had been sent.

One can only imagine the uncertainty this created on the value of electronic signatures and/or electronic writing which would be more controversial in current times since electronic commerce is now part and parcel of our daily lives.

(a) Legislative development regarding the legal recognition of data messages

Prior to the enactment of the ECT Act there was legal uncertainty as to the use of data messages to communicate messages or to create documentation and whether such data messages have legal validity equal to messages written on paper.[441] It raised such questions as: What is the status of electronic writing and electronic signatures in South Africa? Is an individual or company effectively bound by the correspondence that is entered into by means of electronic communication? When and where are contractual agreements formed and enforceable? As such, conventional legal frameworks governing the offline word were proving to be inadequate in the online word. Therefore it became imperative for the national government to have in place a clear policy and eventually legislation governing electronic communications.

The Minister of Communications commissioned a due diligence survey aimed at identifying laws that could constitute barriers to the development of electronic commerce.[442] The due diligence 'Report on E-

[441] For a view affirming the recognition of data messages prior to enactment of the ECT Act see the case**,** *Council for Scientific and Industrial Research* op cit note 413 which the Honorable Judge was of the view that the new means of negotiation, communication and correspondence was a valid means of expressing intent in an action for repudiation of an employment contract. In terms of the Labour Relations Act 28 of 1956, the mode of repudiation by way of e-mail was regarded as a coherent form of communication of which a printout could form sufficient basis for the plaintiff's action.

[442] Department of Communications, *Discussion Paper on Electronic Commerce* (July 1999).

commerce Legal Issues', prepared by a Johannesburg firm of attorneys, led to the launch of the Discussion Paper on Electronic Commerce [443] The report recommended that South Africa should attempt to adopt most of UNCITRAL provisions with the view to drafting its own primary legislation that would cover e-commerce issues. The report was followed by the Green paper on Electronic Commerce in November 2000. The Green paper emphasised the development of policy for electronic commerce and stated that:

> ' [I]t is targeted at information and communication technology (ICT) experts as well as individuals and enterprises using e-commerce. It addresses some of the challenges regarding e-commerce development and implementation. It is divided into four main themes:
>
> - legal and regulatory issues;
> - building trust in the digital economy;
> - enhancing the information communication infrastructure; and
> - maximising benefits.'[444]

On the 2nd of August 2002, after many years of legal uncertainty, the South African Parliament assented to and brought into force the ECT Act.[445] Prior to its enactment, South Africa had no legislation that comprehensively defined the terms 'writing', 'signature', 'electronic agent', 'automated transaction' and 'originals' in their application to electronic transacting.

---

[443] Dicussion Paper available at : http://www.dpsa.gov.za/dpsa2g/documents/acts&regulations/frameworks/e-commerce/ecomm-paper.pdf released in July 1999 (accessed 10 Ocotber 2013).
[444] Green Paper on E-commerce (2000) available at http://www.gov.za/sites/www.gov.za/files/electronic_commerce_1.pdf (accesed on the 8th October 2013).
[445] Act 25 of 2002.

The preamble to the ECT Act clearly shows that this is a piece of pioneering legislation. The objectives in the preamble read as follows:

> 'To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the republic; to promote universal access to electronic communications and transaction and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected herewith.'[446]

This has managed to fill the *lacunae* that have been building up for many years due to new technological advances that neither the legislature nor the common law had catered for. As such, it has brought much needed certainty into this specific area of law that for many years has lacked certainty.

As one can note from this preamble, the ECT Act has managed to cover extensive areas of South African law. Chapter III of the ECT Act addresses these issues in two parts. The first part deals with the legal requirements for data messages, and the second parts deals with the communication of data messages. This distinction is very important because it creates obligatory provisions from Sections 11 to 20 whereas Part 2 of Chapter III provides default positions in law that are free to vary.[447]

Owing to the fact that the ECT Act also covers more issues relating to electronic communications, its objectives in the preamble are much wider than the objectives of the UNCITRAL Model Laws that only seeks to facilitate rather than impose rigid regulations for e-commerce transactions.

---

[446] *Preamble* to the Electronic Communications & Transaction Act, Act 25 of 2002.
[447] Papadopoulus & Snail op cit note 390 at 46.

(b) Interpretation and sphere of application

When interpreting the provisions of the ECT Act, it must be done in such a way that it does not exclude any statutory or common law from being applied which recognises or accommodates electronic transactions, data messages or any other related matter in the Act.[448] The ECT Act applies to all electronic transactions or data messages.

It is noteworthy that the ECT Act has retained the autonomy principle as contained in Article 4 of the Model Law on E-Commerce and Article 3 of the UNECIC. It therefore also permits the contracting parties to establish requirements that deviate from the suggested prescribed form.

(c) Legal recognition of data messages

The recognition of data messages for the purposes of conducting legally relevant acts has now been entrenched into South African law by virtue of Section 11 of the ECT Act. Section 11 of the ECT Act similarly follows Article 5 and the Model Law on E-commerce as well as Article 8(1) of UNECIC. Section 11 states that:

> '(1) Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.
> (2) Information is not without legal force and effect merely on the grounds that it is, not contained in the data message purporting to give rise to such legal force and effect, but is merely referred to in such data message.

[448] Section 3 of the ECT Act. It is also important to note that the ECT Act applies retroactively to current contract see the case of *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd TA Ecowash and Another* – SCA Case No 72513 .

According to Section 1 of the ECT Act, data messages also include 'data generated, sent and received or stored by electronic means and includes (a) voice, where voice is used in an automated transaction, and (b) a stored record. It also provides that 'data' means of 'electronic representation of information in any form'.

Section 11 is the singular key clause of the ECT Act in that it stipulates that information is, 'not without legal force and effect merely on the grounds that it is not in the form of a data message'. It is important to note that the provisions of Section 11 are not intended to override any mandatory provisions in South African law relating to electronic data messages but, on the contrary, provides that information in the form of a data messages may not be denied legal validity or effectiveness. Section 22 of the ECT Act further confirms that no agreement shall be invalid merely because it was concluded in part or wholly by way of data messages.[449]

The use of data messages is at the parties' discretion and not mandatory. Section 4(2)(a) and (b) of the ECT Act states that the Act does not require any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by or in electronic form or prohibit a person from establishing requirements in respect of the manner in which that person will accept data messages. This is clearly re-emphasised in Article 8(2) of the UNECIC [450] which indicates that the use of electronic data messages is not mandatory but may be done by choice or tacit consent based on the conduct of the contracting parties. In these terms, parties may agree to enter into e-commerce agreements using electronic transactions to give effect to their contractual obligations.

[449] Papadopoulus & S Snail op cit note 390 at 46.
[450] Article 8(2) of the UNECIC states : 'Nothing in this Convention requires a party to use or accept electronic communications, but a party's agreement to do so may be inferred from the party's conduct'.

Eiselen states that there is no actual definition for electronic transactions in the ECT Act. Section 1 of the ECT Act merely provides that an electronic transaction means a transaction of either commercial or non-commercial nature and includes the provision of information and e-government services.[451]

(d) Writing and signature requirements

Section 12(a) and (b) of the ECT Act recognises data as the functional equivalent of writing or evidence in writing. It grants data messages the legal validity equal to messages written on paper. It states that a requirement under law that a document or information be in writing is met if the document or information is in the form of a data message and it is accessible in a manner usable for subsequent reference to a person who either wants to rely on the existence of a particular agreement,[452] or for record purposes.[453]

In the case of *Mafika Sihlali v SABC Ltd*[454] the court had to decide the issue as to whether a SMS sent by an employee tendering her resignation was valid and in written form. The court, in deciding in the affirmative on both issues, held that:

> 'Section 37(4)(a) of the Basic Conditions of Employment Act, requires that notice of termination of a contract of employment

[451] Eiselen 'E-commerce' in Van der Merwe et al (ed) *Information and Communications Technology Law* (2008) at 183.
[452] S L Gerda 'The Electronic Communications and Transactions Act' in L Thornton (ed) *Telecommunications Law* (2004) at 270. Also see Papadopoulus & Snail op cit note at 390.
[453] Section 12 similarly follows Article 6 of the Model Law which states: 'Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference' as well as Article 9 (1) & (2) of the UNECIC which states: '(1) Nothing in this convention requires a communication or a contract to be made or evidenced in any particular form. (2) Where the law requires that a communication or a contract should be in writing, or provides consequences for the absence of writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference'.
[454] [2010] ZALC 1; (2010) 31 ILJ 1477 (LC) ;

> must be given in writing, except when it is given by an illiterate employee, and paragraph 9 of the personnel regulations [in this case the SABC personnel regulations], which similarly refer to notice of termination in writing.'[455]

The court also stated that, 'a communication by SMS is a communication in writing'.[456] Section 12 of ECT Act provides:

> '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 1 defines a 'data message' to mean 'data generated, sent, received or stored by electronic means'. The court also referred to the recent earlier in *Jafta v Ezemvelo KZN Wildlife.*[457] The court in the *Mafika* case held that the applicant's resignation by SMS was therefore a resignation submitted in writing. On the other hand, can a SMS constitute acceptance of an offer of employment? This was the issue determined in the case of *Jafta v Ezemvelo KZN Wildlife.*[458]

Jafta responded to an advert for a vacancy at Ezemvelo KZN Wildlife (hereinafter referred to as 'Wildlife') and attended an interview on 5 December 2006. At the interview, he was offered the position; however, Jafta said he was due to go on leave from 22 December 2006 to 7 January 2007 and wanted to accept the position after his leave. On 13 December 2006 Wildlife's Human Resources (HR) Officer e-mailed the offer to Jafta. The only issue preventing him from accepting the offer was that his notice period was two months and Wildlife wanted him to start on

[455] Ibid para 18.
[456] Ibid. Also see Papadopoulus &Snail op cit note 390 at 46.
[457] [2008] 10 BLLR 954 (LC)
[458] Ibid.

1 February 2007. On 28 December 2006 he received a further e-mail from the CEO of Wildlife confirming that the starting date was non-negotiable and they insisted that he respond by the end of December. Jafta was on leave at this stage and had difficulty e-mailing his acceptance. He finally sent the e-mail from an internet café on 29 December 2006.

The HR Officer denied receiving this e-mail. On 29 December 2006 the HR Officer sent a SMS to Jafta urging him to respond to the offer. Jafta then replied to her SMS confirming that he had responded by e-mail in the affirmative. The HR Officer admitted receiving the SMS; however, she did not recall seeing the word 'affirmative' and argued that it was only a valid confirmation if an e-mail had been sent. Jafta made a note of the SMS and the cellphone was subsequently stolen.[459]

Wildlife offered the position to the next candidate and Jafta claimed breach of contract. The first hurdle was to prove that a contract of employment was concluded on 29 December 2006. The onus fell on Jafta to show that he had in fact accepted the offer of employment.

The court identified five issues for determination:

> '(i) Was the content of Jafta's e-mail an acceptance of Wildlife's offer of employment? (ii) Was the content of Jafta's SMS an acceptance of Wildlife's offer of employment? (iii) Did Wildlife receive Jafta's e-mail? (iv) Is an SMS a proper mode of communicating acceptance of an offer? (v) If Wildlife did receive an acceptance of the offer and a valid contract of employment came into existence, what are Jafta's damages arising from Wildlife's repudiation?'[460]

[459] Ibid. at par 6. Also case discussion by K Staude (2008) 'Acceptance by SMS' available at http://www.webberwentzel.com/wwb/view/wwb/en/page1873?oid=19142&sn=Detail , (accessed on 7 January 2011).
[460] D Colliers 'E-Mail and SMS contracts' (2008) 16 *Juta Business Law* 1 at 20.

The court considered the first four issues in the light of the common law requirements and stated the common law requirements for acceptance are: (a) it must be clear, unequivocal and unambiguous; (b) it must correspond with the offer made; (c) it must be made in the mode prescribed by the offeror; and (d) the offeree must communicate acceptance of the offer to the offeror.[461] The court found that Jafta's e-mail response was a clear and unequivocal acceptance of the offer.[462]

The e-mail confirmed that if Wildlife did not accept his counter-proposal of a start date of 15 February 2007 he would accept the terms as stated. He had requested a copy of the contract by 31 December but this was not a condition of acceptance – he merely wanted the security of the written contract prior to his resignation.

The only sticking point with regard to the offer was the starting date. The CEO had urged Jafta for a response to this issue and the court found that his SMS 'to the affirmative' was in direct response to commencing employment on 1 February 2007. Accordingly, the SMS was an unequivocal acceptance of the offer.

The court further found that the SMS was an appropriate mode of acceptance on the basis that it fell within the meaning of an 'electronic communication' as defined by the ECT Act.[463] The HR Officer had initiated the use of SMS and had demanded an urgent response or risk losing the position. The judge stated: 'An SMS is as effective a mode of communication as an e-mail or a written document'.[464]

The court reasoned that because Wildlife initiated communication by an SMS which asked for an immediate response, and that because Jafta

[461] Ibid at 21.
[462] *Jafta v Ezimvelo* op cit note 458 at par 101.
[463] *Ibid* at par 110.
[464] *Ibid* at par 113.

reciprocated in the same manner that Wildlife had tacitly agreed the SMS was a proper mode of accepting its offer.[465] The judge found that Wildlife had repudiated the contract and awarded general and special damages. The damages included the difference between his present salary and the salary he would have earned with Wildlife to the date of the judgment plus a further three years which was the estimated period of time it would take him to find another job.

Wildlife had argued that the HR Officer was not authorized to accept the offer and that the SMS was only confirmation that an e-mail had been sent; however, this was not accepted by the court. It turned out to be an expensive lesson for the employer. It is advisable to avoid the use of SMS for important matters such as offers of employment. If one initiates text messages with the candidate there is risk that the acceptance may be lost in translation.[466]

Eiselen states that the requirements of Section 12 are stricter than the common law rules on writing as the data message is required to fulfil a formality, the object thereof being to provide legal certainty. There is no point in using a data message if it cannot be saved and later referred to.[467]

The intentions of the legislature are clear from the simple wording of the above provision. Furthermore, Section 22(1) of the ECT Act as stated in Article 11 of the Model Law, guarantees the validity of agreements concluded either partly or wholly by a data message.[468] This is a re-affirmation of section 11.[469] In a nutshell, the ECT Act has entrenched in South African law the recognition of data messages as a functional equivalent to a message written on paper. This would suggest that any

[465] Ibid at par 101. Also see Papadopolous 'Short messages services and e-contracts' (2010) 1 *OBITER* at 192.
[466] Papadopoulus & Snail op cit note 390 at 47.
[467] Eiselen op cit note 452 at 147.
[468] Coetzee op cit note 45 at 516.
[469] Eiselen op cit note 144 at 147.

correspondence in any electronic form would be deemed to a written communication.

To answer the question of whether a signature created by means of a data message is valid, one should look at Section 13 of the ECT Act, which ensures that data messages can satisfy the signature requirement when it states:

> '(1) Where the signature of a person is required by law, 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 data message is not without legal force and effect merely on the grounds that it is in electronic form.
> (3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, that requirement is met in relation to a data message if: (a) a method is used to identify the person and indicate the person's approval of the information contained; (b) and having regard to all 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 having created a valid electronic signature and to have been applied properly, unless the contrary is proved.
> (5) Subsection (4) does not preclude any person from: (a) establishing the validity of an advanced electronic signature in any other way; or (b) adducing evidence of the non-validity of an advanced electronic signature.'

The effect of this section is to give legal recognition to e-signatures. However, where legislation or a common law rule requires a signature, only an advanced electronic signature shall be used.[470]

One can immediately pick up the fact from the previous discussion on international instruments that the functional equivalence and integrity requirements as stated in Article 3 and Article 6 of the UNCITRAL Model Law on E-Commerce have been adopted in this provision. Section 13(2) states that an e-signature shall not be without legal force merely because it is in electronic form and does not necessarily preclude signatures that are not advanced electronic signatures.[471]

What does this confusing and ambiguous wording mean? It means that the principle of technological neutrality has been applied in the form of a two-tiered approach in the sense that both simple and technologically advanced e-signatures are legally accepted for different types of electronic contracts. This is not as per the UNCITRAL Model Laws but has been modelled on the EU Directive on Electronic Signatures.[472]

This means that three different contractual situations arise depending on the type of e-signature. In the first instance, as prescribed by Section 13(2), any e-signature or a distinct electronic mark could be sufficient for the existence of a digital contract.[473] In the second instance, as prescribed by Section 13(1), the e-signature will have to be an advanced electronic signature[474] and it has been noted that in terms of Section 13(1) of

---

[470] Gerda op cit note 452 at 270.
[471] Papadopoulus and Snail op cit 390 at 49.
[472] Ibid. Also see'EU Commission Directive on the Protection of Consumers in Respect of Distance Contracts' (Directive 97/7).
[473] Gerda op cit note 453 at 270.
[474] 'Advanced electronic signature' means an electronic signature, which results from a process, which has been accredited by the Accreditation Authority. Automated transaction means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or the data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment'. Section 1 of ECT Act.

then ECT Act being the third instance it would have to be accredited by the South African Department of Communications (the identified Accreditation Authority as required by Section 13(4) of the ECT Act).[475]

An advanced electronic signature is an e-signature that results from a process which has been accredited by the Accreditation Authority. [476] The ECT Act also prescribes certain criteria that must be met before the Accreditation Authority can accredit an electronic signature service or product.[477] These criteria include that: (a) the signature is capable of identifying the user; (b) the signature is uniquely linked to the user; (c) it is created using means that can be maintained under the sole control of the user; and (d) it 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 is based on the face-to-face identification of the user.[478]

The South African Accreditation Authority (SAAA) released Accreditation Regulations in 2007[479] so that applications for advanced electronic signature accreditation could commence. According to their website LAW - Trusted Third Party Services (Pty) Ltd ('LAWtrust') services or products have been accredited[480] since the 29 March 2012 and it is rendering services to its subscribers of advanced electronic signatures. The South African Post Office (SAPO), the Post Office Trust Centre has also now been accredited as the preferred service provider of advanced electronic signatures.[481] One must mention however that Section 37 of the ECT Act states that all electronic signatures must be accredited by SAAA.

---

[475] Coetzee op cit note 45 at 513.
[476] Accreditation Authority is defined in Section 37 of the ECT Act.
[477] Papadopoulus & Snail op cit note 390 at 49.
[478] Section 38 of ECT Act.
[479] *Government Gazette* No 2995 of 20 June 2007.
[480] LAW trust available at *http://www.saaa.gov.za/accreditation_ProductsServices.htm* (accessed 14 January 2013).
[481] SAPO and Post Office Trust Centre available at *http://www.trustcentre.co.za/personal_certificates.php/* (accessed 28 December 2013) and also *http://www.saaa.gov.za/accreditation_ProductsServices.htm/* (accessed 28 December 2013)

In terms of the Accreditation Regulations a service provider of advanced electronic signatures must comply with the SANS 21188 PKI standard.[482] It means that all prospective applicants who want to be accredited must comply with the minimum standards as per SANS 21188 PKI standard of the South African Bureau of Standards (SABS), a public key infrastructure for financial services with respect to PKI standards.[483]

All certificates issued by an accredited service provider must comply with the International Telecommunications Union (ITU) standard[484] X59 and must contain a certificate serial number to distinguish it from others, a signature algorithm identifier, the name of the certification provider, the validity period of the certificates, the public key, the name of the subscriber of the public key and it must confirm that it is indeed accredited by the South African Accreditation Authority and must have a URL link to its website.

The service provider would also have to adhere to the SABS/ISO17799[485] quality standard regarding information-security management. It is important to note that where the law requires a signature that the electronic equivalent will only be fulfilled if an advanced electronic signature is used.[486] This does not, however, preclude parties by agreement to use a foreign signature or any other electronic signature technique.

The requirement, as such, has not been in incorporated the UNCITRAL Model Law on E-Commerce but has been adopted in the

[482] Section 13 of *Government Gazette* op cit note 472.
[483] Van der Merwe op cit note 452 at 129 and also see Papadopoulus & Snail op cit note 390 at 49.
[484] International Telecommunications Union recommendation on public key and attribute certificates frameworks available at https://www.itu.int/rec/T-REC-X.509-201210-I/en (accessed on the 15 July 2013).
[485] The SANS version is available at *http://www.sans.org/score/ISO_17799checklist.php* (accessed 28 December 2013).
[486] J Coetzee op cit note 45 at 514. Also see Papadopoulus & Snail op cit note 390 at 49.

UNCITRAL Model Law on E-Signatures[487] in Article 2(a)[488] read together with Article 6.[489]

The third and last instance as provided for by section 13(5) is in the instance where an e-signature has not been used at all but the intent to be contractually bound has been expressed.[490] This is akin to the popular click-wrap and shrink-wrap agreements which allow online users to express their intent to contract and allow them to enter into valid purchase and sale agreements with vendors from the internet by clicking a mouse on a specific area of the screen.

Furthermore, Section 13(5) of the ECT Act stipulates that any other expression of intent or 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

[487] UNCITRAL Model Law on E-Signatures Resolution 56/80 op cit note 6.

[488] Article 4(2)(a) reads, '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.

[489] Article 6 reads, '(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:

(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.'

[490] Papadopoulus & Snail op cit note 390 at 49.

evidenced by an electronic signature but is evidenced by other means from which such person's intent or other statement can be inferred.[491]

Parties to a contract may thus agree to use a method other than an electronic signature, to express intent or consent. Electronic contracts may thus be validly concluded through 'click wrap agreements' by clicking on the 'I agree' icon, or by expressing intent to be bound through passwords or any other method from which such intent can be inferred.[492]

De Andrade suggests that the provisions of Section 13(1) and (4) should be read together. This is to avoid any adverse legal consequences in the event of dispute about the validity of the said advanced electronic signature.[493] There are various types of electronic signatures that vary according to the financial resources of the contractors. Some of the 'low-tech' solutions are e-signatures with password protection, a picture scan of a handwritten signature, a light pen, and so on.[494] Other more expensive solutions better known as 'biometrics'. These range from retinal scans, face recognition, finger print, hand print, hand and/or finger geometry and voice recognition.[495]

It is submitted that such unaccredited electronic signatures would carry no weight, 'where the law requires a signature' as it would be 'void ab initio' as the wording of Section 37 (which governs the establishment and functions of the South African Accreditation Authority (SAAA))[496] is mandatory and specifically refers to a South African accreditation authority

[491] Tana Pistorius 'Monitoring, Interception and Big Boss in the Workplace: Is the devil in the details?' (2009) *in Potchestroom Electronic Review* at 6-7.
[492] Ibid .
[493] D Andrade 'Is the Pen Mightier than the Electronic Signature?' (2005) *De Rebus* at 20.
[494] L Brazell *Electronic Signatures Law and Regulation* (2004) at 37-9.
[495] Ibid at 40-2.
[496] South African Accreditation Authority (SAAA) available at *www.saaa.gov.za* (accessed on 3 March 2014).

having to accredit a service provider before a signature could be called an advanced electronic signature.[497]

A foreign service provider is not excluded from the accreditation process and may also apply for accreditation. To date, however, no foreign electronic signatures have been accredited by the South African Accreditation Authority (SAAA). The ECT Act specifically, however, excludes four different instances where an electronic writing or signature would not be valid.[498]

The four excluded acts are: (a) concluding an agreement for the alienation (disposal) of immovable property as provided for in the Alienation of Land Act; (b) concluding an agreement for a long-term lease of immovable property in excess of twenty years as provided for in the Alienation of Land Act;[499] (c) the execution of a bill of exchange as defined in the Bills of Exchange Act; and (d) the execution, retention and presentation of a will or codicil as defined in the Wills Act.[500]

One must however, note the decision of *Macdonald v The Master* [501] where the court held that a court may condone a 'draft will' in the form of an electronically stored document, which was stored on a computer hard-disk may be condoned in terms of Section 2(3) of the Wills Act, if not all statutory requirements have been satisfied, and admit such as valid proof of an existing will.[502] The court used its power to condone a document intended

[497] The Department of Postal Services and Telecommunications (DSTP) hosts the Accreditation Authority. It is the sole body that can accredit 'advanced electronic signatures' that are valid in South Africa. This, however, does not preclude parties from stating in a contract that an advanced electronic signature of certain country will be a valid electronic signature for the purposes of the said contract.
[498] J Hoffman 'The meaning of exclusions in Section 4 of the ECT, Act 25 of 2002', (2007) *South African Law Journal* (2) at 261.
[499] Ibid.
[500] Act 34 of 1964. However see S Snail 'The validity and enforceability of Electronic Wills' (2006) *De Rebus* August at 48.
[501] 2002 5 (SA) O 697 at [71A-B].
[502] Ibid at 6. Also see S Cornelius 'Condonation of Electronic documents in terms of section 2(3) of the Wills Act' (2003) *Tydskrif vir Suid Afrikaanse Reg* at 210.

to be a will in terms of Section 2(3) of the Wills Act by using a computer print-out of the electronic document containing the deceased wishes as an indication of the deceased last wishes.[503]

Arguably, the *Macdonald* decision ought to be extended not only to a draft will but to a will executed electronically and the ECT Act ought to be amended accordingly to make provision for situations that would comply with Section 2(3) of the Wills Act. The proposal for the amendment of the ECT Act would be that an electronic document that has been electronically signed by the testator with an advanced electronic signature be considered to be the testator's last and final wishes.

The facts in the *Macdonald* decision were to become the facts similar to the case of *Hendrik Van der Merwe v Master of the High Court* [504] where the Court had to consider the formalities required in the execution of a will are set out in Section 2(1) of the Wills Act where a draft will was not signed by the Testator. The relevant parts of Section 2(1)(a) of the Wills Act provide that:

> '(a) [N]o will executed on or after the first day of January, 1954, shall be valid unless ─
>
> (i) the will is signed at the end thereof by the testator or by some other person in his presence and by his direction; and
>
> (ii) such signature is made by the testator or by such other person or is acknowledged by the testator and, if made by such other person, also by such other person, in the presence of two or more competent witnesses present at the same time; and
>
> (iii) such witnesses attest and sign the will in the presence of the testator and of each other and, if the will is signed by such other person, in the presence also of such other person; and

[503] Ibid.
[504] 2010 (605/09) ZASCA 99 at par 11.

(iv) if the will consists of more than one page, each page other than the page on which it ends, is also so signed by the testator or by such other person anywhere on the page.'

On the other hand, Section 2(3) of the Wills Act , Act 7 of 53 sets out the power of a court in relation to a will or amendment thereof which does not comply with the prescribed formalities. It reads as follows:

'If a court is satisfied that a document or the amendment of a document drafted or executed by a person who has died since the drafting or execution thereof, was intended to be his will or an amendment of his will, the court shall order the Master to accept that document, or that document as amended, for the purposes of the Administration of Estates Act, 1965 (Act 66 of 1965), as a will, although it does not comply with all the formalities for the execution or amendment of wills referred to in subsection (1).'

It is clear that the formalities prescribed by Section 2(1) and Section 2(2) of the Wills Act in relation to the execution of a will and amendments thereto are to ensure authenticity and to guard against false or forged wills. The court, in finding in the case of *Hendrik van der Merwe*[505] that the draft electronic will was valid, considered the following.[506]

By enacting of Section 2(3) of the Wills Act the legislature was intent on ensuring that failure to comply with the formalities prescribed by the Act should not frustrate or defeat the genuine intention of testators. It has rightly and repeatedly been said that once a court is satisfied that the document concerned meets the requirements of the subsection a court has no discretion

[505] *Hendrik Van der Merwe* op cit note 505.
[506] Ibid at par13.

whether or not to grant an order as envisaged therein.[507] In other words, the provisions of Section 2(3) are peremptory once the jurisdictional requirements have been satisfied. Turning to the provisions of Section 2(3) the first question to be considered is whether the document in question was drafted or executed by the deceased. Following on this, is the question whether the deceased intended it to be his will which the court answered by referring to the case of *Letsekga v the Master & Others.*[508]

In *Letsekga v the Master & Others*[509] the following was stated:

> 'The wording of Section 2(3) of the Act is clear: the document, whether it purports to be a will or an amendment of a will, must have been intended to be the will or the amendment, as the case may be, i.e. the testator must have intended the particular document to constitute his final instruction with regard to the disposal of his estate.'

The lack of a signature has never been held to be a complete bar to a document being declared to be a will in terms of Section 2(3).[510] In the court case of *Letsekga,* the lack of a signature was not held to be a bar to an order in terms of Section 2(3) of the Act. In the matter of *Ex parte Maurice*[511] which was decided in the same year as *Letsekga,* was to the same effect. In *Thirion v Die Meester & andere*[512] an unsigned document drafted by a person shortly before he committed suicide was held to be a valid will and declared as such in terms of Section 2(3). In that case the deceased had executed a prior will that had complied with all the prescribed formalities.

[507] Ibid. at par 14.
[508] 1995 (4) SA 731 (W).
[509] Ibid. at par 735F-G.
[510] *Hendrik Van der Merwe* op cit note 505 at par 16.
[511] 1995 (2) SA 713 and 1995 (2) SA 713 1.
[512] 2001 (4) SA 1078 (T).

The object of Section 2(3), is to ameliorate the situation where formalities have not been complied with but where the true intention of the drafter of a document is self-evident.

A review of the decided cases[513] reveals the following regarding Section 2(3) of the Act:

> 'Section 2 (3) is in the nature of a special exemption from the rigours of the requirements of Section 2 (1)' and the cases cited above indicate that the absence of a signature has not been seen as a bar to relief in terms of Section 2 (3). On the other hand, it must be emphasised that the greater the non-compliance with the prescribed formalities the more it would take to satisfy a court that the document in question was intended to be the deceased's will'.[514]

The court, in *Hendrik van der Merwe v The Master*[515] then went to consider the document in question against the jurisdictional requirements of Section 2(3) of the Act. The appellant had provided proof that the document had been sent to him by the deceased via e-mail, lending the document an aura of authenticity. It was uncontested that the document still existed on the deceased's computer and was genuine. Thus it was clear that the document was drafted by the deceased and that it had not been amended or deleted. In explaining its satisfaction with that requirement, the court stated: [516]

> 'The document is boldly entitled "TESTAMENT" in large type print (6 mm high), an indicator that the deceased intended the document to be his will. Furthermore, the deceased nominated the appellant as the sole beneficiary of his pension fund proceeds.'

[513] See also the cases of *Ramlal v Ramdhani* 2002 (2) SA 643 (N) and *Back and Others NNO v Master of the Supreme Court* (1996) 2 All SA 161 (C)
[514] *Hendrik Van der Merwe* op cit note 505 at par 16.
[515] Ibid.
[516] Ibid. at par 17.

This was an important and objective fact which is consonant with an intention that the appellant be the sole beneficiary in respect of the remainder of his estate. It was also of importance that the deceased had no immediate family and that the appellant was a long-time friend and confidante.[517]

The fact that his previous will nominated the second respondent as his sole heir indicates that he had no intention of benefiting remote family members. The appellant's version of the mutual agreement to benefit each other exclusively by way of testamentary disposition is uncontested by the second respondent, the sole beneficiary of the prior will, and is supported by the fact that after the deceased had sent the document to the appellant, the latter executed a will nominating the deceased as his sole beneficiary ─ another objective fact. All of this leads to the inexorable conclusion that the document was intended by the deceased to be his will.[518]

It is submitted that the legislature ought to consider the law relating to the inclusion of the above-stated excluded acts every five years similar to German law, as Vogel suggests, to accommodate changing times.[519] The main purpose behind considering the law over such a generally short period is to provide equal treatment to the use of the various e-signature techniques currently being used or still under development with the purpose of replacing the use of hand-written signatures and other kinds of authenticated mechanisms used in the traditional paper-based transaction (e.g. seals or stamps).[520]

There are two key considerations that would have to be considered when dealing with an electronic will, one of the them would be the

[517] Ibid at 18.
[518] Ibid.
[519] H J Vogel 'E-commerce: Directives of the European Union and Implementation in German law' in D Campbell and S Woodley (eds) *E- Commerce: Law & Jurisdiction* (2003) at 53.
[520] Papadopoulus & Snail op cit note 390 at 51.

requirement of the witnesses being in each other's presence and that of the testator. The second other important requirement is that they (the witnesses) sign the will in each other's presence. These areas would require some further investigation on how they can be overcome in terms of the functional equivalence approach.

(e) Time and place that the contract enters into effect

South African law makes provision for different methods of contract acceptance as discussed in Chapter IV of this work. Such methods of contract acceptance could vary and affect the time and place of contract conclusion. The place where a contract is formed is very important in case of a contract between parties who are in different jurisdictions, or where one party suffers prejudice due to conflicting legal rules.[521] The determination of where the contract comes into existence is also important as the 'lex loci contractus' of a particular country may insist on particular formalities that must be complied with for an agreement to be valid as well as the 'lex loci' solution when having to consider where performance must take the place of contractual obligation.[522]

The moment and place of contract conclusion of electronic contracts are now being regulated by Section 22(2) of the ECT Act which states: 'An agreement concluded between parties by means of data messages is concluded at the time and place where the acceptance of the offer was received by the offeror'.[523]

[521] Eiselen op cit note 452 at 161.
[522] Ibid.
[523] See discussion by Papadopoulus & Snail op cit 390 at 53.

As one can see, the time and place of contract conclusion are where and when the originator receives the addressee's [524] message of acceptance, unless the parties have agreed otherwise.[525] For our purposes, it is only important to look at both the information theory and the expedition theory as explained in the case of a contract concluded by letter and/or telephone or fax – as these are akin to e-mail. The ECT Act has rejected the expedition theory and has now introduced the reception theory as a preferred legal rule when determining the place where the agreement has been concluded.[526]

The ECT Act's provision is clearly a deviation from our two traditional common law theories i.e. the information theory and the expedition theory, and is a modified version of the reception theory where the risk of the message being lost or not reaching the addressee is placed squarely on the sender.[527] The wording of these sections has also been questioned in light of the problems surrounding the malfunction of information systems.[528]

One must also note that the provisions of Section 22(2) are only applicable where the parties have not by express agreement varied the rules of the ECT Act by means of contractual determination.[529] Since the transmission of data messages usually occurs in the manner of the sender's computer sending small data packets that eventually arrive at the recipient's computer to form the original message, it could become technical in certain instances when trying to establish the exact time when the messages are deemed to have been received. [530]

---

[524] 'Addressee' in respect of a data message means, a person who is intended by the originator to receive the data. This can person can also be referred to as the offeree in terms of the law of contract section 1 of the ECT Act.
[525] J Coetzee op cit note 45 at 517. Also Eiselen op cit note 452 at 162.
[526] Eiselen op cit note 452 at 162. Also Papadopoulus & Snail op cit 390 at 53.
[527] W Jacobs 'Sale of medicine over the Internet' (2005) 11 *SAMLJ* 17 at 241. The use of the reception theory has been criticized, see for example Lötz and Du Plessis op cit note 50 and defended by D Van der Merwe op cit note 452 at 151.
[528] S Papadopoulos op cit note 390 at 188.
[529] Section 21 of ECT Act.
[530] 'A data message – (a) Used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information'

The rules pertaining to time of sending and receipt of data messages set out in Section 23 of the ECT Act. Section 23 provides for different scenarios[531] by virtue of Section 23 (a), which deals with the status of electronic data messages that are sent, and states:

> '[D]ata message - *(a)* used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee.'

Furthermore in terms of Section 23(b):

> 'A Data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee.'

In the situation, as stated in Section 23(a) the e-mail is deemed to be sent when accessible by the recipient on sending it through the intra-mail or when the complete data message enters an information system outside the sender's control in the case of parties in two different information systems.[532] Eiselen states that the e-mail message or SMS is deemed to have been sent when it leaves the originator's server.[533]

---

system ,when it is capable of being retrieved by the addressee; (b) must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee; and (c) must be regarded as having been sent from the originators usual place of business or residence and as having been received at the addressee's usual place of business or residence.

[531] Papadopoulus & Snail op cit note 390 at 53.

[532] Ibid.

[533] Eiselen op cit note 452 at 152.

Section 23(b), on the other hand, states that the e-mail will be deemed received when the complete data message enters the designated (or whatever is used for that purpose) e-mail address for the recipient's information system and it is capable of being retrieved.

In the case of *Jafta v Ezemvelo Kzn Wildlife* [534] the judge applied the ECT Act law in resolving the dispute that had arisen regarding the use of SMS and e-mail for an employment contract,[535] and the exact time and place where the contract was concluded with reference to the common law and ECT Act. The court had an opportunity to interpret this provision where there was a dispute as to whether an e-mail containing an acceptance of an employment contract had indeed been received by the employer.

In rejecting the application of the common law principles the court stated that it is clear that: 'Section 23 supplants the general rule of the common law that an acceptance must come to the knowledge of the person it has been sent to'.[536] The court went to the extent of doing a comparative review of the model law and foreign decisions to confirm the legal position that the reception theory applies in cases of electronic contracts. The court also confirmed that an electronic employment contract can be formed by way of e-mail or SMS.

Section 23(c) attributes the sending of the originator's e-mail at his/her place of business and the same reasoning is applied to receipt. The ECT Act is clearly a deviation from our two traditional common law theories of information and acceptance with regard to the use of electronic data messages and appears to be a modified version of the reception theory.[537] Article 15(1)(2)[538] of the UNCITRAL Model Law on E-Commerce and

[534] [2008] 10 BLLR 954 (LC).
[535] Colliers op cit note 461 at 21.
[536] Ibid at 41.
[537] Jacobs op cit note 528 at 251. Also see Eiselen op cit 127 at 162.
[538] Article 15 reads: '(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the

Article 10 [539] of the UNECIC lay down some basic principles regarding the dispatch and receipt of data messages and are embodied in Section 23(a) and (b) South Africa does not follow the principles of the Model Law to the tee as it requires the full data message to have entered the information system. The ECT Act also does not address the time of receipt where an information system other than the senders designated system is used.

(f) Attribution of data messages

Prior to the ECT Act there was no specific law to deal with attribution of data messages. The ECT Act recognises, for example, that a contract may be concluded with either party using an electronic agent. Nonetheless, a party using an electronic agent to conclude a contract is not bound if the terms of the agreement were not capable of being reviewed by a natural person representing that party prior to formation of the contract.[540] Section 25 of the ECT Act states that:

---

control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or (ii)if the data message is sent to an information system of the addressee that is not stelznerthe designated information system, at the time when the data message is retrieved by the addressee;

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.'

[539] Article 10 reads: '(1) The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

(2) The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.'

[540] Gerda op cit note 453 at 274.

> ‘a data message is that of the originator if it was sent by the originator personally, a person who had authority to act on behalf of the originator in respect of that data message or an information system programmed by or on behalf of the originator to operate automatically unless it is proved that the information system did not properly execute such programming.‘

This creates a rebuttable presumption that a message is that of an originator using any information until he can prove that it was sent in error or as a result of unauthorised or fraudulent use.

(g) Shrink wrap, click wrap, web wrap agreements

Traders and consumers have, through the years, exploited the possibilities of e-commerce. Prior to the ECT Act, there was a lot of uncertainty as to the validity and the enforceability of shrink wrap, click wrap and web wrap agreements.

Fortunately, Section 13(5) of the ECT Act stipulates that any other expression of intent or 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.[541]

Incorporation by reference, which is discussed below, is a technique used widely in commerce to include standard terms and conditions in a contract and can be found in, for example: (a) insurance contracts where an applicant for insurance can be telephonically informed that the standard terms and conditions apply to the contract; (b) an application form which contains a reference to the fact that standard terms and conditions apply; or (c) notice boards at the entrance to business premises that warn that entrance

[541] Pistorius op cit note 492 at 6-7.

is at own risk, and that liability is not accepted for any damages sustained while on the premises.[542]

Inevitably, in disputes regarding these types of contracts, the question arises about whether or not a party is bound by these standard terms and conditions that were incorporated into the agreement. This question is usually answered with reference to the requirements set out in terms of the so-called 'ticket contracts'. According to Christie the contracting party will be bound to these terms and conditions if the following questions can be answered in the affirmative:

> 'a) Did the contracting party know that certain words appeared on the document/ ticket i.e. did they read it?
> b) Did the contracting party know that these terms and conditions referred to a contract/to contract terms and conditions?'[543]

If the answer to both questions is in the affirmative, the contracting party will be bound to the contract terms and conditions. Should the answer, be in the negative then a third question is asked:

> 'c) Did the party issuing the contract/ ticket do everything in his/her power to draw the attention of the other contracting party to the fact that the words refer to the terms of the contract would a reasonable customer have taken notice of the terms and conditions?'

If this third question is answered in the affirmative, the contracting party will be bound to the terms and conditions as stipulated; if not, then they will not be bound by them.[544] These uncertainties are mainly due to the shift from paper-based trading to the practical, paperless conclusion of contracts. The law has evolved certain principles concerning the so-called ticket cases

[542] Papadopoulus & Snail op cit 390 at 53-4.
[543] Christie op cit note 381 at 179.
[544] Ibid.

to dispense with the requirement of obtaining signatures to signify consent.[545]

These contracts are, by nature, defined as contracts of adhesion-contract negotiation and are excluded as one simply, unilaterally declares his/her acceptance.[546] A shrink wrap agreement is one form of a contract of adhesion. Other terms used for this type of agreement are 'box top', 'tear me open' or 'blister pack' agreements.[547] The terms of the agreement become valid and enforceable when the plastic shrink wrap is broken and/or the software package is installed.[548]A retailer's failure to draw the buyer's attention, specifically to the conditions and terms contained in the shrink wrap agreement may amount to a misrepresentation by silence,[549] 'rendering the contract voidable'.[550]

Akin to the concept of shrink wrap agreements are the 'click wrap', agreements, also known as 'web wrap' agreements that have been developed in e-commerce.[551] If the online consumer[552] wishes to purchase products offered through an e-shop he/she will be instructed to 'click' on certain icons indicating his her acceptance to the terms. Courts in the United States have ruled on the enforceability of shrink-warp and web-wrap agreements on the basis of the facts of each case.[553]

In *Hotmail Corporation v Van Money Pie Inc*[554], Judge James Ware of the U.S. District Court for the Northern District of California granted the

[545] T Pistorius 'Click Wrap and Web Wrap Agreements' (2004) 16 *SAMLJ* at 568.
[546] Ibid.
[547] Papadopoulus & Snail op cit 390 at 54.
[548] Pistorius op cit note 3 at 292.
[549] Ibid.
[550] *Kempstone Hire v Snyman* (1988) (4) SA 465 (T) at 468 H.
[551] Ibid.
[552] 'Consumer' means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier. See section 1 of the ECT Act.
[553] Papadopoulus & Snail op cit note 390 at 53.
[554] *Hotmail Corporation v Van Money Pie Inc* C 98-20064 (N.D. Cal , April, 20 1998) also see the Canadian Position in the case of *North American System Shops* 68 ALR 145 (Can

plaintiff's motion for an injunction in trademark infringement and breach of contract suit involving a click wrap agreement on the basis that the defendant had breached one of the 'Terms of Service' namely, 'not to use the Hotmail e-mail account to facilitate the transmission of unsolicited commercial email, otherwise known as "spam"'.[555] One must note that the court's approach towards these forms of agreement is extremely cautious. The defendants usually raise the 'did not know' or 'did not see' online agreement defence.[556]

Although these click-wrap agreements have not yet been tested in our South African courts, Pistorius states, 'there would appear to be no reason as to why they should not be enforceable'.[557] Compared to shrink wrap agreements, where the contract terms are unread until the purchaser has unwrapped the software, with click wrap agreements the customer is aware of the contractual terms before a commitment is made to acquire the goods or services.

The ECT Act decided to ensure legal certainty in this arena and therefore incorporation by reference in electronic transactions is governed by the provisions of Section 11 of the ECT Act. To accommodate these types of transactions the ECT Act sets down the requirements for enforceable incorporation by reference transactions as follows:[558]

QB 1989) where the court hinted at the probability of such contracts being valid and enforceable.

[555] S Nagalingam op cit note 37 at 20.

[556] *Ticket Masters Corporation v Tickets Inc No* Cv 99-7654, 2000 WL 525390 (CD Cal 27 *March 2000)* and *Spreht Netscape Communications Corporation 150 F supp* 2d 585 (SDNY 2001) . For further examples of United States case law were the court refused to recognise the validity of the similar shrink-wrap agreements was in the case of *Vault Corp.v Quid Software Ltd* 847 F. 2d 255(5th Cir.1988*)* and *Systems Inc. v. Wyse Tech* 939 F 2d 91 (3rd Cir. 1999).

[557] Pistorius op cit note 546 at 292.

[558] Ibid.

‘ • Information is not without legal force and effect merely on the grounds that it is not contained in the data message, but is merely referred to in a data message;[559]

• Information is incorporated into an agreement or data message, even though it is not in the public domain only if the information is:

- Referred to in a way in which a reasonable person would have noticed it and
- Accessible in a form that can be read, stored and retrieved by a contracting party, either electronically or as a computer printout.’ [560]

This section clearly reflects the common law position as being the objective test of incorporation by reference as discussed in the case of *Durban's Water Wonder Land v Botha*,[561] which comprises three elements, namely: first, would the reasonable person have expected terms and conditions of that nature at a resort of that nature? Secondly, were the terms and conditions displayed where one would have reasonably expected them to be displayed, in various languages and in clear and eligible print? Thirdly, were the terms and conditions what may reasonably have been expected, given the nature of the activities?[562]

The translation of these requirements to the online world could be: first, would the reasonable user have expected terms and conditions of that nature as being applicable to that message? Secondly, were the terms and conditions displayed where one would have reasonably expected them to be displayed, in various languages and in clear and eligible print? Thirdly, were

[559] Section 11(2) ECT Act.
[560] Section 11(3) ECT Act.
[561] 1999 1 All SA 411 (A).
[562] Pistorius op cit note 546 at 1.

the terms and conditions what may reasonably have been expected, given the nature of the activities?[563]

New and different standards for incorporation by reference have been created in Section 11(3), which could cause confusion. This section embodies the common-law approach but adds the requirement that the information to be incorporated needs to be available to the other party online. Uniform resource locators (URLs), which direct the reader to the referenced document, may, for example, be embedded in a message. Such URLs can provide 'hypertext links' allowing the reader to use a pointing device (such as a mouse) to select a key word associated with a URL. The referenced text would then be displayed.[564]

In assessing the accessibility of the referenced text, factors to be considered may include: (a) availability (the hours of operation of the repository and the ease of access); (b) the cost of access; (c) integrity (verification of content, authentication of the sender, and a mechanism for communication error correction); and (d) the extent to which the referenced text is subject to later amendment (notice of updates; notice of policy of amendment). It has been noted that Section 11(3) should be abolished, as it increases the common law burden of incorporation by reference.[565]

Due to the possibility of exploitation, Section 11(3) requires the website owner, electronic trader or issuer of the terms and conditions incorporated by reference to ensure that the terms and conditions can be read, printed out, stored electronically and that they are retrievable before these terms and conditions will be deemed to have been properly incorporated – a slight deviation from the general common law rule.

[563] Ibid at 2-3.
[564] Ibid.
[565] Ibid.

*(h) Automated transaction***s**

An automated transaction is an electronically concluded transaction where one or both of the parties make use of automated systems. (i.e. a software programme that communicates with or responds to third parties without any human intervention.)[566] When dealing with automated transactions, the analysis of offer and acceptance at common law level provides assistance in determining whether parties have, objectively speaking, reached consensus but may not always be helpful in establishing whether there is subjective consensus or whether the agreement was vitiated by mistake.[567]

In the case of *Sonop Petroleum v Papadogianis*[568] the court made it clear that sometimes it is necessary to qualify the generally subjective approach to consensus by holding a person liable due to their conduct which may instil the reasonable belief that a party may have reasonably relied on [569] - in this case the reliance could be either way, from the e-consumer's perspective or that of the e-vendor. In the case of *Sonop Petroleum v Pappadogianis* the appeal court unanimously believed that the signatory was misled and that the other party was alive to the real possibility of a mistake and that he had a duty to speak but chose instead to snatch a bargain.[570]

One must immediately note that section 1 of the ECT Act which defines a 'consumer' as:

[566] In terms of Section 1 of the ECT Act 'automated transaction' means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment.
[567] Eiselen op cit note 127 at 158.
[568] 1992 (3) SA 234 (A) at 56.
[569] Ibid. Also see the article of Eiselen op cit note 127 at 158.
[570] *Sonap* op cit note 569 at 56.

> 'any natural person who enters into or intends entering into an electronic transaction with a supplier as the end user of goods or services offered by that supplier. '

A consumer only means 'natural person' and therefore the provisions thereof do not apply to transactions between suppliers and companies and other juristic persons such as businesses and trusts.[571] Section 22(1) of the ECT Act states that, 'an agreement is not without legal force and effect merely because it was concluded partly or in whole by means of data messages'.

Section 24 of the ECT Act provides for the valid expression of intent by means of a data message.[572] This section strengthens the provisions of Section 11 and Section 22, and solidifies the legal effectiveness of data messages used in transactional communication.[573] Validity is also provided for unilateral 'statements' by means of data messages.[574]

Fortunately, the ECT Act has now clarified the position regarding the conclusion of contracts with electronic agents.[575] Section 20 has created a statutory regime[576] for the validity and enforceability of automated

[571] See the view of R Buys 'Online Consumer Protection and Spam' in *Cyberlaw @ SA II: The Law of the Internet in South Africa*,(2004) R Buys (ed) at 142. Also the view of B Rheeders, 'Managing e- business: A Business Approach to Legal Aspects', Paper presented at Melrose workshop on the 'Legal Ramifications in Information Technology & Cyberspace', 27th -28th July 2006 – Johannesburg at 2.

[572] See the view of T Pistorius op cit note 233 at 8. Also R Meiring 'Electronic Transactions' in *Cyberlaw @ SA II: The Law of the Internet in South Africa,* (2004) R Buys (ed) at 99.

[573] Ibid.

[574] Section 24 (1) of the ECT Act.

[575] Section 1 of the ECT Act defined a 'Electronic agent' as , 'a computer programme or an electronic or other automated means used independently to initiate an action or respond to data message or performances, in whole or in part, in an automated transaction.'

[576] Section 20 of the ECT Act provides that for an automated transaction:
(a) an agreement may be formed where an electronic agent performs an action required by law for agreement formation:
(b) an agreement may be formed where all parties to a transaction or either one of parties uses an electronic agent
(c) a party using an electronic agent to form an agreement is, subject to paragraph
(d) presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement:
(d) a party interacting with an electronic agent to form an agreement is not bound by the terms of the agreement unless those terms were capable of being reviewed by a natural person representing that party prior to agreement formation.

transactions. In terms of Section 20(a) and 20(b) of the ECT Act, a party as well as the party on whose behalf a computer or electronic agent has been programmed, will be bound to the pre-programmed actions of the automated message system. Section 20(c) provides that a party using an electronic agent to form an agreement is, subject to the provision of paragraph (d), which state that a person is presumed to be bound by the terms of that agreement irrespective of whether that person reviewed the actions of the electronic agent or the terms of the agreement.[577] Section 20(c) is in line with South African common law.[578]

Section 20(d) has new important consequences, in that it gives the party contracting with an electronic agent the right to review the transaction failing which the party will not be bound to the terms as stated.[579] Section 20 (e) also specifies the procedure to be followed in the case where a party makes a material error and wishes to cancel the contract.[580] Eiselen is of the view that it is similar to the common law position on mistake and states that the provisions of section 20(e) are cumulative and that all requirements must have been fulfilled to escape contractual liability.[581]

The person making use of an electronic agent is saddled with a heavy burden in that it must not only provide the natural person with an opportunity to correct the error, it must also provide that person with the opportunity to prevent the error. To be entitled to this protection, it is

[577] T Pistorius op cit note 233 at 9.
[578] Ibid.
[579] Eiselen op cit note 452 at154.
[580] Section 20(e) provides that 'no agreement is formed where a natural person interacts direct with the electronic agent of another person and has made a material error during the creation of a data message and -
(i) the electronic agent did not provide that person with an opportunity to prevent or correct the error:
(ii) that person notifies the other person of the error as soon as practicable after that person has learned of it;
(iii) that person takes reasonable steps, including steps that conform to the other person's instructions to return
any performance received or if instructed to do so to destroy that performance: and
(iv) that person has not used or received any material benefit or value from any performance received from the other person'.
[581] Eiselen op cit note 452 at 159.

required that a natural person must notify the other party of any mistakes as soon as such mistake is noticed.[582] It is clear that automated transactions are now part of our South African law of contract and certain principles have derived from some of our old common law principles.

(i) Jurisdiction in cases of e-contracts and transborder contracts

Cyberspace holds many opportunities for e-commerce but unfortunately, cyberspace is not 'Eden'. Instead, the internet is driven and frequented by people and wherever you find people you are bound to find disputes.[583] Electronic commerce, however, by its very nature is transborder. It doesn't acknowledge geographical borders or jurisdictional principles that recognise state, unions and trade areas but only networks, domains, servers and clouds.

This leaves the courts in a predicament as to which laws to apply to certain disputes and in which forum. The place a contract is formed or breached is mainly of interest in international transactions where the parties have not agreed to a specific jurisdiction or where there is no applicable international convention that determines jurisdiction.[584]

While the recognition of electronic data messages and electronic signatures as functional equivalents to writing and signing have been internationally recognised and much international uniformity exists, one of the most vexatious legal problems in the regulation of electronic commerce, relates to the issue of jurisdiction. When concluding a contract in the online environment it becomes a legal problem to establish which court has jurisdiction and which laws may apply to disputes that may arise out of the contract. There are different views on how jurisdiction of an online contract should be established.

[582] T Pistorius op cit note 233 at 13.
[583] Nagalingam op cit note 37 at 35.
[584] Buys op cit note 11 at 164.

Cyber-libertarians favour a separate cyberspace jurisdiction, maintaining that online activities should be regulated entirely separately without recourse to national courts and laws.[585] Traditionalists maintain that the existing paradigms of location and activity are capable of determining the jurisdiction of a court to adjudicate upon an online contract.[586]

Jurisdiction is the legal term used to describe the power or competency of a court to hear a dispute and decide disputes.[587] Sibanda states that the classic definition of the term 'jurisdiction', which has been incorporated into its traditional understanding, was given by the court in *Ewing McDonald & Co v M & M Products Co.*[588] The court defined 'jurisdiction' as the 'power vested in a court to adjudicate upon, determine and dispose of a matter'.[589] Thus, for the court to exercise jurisdiction, such court must satisfy two requirements. Firstly, the court must have the authority to hear the matter, and secondly, it must have the power to enforce its judgment.

The first requirement is satisfied when there is a jurisdictional connecting factor, which means that there is a link between the court and the parties to the action or the cause of action. The second requirement is derived from the principle of effectiveness in terms of which the court should not exercise jurisdiction unless compliance with its judgment can be expected.[590]

---

[585] L Gillies 'Addressing the Cyberspace Fallacy: Targeting the Jurisdiction of an Electronic Consumer Contract' (2008) 16 *IJLIT* 3 at 242.
[586] Ibid.
[587] Ibid. Also see definition in Poznak Law Firm Ltd (2000) Internet Guide at 1 available at *www.poznaklw.com/articles/cyberjuris.html* (accessed 20 September 2003) which states 'Jurisdiction refers to a courts power to compel you to physically appear in a distant forum to defend or prosecute a lawsuit' as cited in Snail op cit note 16 at 18.
[588] O Sibanda 'Civil Jurisdiction in International e-disputes in the South African Magistrates'Courts: A case of Gaps and Complexities' (2008). Paper presented at the Convention on 'Lex Informatica: The Law on Electronic Communications, Electronic Commerce and Information Technology' 2008 at 4, Pretoria, South Africa.
[589] *Ewing McDonald &Co v M & M Products* Co 1991 (1) SA 252 (AD) at 5.
[590] As previously in Sibanda op cit note 589 it is stated therein that 'traditional common law and statutory 'ratione jurisdictionis' or jurisdictional links may be applied to e-jurisdiction disputes. The 'rei sitae' principle (place where the property is situated if such property is the

Generally speaking, the public international law principle of territorial sovereignty provides that the courts of any given country only have jurisdiction over the individuals or companies who reside within that country, or over the activities (including transmissions) that occur within the borders of that country.[591] A contract is concluded at the time and place where the last act necessary to constitute the agreement, was performed. In terms of Section 22(2) of the ECT Act, the place and time of contract conclusion would be at the place and time where the originator receives the addressee's message of acceptance - this would be the last legally relevant act. [592] But does this mean that a party may approach a South African court in the case of a dispute? The matter becomes even more complex where one or more parties to the agreement are in different jurisdictions.

Eiselen states that Section 19(1)(a) of the Supreme Court Act[593] empowers any Provincial or Local Division of the South African High Court's jurisdiction in South Africa over all persons or all legally recognisable causes of action arising within its area.[594] The courts interpret this as simply meaning that the common law principle must be applied when establishing jurisdiction. [595] A party will have to satisfy one of the following four common law requirements to be heard, granted relief and to be able to take execution steps in a South African court. The South African business or person being sued must conduct business or be domiciled within a specific court's jurisdiction,[596] the cause of action must have arisen within the court's area of jurisdiction,[597] or the foreign party must have expressly, by way of

---

subject matter of the suit); 'ratione domicilii' (the place of domicile of the defendant); locality or residence of the defendant; and 'ratione rei gestae' (the cause of action). The generally accepted rule in South African law is that a contract must be determined according to the 'lex loci contractus' of the last legally relevant act.'

[591] Werkmans Inc. op cit note 25 at 15.

[592] Snail op cit note 16 at 18.

[593] Act 59 of 1959.

[594] Eiselen op cit 127 at 171.

[595] Sibanda op cit note 589 at 4.

[596] Eiselen op cit 127.

[597] *Leobowitz t/a Lee Finance v Mhlana* 2006 (6) SA 80 (SCA) also see the case of *Federated Insurance Werks Co Ltd v Malawana* 1986 (1) 751 (A) were the court *a quo*

submission,[598] or implied consent to jurisdiction of a particular court or the foreigners assets must be attached to confirm jurisdiction.[599]

South African companies that provide international access to their websites and transact electronically with citizens from around the world should ensure that all their website terms and conditions and all other cross-border electronic contracts should include a 'Choice of Court' clause and a 'Submission to Jurisdiction clause'.[600] Jurisdiction however still remains a legal chameleon and a party cannot be completely sure as to which court will have or accept jurisdiction in the case of a dispute that arise from a transnational electronic transaction.

It is quite clear that jurisdiction will remain a worldwide legal uncertainty as courts will not easily bow down to court orders from courts from other jurisdictions which may, in certain instances, hinder or may make litigation expensive and unaffordable for a plaintiff. It would be in the interest of all states in the world to draft another model law that specifically deals with disputes arising from contracts concluded or delicts committed on the internet.[601]

---

held that where a company has a branch office within the jurisdiction of the court that place should be regarded as its principal place of business for purposes of jurisdiction and *Bisonboard Ltd v K Braun Woodworking Machinery (Pty) Ltd* [1990] ZASCA 86; 1991 (1) SA 482 (A) at 496 C.

[598] *Jamieson v Sabingo* op cit note 431.

[599] See *Veneta Mineraria Spa v Carolina Colleries (Pty) Ltd* (In Liquidation) 1987 (4) SA 883 (A) at 994) and O Dean 'Stalking the sleeping Lion' *De Rebus* July 2006 at 20.

[600] Ibid.

[601] Papadopoulus & Snail op cit note 390 at 58.

(j) Conclusion

In short, the ECT Act has now entrenched the law reorganising electronic data messages for the purpose of executing valid legal acts such as the legal formalities of writing and signatures. It appears as if the principles contained in the UNCITRAL Model Laws for E-Commerce and E-Signatures have been entrenched in our South African law. The ECT Act follows a similar legal regime to that of the Singapore,[602] Germany and the United States.. It is noteworthy to mention that the ECT Act also provides for electronically giving power of attorney and commissioning of electronic documents. The law, ought to be regularly revisited as some important current commercial legal acts have been excluded and new technologies being developed could give sufficient reason to reform the law to incorporate them in the scope of the ECT Act. The validity of the electronic Will should also be revisited and research in the area must be taken further.

The ECT Act has also now adopted the reception theory as a legal rule regulating the time and place where a contract enters into effect, which is in line with international best practice. There is no longer any legal uncertainty as to whether click wrap, web wrap agreements and online automated transactions are valid in South Africa. The question of whether a South African court has jurisdiction is generally governed by common law principles and principles of private International law.

The ECT Act only regulates jurisdiction in the case where a criminal matter comes before a South African court and perhaps this aspect should be revisited to create clarity at least from a South African perspective. It would be step in the right direction if the recently proposed amendments to the

[602] Phang & Seng op cit note 116. Also see section 4(1) of the Electronic Transactions Act 1998.

ECT Act could also encompass the proposed measures as contained in UNECIC and the AU Convention on Cyber Security.

CHAPTER VI: REGULATION OF E-CONTRACTING IN THE UNITED STATES

(*a) Overview of chapter*

The technological evolution and development of the internet took the United States and the whole world by storm. It was clear that the United States government would have to give a clear legislative response to its legal ramifications. In July 1997, the Clinton administration remarked that, 'we are on the verge of another revolution . . . the internet [is] changing the way we work, learn and communicate with each other . . . the internet dramatically lowers costs and facilitation of commercial transactions.'[603]

As previously mentioned, United States e-commerce law is now regulated by the UCITA,[604] UETA,[605] and Electronic Signatures in Global and National Commerce Act (E-Sign).[606] The UCITA was passed in 1999 and in the same year the National Conference of Commissioners of Uniform State Laws endorsed the UETA and soon thereafter the E-sign Act was passed amid concerns that the UETA might be adopted too slowly.

(b) Sources of law in the United States

In the early 1990s the United States government recognised that e-commerce legislation was becoming a national priority. This chapter will show that only a few legislative interventions have been made in the United States despite the priority it has had. In the United States, there is a true federal system[607] with 52 jurisdictions imposing laws, and operating separate

[603] Presidential Directive on Electronic Commerce, 1 July 1997.
[604] Uniform Computer Information Transaction Act, 1999.
[605] Uniform Electronic Transactions Act, 1999.
[606] Electronic Signatures in Global and National Commerce Act. 30 June 2000.
[607] In a federal system, national government holds significant centralised powers , however the smaller political subdivisions hold significant power. Examples of this can be found in

court systems. These are the 50 states, the District of Columbia and the Federal Government.

In the United States federal system, there is a division of power between the states and the central government so that, at least in theory, states may adopt their own legal regime to regulate e-commerce on a state level.[608] This was also confirmed in the case *US v Butler*[609] where the Court held that:

> 'Our government is a dual form of government, in every state there are two governments – the state government and the United States. Each State has all governmental powers save such as the people, by the Constitution, have conferred upon the United States, denied to the States, or reserved to themselves.'[610]

The effect thereof is that intrastate commerce may be regulated internally within a state and interstate commerce is regulated by federal law. The United States Constitution, being the supreme law of the land, provides that federal law supersedes any state law and that conduct or laws inconsistent with it are unconstitutional and therefore unlawful.[611] The United States law follows a doctrine of pre-emption under the Supremacy clause.[612] This means that any constitutionally-valid federal law and regulation issued by federal agency pursuant to an express delegation of regulatory power to such agency by the United States Congress trumps any state law that may be inconsistent with federal law.[613]

Brazil , Canada, Australia and Germany. Also see J S Rainey, *United States*, (2004) at 309 on this issue.

[608] Ibid.

[609] 297 U.S 1 (1936).

[610] Ibid at 97 U.S. 63.

[611] US Constitution, Article VI, Clause 2 reads: 'This constitution, and the Laws of the United States which shall be made in pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the Supreme Law of the Land; and Judges in every state shall be bound thereby, anything in the Constitution or Law of any state to the contrary notwithstanding'.

[612] J S Rainey op cit 608 at 310.

[613] *Shaw v Delta Air Lines Inc* 463 US 85, 95-96 (1983).

Just as in South African law, United States law comprises the common law which is contained in the decisions of court as well as statutes. For the purposes of this discussion, the Uniform Commercial Code (UCC) will be of importance because it contains the most common law rules in codified forms. The Restatement (second) of Contracts is also an important source, but its principles have not been adopted on a uniform basis. Therefore, any search for uniform contract law will ultimately lead to the UCC.[614]

In addition to the UCC, the United States government came up with three different codes to deal with the advent of the computer and its impact on commerce as a whole, namely: UCITA,[615] the UETA and the Electronic Signatures in Global and National Commerce Act[616] (hereafter referred to as the 'E-sign Act').

(i) Overview of the law prior to enactment of electronic contracts legislation

Before considering the transacting of business via the internet or other online methods, one must first understand the US law of contract formation in the off-line world.[617] As stated previously in this treatment, while a statute enacted by congress will supersede the common law (in other words, judge-made law) most of the statutes are based upon the general principles as laid down by the common law.[618] Due to this bizarre contradiction, the courts have chosen to apply existing common law principles to current legal disputes relating to e-contracts and therefore the study of the common law before the application of statute is most important as it is of high persuasive value to the courts.[619]

[614] H K Towle 'Legal Developments in Electronic Contracting' in *PLI Fourth Annual Internet Law Institute* (2000) at 93-94.
[615] §§ 101 – 905 (2002).
[616] 15 USCA §§7001 – (2005).
[617] J S Rainey op cit note 608 at319.
[618] W H Thurlow op cit note 112.
[619] Ibid.

(ii) The valid offer

An offer is an expression by a person or legal entity regarding their intent as the offeror to be bound to an agreement. An offer is an act or promise where one person (the offeror) confers upon another (the offeree) the power to create contractual relations. Certain additional formalities may be required to form a valid contract.[620]

The said offer must refer to an act that must be performed or refrained from doing and must be done seriously and the offeror must be able to perform and must have the contractual capacity to do so.[621] As in the South African common law, an advertisement does not constitute an offer to do business but merely an invitation to do business. More than a hundred years ago, in the New Hampshire's highest court, in language as applicable to electronic data messages as to telegraph transmittal, held that an offer and subsequent acceptance by telegraph satisfied the Statute of Frauds[622]– that places minimum requirements for written agreements in the US[623]. The honourable court in its 'ratio dicidendi' (reason for decision) stated that:

> 'It makes no difference whether the operator writes the offer or the acceptance … with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case, the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common red ink is used, while in the other case a more

[620] See Kent D. Stuckey *Internet and Online Law* (2004) (14) at 1.10-2 wherein he also refer to the *Second Restatement* of Contracts § 22 (1974).
[621] J S Rainey op cit note 608 at 320.
[622] Isaac Bowman , *The History of Electronic Signatures* at http://www.isaacbowman.com/the-history-of-electronic-signature-laws (accessed on the 16 May 2014) .
[623] Marianne Menna, 'From Jamestown to the Silicon Valley, Pioneering A Lawless Frontier: The Electronic Signatures in Global and National Commerce Act' *in Virginia Journal of Law and Technology Association* (2001)(6) at 12. *at* http://www.vjolt.net/vol6/issue2/v6i2-a12-Menna.html (accessed on the 14 May 2014).

> subtle fluid, known as electricity, performs the same office.'[624]

This reasoning should apply readily to electronic data messages, which are transmitted over long telephone lines [625] and satellite links where the user enters a data message by pressing his fingers on the keys of the keyboard. Zanger, in explaining the validity of an electronic offer, argues that an offer may be made in writing, orally or by conduct.[626] He further argues that there is no reason as to why an electronic offer should not be recognised as a valid offer based on the premise of what has been said in the preceding sentence.[627]

In *LLan Systems Inc v Netscout Service Level Corp*[628] it was held that UCC 2- 204 authorises the uses of electronic means for offer and acceptance by confirming the validity of a click-wrap agreement.

(iii) The acceptance

Acceptance is 'an agreement, either by an express act or by implication from conduct, to the terms of an offer so that a binding agreement is formed'.[629] Once a party receives an offer, it and only it, may accept or reject it. If an offer specifically specifies the mode of acceptance that will be the mode of acceptance that will be applicable, save for silence.[630] Zanger explains that

[624] *Howley v Whipple*, 48 N.H.487at 488 (1869).
[625] This also relates to GPRS links as well as 3G and fibre optical connections as used in the modern telecommunications world.
[626] L M Zanger 'Electronic contracts – some of the basics' (2000) p.2 from www.mbc.com (accessed on the 6th October 2006).
[627] Ibid.
[628] *LLan Systems Inc. v. Netscout Service Level Corp.*, 183 F. Supp. 2d 328 (D. Mass. 2002)
[629] *Hines v Davidowitz* , 312U.S. 52, 67 (1941) and *Michigan Canners & Freezers Assoc Inc v Agricultural Marketing & Bargaining bd* , 467 U.S. 461, 469 (1984).
[630] J S Rainey op cit note 608 at321.

an acceptance may be accepted in 'any manner and by any medium reasonable in the circumstances'[631].

In *LLan Systems Inc v Netscout Service Level Corp* [632] the Court held that such acceptance could be done by electronic means. Such a reasonable method may include that acceptance be performed by phone, fax or even e-mail.[633]

(iv) Writing and signature requirements

Notwithstanding the above approval of the e-mail being an acceptable mode of offer and acceptance, the concern that generated most legal is whether electronically written and signed documents meet the writing and signature requirement as stipulated by the Statute of Frauds[634] and thousands of Federal and State statutes and regulations.[635]

Statute and regulations that require transactions to be 'in writing' and to be 'signed' were generally perceived to constitute barriers to e-commerce – barriers that had to be removed in order for e-commerce to flourish.[636] It must be noted that the writing requirement serves many functions. The most significant being: (a) evidence of the transaction; (b) confirmation of the parties' intent to be contractually bound; (c) ability to reproduce the document for record purposes; and (d) allowing authentication of the data contained in the document by means of a party's signature.[637]

[631] L M Zanger op cit note 627 at 2.
[632] Ibid at 620.
[633] Ibid.
[634] Section 2 – 201 (1) provides that, '[a contract] for the sale and of goods for a price of $ 500 or more must be memorialized in signed and written form'.
[635] T J Smendinghoff & R Hill 'Electronic Signature Legislation' (1999) p.6 available at http://library.findlaw.com/1999/Jan/1/241481.tml (accessed on the 6 October 2008).
[636] Ibid.
[637] As cited by T J Smendinghoff & R Hill 'ElectronicSignature Legislation (1999) p.23, ft 37available at http://library.findlaw.com/1999/Jan/1/241481.tml (accessed on the 6 October 2008) and referring to 'Commission on Electronic Commerce and Crime',

Once again the dictum of *Howley v Whipple*[638] finds its application to this legal scenario. Douglas Morrison even went to the extent of saying in his commentary that, 'the Whipple opinion was a bit eccentric in its metaphors, to be sure, but was not maverick in its results'.[639] Courts in the US have also found telexes, [640]Western Union Mailgrams[641] and even tape recordings[642] to be writing under the Statute of Frauds. [643]

The UCC defines a 'signature' as 'any symbol executed or adopted by a party with present intention to authenticate a writing'.[644] 'Writing' is defined in the UCC as including 'printing, typewriting, or any other intentional reduction to tangible form'.[645] Smendinghoff and Hill thus submit that the key requirement is not ink on paper, but rather the presence of a symbol coupled with the party's intention to be bound.

Courts in the US have also accepted that the use of a symbol on various media may be recognised as valid signatures. For instance, names on a telegram,[646] names on telexes,[647] typewritten names,[648] faxed signatures[649]

Final report of the Commission on electronic commerce and crime. (May 26,1998) also see J L Koger 'You Sign, E-sign, we all Fall Down: Why the United States should not Crown the MarketPlace as PrimaryLegislator of Electronic Signatures' (2001) *Transnational Law & Contemporary Problems* 11 p. 491.

[638] *Howley v Whipple* op cit note 625.

[639] D Morrison (1992) 'The statute of Frauds Online: Can a computer Sign a Contract for the ale of Good ?' *Geo Mason U.L Rev (*14) p. 637.

[640] *Joseph Denzunzio Fruit v Crane* , 79 F Supp.177 (S.D. Cal 1948) affd 88 F.2d 569 (9th Cir), cert, denied 342 U.S. 820 (1951)

[641] *MacMillian v Weimer Drilling & ng. Co.*, 512 So. 2d 14 (Ala.1986)

[642] *Ellis Canning Co v Bernstein* , 348 F. supp 1212 (D.Colo.1972) at 1228

[643] J C Anderson and L. Closen 'Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority' (1999) *John Marshall Computer & Information Law Journal* , Vol 17 at 833 available at http://repository.jmls.edu/cgi/viewcontent.cgi?article=1263&context=jitpl (accessed on 14 May 2014).

[644] UCC § 1-201 (39) (1998).

[645] UCC § 1-201 (47) (1998).

[646] *Selma Savings Bank v Webster County Bank 206 S.W. 870 (Ky. 1918) at 870-876.*

[647] *Franklin County Coop v MFC Services , 441 So.2d 1376 (Miss. 1983)* at 1378.

[648] *Save–On Carpet of Arizona, Inc* 545 F.2d 1239 (9th Cir, 1976 *)* in which it was held that a typewritten signature on a UCC financing statement satisfied the signature requirement of the Statute of Fraud.

[649] See the case of *Kohlmeyr & Co v Bowen* 192 S.2d 400 (Ga. Ct App.1972).

and also names on a letterhead[650] and e-mails [651] were held to be the functional equivalence of a writing and signature. As a result many symbols may constitute a signature in terms of United States Law. Benjamin Wright goes further to state, 'even [a] name typed at the end of an e-mail should qualify as a signature, so long as it was created with the proper intent'.[652] Yet concerns have lingered not only because some courts have not agreed with the approach as suggested by Wright but also because of lack of statutory authorization. This gave rise to a legal movement which argued in favour of legislation that clearly and unambiguously states that electronic signatures and writing satisfy the paper-based equivalent.[653]

The court had to interpret the meaning of an electronic signature in the matter of *Corporation v Hasbro, Inc* [654] where the Court had to decide as to whether correspondence that was exchanged between parties without a express electronic signature, with simply names at the bottom of the e-mail, could fulfil the signature requirement of the Statue of Frauds. The court noted that the intention of the Statute of Frauds was to create certainty of the contract and no additional formality pertaining to hand written signatures had been included or affected. The court, in answering the question in the affirmative, stated that neither the common law or nor the UCC required a hand-written signature. [655]

---

[650] *Beatty v First Exploration Fund 1987 and another,* 25 BCLR 2d.377 (1988).
[651] In *Shattuck v. Klotzback* 2001 WL 1839720 (Mass. Super., Dec. 11, 2001) the plaintiff sued to enforce a real estate sales contract based on e-mail messages that the parties exchanged. The plaintiff argued that the parties had formed a contract by the e-mail exchange and the court agreed. And also see George B Delta (2009) Law of the Internet at 14.04B.
[652] B Wright *The Law of Electronic Commerce*, (1994) p. 102, and also see the case *of i.Lan System Inc v Netscout service Level Corp*183 F Supp 2d 328 (D mass 2002) where the court concluded that Section 2-204 of the UCC could be interpreted in a manner recognising an electronic click wrap agreement.
[653] T J Smendinghoff & R Hill op cit 628 p.7.
[654] No 02-2486, 314 F.3d.289.
[655] No 02-2486, 314 F.3d.289 also compare with *Jonathan P Shattuck v David K Kolzenbach et al Barbara Kolzenbach.* 01-1109A .

(v) Time and place that the contract enters into effect

Time and place of acceptance, as in South African law, is important to determine where and when a contract was concluded for the purpose of establishing the parties obligations as well as the applicable jurisdiction should a dispute arise at a later stage. An offer can generally be revoked, if it has not yet been accepted.[656] Similar to South African law, the United States law follows the theories on contract formation such as the 'information theory' and, most interestingly, the 'mailbox rule' which recognises that contractual obligations commence when the letter of acceptance enters the mailbox of the offeror [657]

United States jurisprudence recognises the application of the mailbox rule to telegraph, [658] telephone[659] and telex. [660] Without going into details of the United States common law position, it is clear that the United States also had legal uncertainty before the enactment of its legislation and no specific cases could point to the correct legal position [661] and whether it would be correct to apply the mailbox rule.

[656] L M Zanger op cit note 627.
[657] Ibid.
[658] *Weld & Co Victory Mfg co* 205 F 770 at 775 (EDNC 1913)
[659] *Bank of Yolo v Sperry Flour Co* 74 P 855 (CAL 1903)
[660] V Watnick 'The Electronic Formation of Contract and the Common Law – Mailbox Rule' (2002) *Baylor Law Review(*56) p. 176.
[661] D Kidd, Jr and W Daughtery, Jr, (2000) op cit note 51 at 267 as well as the case *International Casings Group Inc v Premium Standard Firm Inc* 358 F Supp 2d 863 , 56 U.C.C Rp. Rv. 2d 736 (W.M. Mo. 2005).

(c) *Electronic contracts legislation in the United States*

(i) Interpretation and sphere of application of electronic contracts legislation

There are three (3) sources of United States legislation on e-commerce; the UCITA, UETA and E-Sign Acts which all govern federal law.

(i) The UCITA

The UCITA was an attempt to introduce a Uniform Act for US States to follow. As a model law, it only specifies a set of guidelines, and each of the states should decide if to pass it or not, separately. The UCITA has been drafted by National Conference of Commissioners on Uniform State Laws (NCCUSL).[662]

UCITA has been designed to clarify issues which were not addressed by the existing UCC.[663] The UCITA deals with contracts or transaction in 'computer information'.[664] A contract involving computer information (for example a software licence) may be concluded electronically or may be concluded in person or by other means.[665] Although the UCITA deals with information technology, it does not solely deal with electronic contracting.[666] It was intended as an amendment to the UCC but eventually

[662] James S. Huggins 'UCITA: Uniform Computer Information Transactions Act' (2002) Available at .*http://www.jamesshuggins.com/h/tek1/ucita.html* (accessed on 14 May 2014) .
[663] Ibid.
[664] § 103 of UCITA
[665] S M Kierkegaard 'E-contract formation: US and EU perspectives' (2004) available from *http://www.ictjournal.washington.edu/vol3/a012kierkegard.html* (accessed on 18 August 2008).
[666] This also includes software, multimedia products and access to databases, including online content.

introduced as a document to be considered independent of the Code.[667] To date, the 280 page UCITA has proved to be tough to sell, having been adopted only in Maryland and Virginia.[668] Some of its provisions have been replicated in the UETA and E-sign Act therefore, its exclusion from this discussion of United States law would be a '*faux pas'* (translation 'mistake').[669]

(ii) The UETA

The UETA is one of the several United States Uniform Acts proposed by the NCCUSL. Since then 47 States, such as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have adopted it into their own laws.[670] Its overarching purpose is to bring into line the differing state laws over such areas as retention of paper records (cheques in particular), and the validity of electronic signatures, thereby supporting the validity of electronic contracts as a viable medium of agreement.

The UETA is a statute with broader reach than the UCITA, focusing on all types of electronic transactions.[671] The UETA is also a product of the NCCUSL. Unlike the UCITA, it was never intended to be part of the UCC. The purpose of the Act is stated in its preamble:

> 'The purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute - the substantive rules of contracts remain unaffected by UETA.

[667] J M Norwood (2006) 'Summary of statutory and case law associated with contracting in the electronic universe' *De Paul Business & Commercial Law Journal* (4), pp. 415-416
[668] S Rainey supra op cit note 608 at 335.
[669] Ibid.
[670]) 'Uniform Electronic Transactions Act'op cit note 598.
[671] See S M Kierkegaard op cit note 658 and Virginia (passed 2000) access *http://leg1.state.va.us/cgi-bin/legp504.exe?001+ful+SB372ER*

> Nor is it a digital signature statute, To the extent that a State has a Digital Signature Law, the UETA is designed to support and compliment statute.'

The UETA compared to the UCITA is a modest project which is less than 60 pages. The UETA has also proven to be more popular among states and has been adopted in 40 states (by 2006) including the District of Columbia.[672]Section 3 gives the scope of the Act which states:

> 'The Scope of this Act is inherently limited by the fact that it only applies to transactions related to business, commercial (including consumer) and governmental matters. Consequently, transactions with no relation to business, commercial or governmental transactions would not be subject to this Act. Unilaterally generated electronic records' and signatures which are not part of a transaction also are not covered by this Act.

Section 3(a) of the Act indicates that it applies to 'electronic records and electronic signatures relating to a transaction'. Section 3(b) also clearly stipulates that certain transaction are excluded – the most noteworthy being wills, codicils, the UCC (save for Section 1-107 and Section 1-206, Article 2 and Article 2A) and any other laws, if identified by a state.

Section 4 of the UETA goes on to state that the Act 'applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored. Furthermore, Section 5(a) of the UETA states that transactions are not required to be in electronic form and 5(b) states that:

[672] J M Norwood supra op cit note 660 at 429-430.

> 'This [Act] applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.'

The above provision seems to be consistent with the 'party autonomy' principle as stated in the UNCITRAL Model Laws as discussed earlier in this work. Section 4 of the UETA makes it clear that the Act is not applied retrospectively and that in terms of Section 5(a) and 5(b), party autonomy is still effective and that it is in the parties' discretion to decide whether electronic communications can be used and be of legal effect.[673] In order to establish if the Act must apply that the court will look at all surrounding circumstances, such as the context, and the conduct of the parties, to establish whether the Act applies or not. [674]

Other excluded acts include court orders, briefs, pleadings and other documents required to be executed in connection with judicial proceedings, notices regarding the termination or cancellation of utility services, notices regarding default, acceleration, repossession, foreclosure, or eviction, notices relating to personal and health insurance.[675]

The UETA was passed to make it clear on a national level, that a record does not fail to become an enforceable agreement solely because it was concluded, or part thereof concluded by electronic means. [676]

[673] R A Lord (2008) 'Electronic Signatures and transactions under the UETA' in *Williston on Contracts*, p.3 (Retrieved from Touro University using Westlaw on the 27 June 2008).
[674] Ibid.
[675] Ibid at 2.
[676] J S Rainey op cit note 608 at 332.

(iii) The E-Sign Act

The E-Sign Act,[677] generally known as E-sign, was passed less than a year after the endorsement of the UETA and took effect on 1 October 2000.[678] E-Sign is a United States federal law passed by the US Congress to facilitate the use of electronic records and electronic signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.

Although every state has at least one law pertaining to electronic signatures, it is the federal law that lays out the guidelines for interstate commerce. The general intent of the E-Sign Act is spelt out in the very first Section 101(a) states that a contract or signature 'may not be denied legal effect, validity, or enforceability solely because it is in electronic form'. This simple statement provides that electronic signatures and records are just as good as their paper equivalents, and therefore subject to the same legal scrutiny of authenticity that applies to paper documents.

E-sign has no effect on many substantive rights of contracting parties[679]. For example, it does not purport to alter any requirement under a statute, regulation or law, state or federal, except for any requirement that to be enforceable the contract must be in writing, manually or mechanically signed or in the non-electronic form.[680]

Similarly, E-sign re-echoes the principle of party autonomy and the use of data messages or electronic signatures is not compulsory on anyone. It has now created legal certainty for online users regarding the legal

[677] 15 USC §§ 1001 (2004) (signed into Law by President Clinton on June 30, 2000 and effective October 2000.)
[678] W H Thurlow op cit note 112.
[679] J S Rainey op cite note 608 at 333.
[680] Ibid.

enforceability of agreements concluded online.[681] It is also made clear that the Act has no retrospective effect.[682]

(ii) Legal recognition of electronic writing and signatures

(i) The UCITA

Legal recognition of electronic writing and signatures it is said was an area of uncertainty until Congress enacted the various e-commerce laws to deal with the deficiency in the law.[683] Section 107 (a) of the UCITA states that, 'a record or authentication may not be denied legal effect or enforceability solely because it is in electronic form.

In the case of *Richard S Berger v Piranha Inc Civil Action* [684] the Court held that Section 107(a) of the UCITA was to be applied to an electronic signature in giving validity to it and also held that Section 109(a) of the UCITA provides that 'an electronic signatures is attributable to a person if it was the act of a person. The Court also cited Section 109(b) which also states that attribution under subsection (a) was to be determined from the context and surrounding circumstances at the time of creation, execution or adoption including the agreement of the parties, if any, and otherwise provided by law.

Norwood states that it is clear from the wording of the UCITA that 'signatures' include things such as one's voice on an answering machine, one's name on the bottom of an e-mail, a firm's name on a facsimile document, a mouse click on a web page or digital signature.[685]

[681] 15 USC § 7001 - §101 1 (b) (1) and (2)
[682] 15 USC § 7001 - §101 4
[683] D Kidd, Jr and W Daughtery, Jr, Op cite note 51 p.237.
[684] No 3:-01-CV 2223-D
[685] J M Norwood op cit note 668 at 430.

In Section 102, the term 'authenticate' is defined as:

> '(a) to sign or (b) with the intent to sign a record, otherwise to execute or adopt an electronic symbol, sound message, or process referring to, attached to, included in or logically associated or linked with that record'.

It is clear that the term 'authenticate' in this context means sign as per Section 1-201 of the UCC.[686]

The term authentication is an alternative to the traditional word signature and fulfills the purpose of a signature. An authentication may not necessarily comply with all the requirements of a traditional signature. It is interesting to note that the word 'signature' reappears in the UETA.[687] The UCITA has imported the rule that a document must be reduced to physical copy or printout. The 'writing' requirement is fulfilled by 'a record which includes any information that is stored in an electronic or other medium and is retrievable in perceivable form'.[688] Kidd and Daughtery argue that the UCITA's Section 201 presents the new and improved Statute of Frauds using the concept of writing.[689]

(ii) The UETA

Looking at the UETA, it is immediately evident that they have the same limited objective, namely to facilitate electronic transactions by removing barriers to electronic commerce.[690]

---

[686] J M Norwood op cit note 668 at 417–418.
[687] See discussion by H K Towle 'Legal developments in electronic contracting' (2000) in *PLI Fourth Annual Internet Law Institute*, p.104.
[688] D Kidd, Jr and W Daughtery, Jr, op cit note 51 at249.
[689] Ibid.
[690] See as cited by J E Murray Jr and H M Flechtner *Sales, Leases and Electronic Commerce*, (2001) p.64, ft "The preamble to E-Sign describes the legislation as an act to facilitate the use of foreign and interstate commerce. According to UETA §6, the statute

Section 7 of the UETA expresses the underlying theme of the Act, namely to validate electronic transactions and electronic signatures. Its provides that, 'a record or signature is not to be denied legal effect or enforceability because of its electronic form'. Section 7 also provides that a contract shall not be denied validity solely on the grounds that it was concluded in electronic form'.[691] Moreover, when a law requires a writing or signature, an electronic record or electronic signature is deemed to suffice.[692]

It is important to note that Section 8 of the UETA is a saving provision designed to ensure that other laws affecting the nature of writings, their format or the manner in which they are to be sent or received are not overridden except to the extent that those laws permit. [693] Thus as long as the parties have agreed to the use of electronic records for the purpose of contract conclusion and the message can be retrieved at a later stage, it meets the requirement of writing.

One must not neglect the mandatory tone of section 8 which states that the sender of the message may not inhibit the recipient from storing and or printing the message as the said actions will make the agreement non-enforceable.[694] Party autonomy is once again retained and parties may decide on the method and type of electronic signature that they will deem acceptable.[695]

Additionally, the so-called 'click through' transactions, concluded over the internet by which a patron agrees to a transaction without specifically signing its name, by mere clicking 'OK' or the like, will be

---

must be construed and applied to facilitate electronic transactions consistent with other law.'

[691] R A Lord op cit note 674 at 3.
[692] UETA § 7 (b) and (d).
[693] R A Lord op cit note 674 at 3.
[694] Ibid at 4.
[695] R A Lord op cit note 674 at 4.

attributable to that person who clicked it subject to sufficient proof that the said action was authorized. Security procedures or measures to identify a party were used in the transaction.[696]

(iii) The E-Sign Act

The E-Sign Act provides a general rule of validity for electronic records and signatures for transactions in or affecting interstate or foreign commerce.[697]

The E-Sign Act allows the use of electronic records to satisfy any statute, regulation, or rule of law requiring that such information be provided in writing, if the consumer has affirmatively consented to such use and has not withdrawn such consent.[698]

The E-Sign Act makes it clear that online agreements are considered to be 'in writing' whenever a law, such as the Statute of Frauds requires that the contracts between parties be in writing to be enforceable.[699] The E-Sign Act contains a mirror definition of electronic signature as contained in the UETA and states that an electronic signature is, 'an electronic sound, symbol, or process attached to or logically associated with a record and executed or adapted by a person with the intent to sign the record'.[700]

[696] Ibid at 5.
[697] FDIC Compliance Manual — January 2014, x3.1(Accessed at http://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf on the 26 May 2014).
[698] Ibid.
[699] E-sign 15 USCA § 7001(a) (1) 2005
[700] E-sign 15 USCA § 7006 (5) 2005[700] *Ibid* at 5.
FDIC Compliance Manual — January 2014, x3.1 (Accessed at http://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf on the 26th May 2014) also see E-sign 15 USCA § 7001(a) (1) 2005.

Murray and Flechtner note that E-Sign Act is silent on the issue of attribution but are of the view that this is sufficiently addressed in the UETA and that the omission is not material to United States law.[701]

(iii) Time and place the contract enters into effect

(i) The UCITA

Section 203 of the UCITA establishes the basic rule of when an acceptance results in contract formation between the parties. The famous mailbox rule is rejected by this provision in favour of the 'time of receipt' rule. Norwood[702] is of the view that the most interesting aspect of this section is in the statement that:

> 'If an offer in an electronic message evokes an electronic message accepting the offer, a contract is formed:
> a) when an electronic acceptance is received[703]; or
> b) if the response consists of beginning performance, full performance, or giving access to information when the performance is received or the access is enabled and necessary access materials are received'[704]

[701] J E Murray Jr and H M Flechtner , op cit note 683 at 65.
[702] J M Norwood Op cit note 668 at 422-423.
[703] According to section 102(52). 'receipt' means :
'(A) with respect to a copy, taking delivery; or (B)with respect to a notice:
(1) coming to a person's attention; or (2) being delivered to and available at a location or system designated by agreement for the purpose, or in the absence of an agreed location or system … :
(II) In the case of an electronic notice, coming in to existence in an information processing system or at an address in that system in a form capable of being processed by or perceived from a system of that type by a recipient, if the recipient uses, or otherwise has designated or holds out, that place or system for receipt of notices of the kind to be given and the sender does not know that the notice cannot be accessed from that place.'
[704] § 201 of UCITA.

Section 203(4) provides that a contracts is formed when an electronic acceptance is received by the offeror. Norwood points out that this is akin to the traditional common law reception rule also known as mail box rule in terms of which arrival at an appropriate post office box is deemed to be receipt even if the addressee is not aware of the message.[705]

Zanger notes that in terms of Section 214 of the UCITA an electronic message will be deemed effective when received even if no individual is aware of its receipt, which is the same as the rule with paper-based mail that does not require the person to be aware of the postal or mail to be opened.[706] Regrettably, the UCITA does not lead to clarity on the issues of when receipt takes place; it only gives certainty regarding the place of receipt .

As previously stated, it has only been adopted by a few states. This is not similar to the Model Law which provides a rule for e-receipt but is silent on time of contract formation.

(ii) The UETA

Section 15 of the UETA outlines specific rules as to when an electronic message is considered to be 'sent' and 'received'. It has significance to contract formation, enforcement and breach of contract for it specifies when it is deemed to have been sent or received.[707] However, Norwood is of the view that this section does not take a position on whether an acceptance is considered to be valid when mailed (the mail box rule).[708]

Section 15(a) deals first with the question of when is a message deemed to have been sent and lays down a three-pronged test. First, the

[705] J M Norwood op cit note 668 at 422-423.
[706] L M Zanger op cit 627 note at 3. Also see Watnick, V J op cit note 653.
[707] R A Lord op cit note 674 at 14.
[708] J M Norwood 'Summary of statutory and case law associated with contracting in the electronic universe' 2006(4) *De Paul Business & Commercial Law Journal* at 435.

message must have been addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent, from which the recipient is able to retrieve the information.

Secondly, the sent information must be capable of being accessed on the receiving information system. Thirdly and lastly, the said sent message must have entered an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender, or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

It is tempting to suggest that Section 15(a) codifies what might be called the mailbox rule. However, the drafters clearly did not intend that to be the case if one reads the early drafts of the UETA which specifically abolish the mailbox rule.[709] Section 15 (a) essentially only deals with the aspect of when a message has been sent and it does not in any way give certainty as to whether a message has constituted a valid acceptance of an offer made.[710]

Section 15 (b) addresses the second question that specifically deals with when a data message is deemed to have been received. The test is a dual one which requires first, that the data message must enter an information system from which the recipient is able to retrieve the record or an information system customarily used for the receipt of similar electronic records; and secondly the recipient is able to retrieve the record that has been sent.[711] Norwood notes that the provision makes it clear that receipt is not dependent on a person having noticed that the record is in the person's system.

[709] R A Lord Op cit note 674 at 14.
[710] Ibid.
[711] R A Lord op cit note 674 at 17.

Reception occurs as soon as it enters a used or designated information system, whether or not it has been retrieved.[712]

To sum up the legal position Lord states that:

> 'Section 15 (b) does not establish any substantive rules concerning the effect that receipt of particular information or information in general . . . It solely concerns itself with determining whether information has been received, leaving to the other law the question of the effect of that receipt … . Nevertheless . . . two important substantive effects [can be noted] . . . It will trigger and mesh with other rules of law that are dependent for their applicability on "receipt" . . . whether the recipient can manipulate the timing of receipt by his failure to open his mail.'[713]

Lord concludes that the only reasonable inference that can be drawn is that the agreement is concluded at the time and place where the recipient receives the information such as in true paper-based transactions.[714] The said approach is akin to the reception theory. Although some writers are of the view that the United States may have adopted the reception theory,[715] other more cautious writers are of the view that the mailbox theory stands,[716] especially in the light of the fact that the UCITA has limited application in the United States legal milieu.[717]

An electronic record is deemed to be sent from where the sender has its place of business. In the case of multiple places of business, the closest

[712] Norwood op cit note at 668.
[713] R A Lord op cit note 674.
[714] Ibid.
[715] C Pacini, C Andrews & W Hilson ' Contracting in cyberspace (the CPA and the computer) in the New York State' (2002) , *Society of Public Accountant CPA Journal* 65 (1/3), at 72 –73.
[716] V Watnick op cit note at 661 at 196 at 203 and see the cases *Weld & Co Victory Mfg co* 205 F 770 at 775 (EDNC 1913 *), Bank of Yolo v Sperry Flour Co 74 P 855 (*Cal 1903).
[717] T Pistorius "From Snail mail to E-mail- a South African Perspective on the Web of Conflicting Rules on the Time of e-contracting. (2006)(39) *CILSA*,198.

place that has a relation to the transaction will be deemed as such a place of business.[718]Accordingly, where there is an issue regarding the place of sending or receipt, the location of the information system should not be regarded as the location, but the location of the place of business is of importance.[719] In the instance when the party is aware that a message that was purportedly sent or received was actually not sent or received, the legal effect of the sending and/or the receipt is regulated by other applicable law.[720]

(iv) Automated transactions

Both the UCITA and the UETA deal with the issue of automated transactions that have wholly or partially been concluded by electronic agents. Section 206 of the UCITA recognises this means of contracting as an enforceable contract but gives an interpretation as an option[721] where there is proof that the said agreement was a result of 'fraud , electronic mistake or the like'[722] to decide otherwise. Section 14(1) of the UETA deals with the increasing methods of automated contracting.[723] It provides that :

> 'a contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms of the agreement.'

Norwood adds that machines can represent parties in a legally binding agreement and that the defence of lack of human interaction or intent cannot

[718] UETA § 15 (c) & (d).
[719] T Pistorius 'Contract Formation: A Comparative Study of Legislative initiatives on Select Aspects of Electronic Commerce' (2002) *CILSA* (35) at 150.
[720] UETA § 15(g).
[721] J M Norwood op cit note 668 at 423.
[722] § 206 (a) of UCITA.
[723] J M J M Norwood op cit note 668 at 435.

be used as a valid defence.[724] A similar provision is contained in Section 101(h) of the E-sign Act.[725]

(v) Interesting cases dealing with click-wrap, web wrap agreements

The majority of cases involving electronic contracting mostly relate to assent to contractual terms and the jurisdiction of courts. The provisions of the UCITA, UETA or E-Sign Act have not been subjected to judicial scrutiny. It is interesting to illustrate (for comparative purposes) the court's rulings towards click-wrap, browse-wrap and web-wrap agreements in the United States.

- *Click-wrap and web wrap agreements*

The first decision is of *Llan Systems v Netscout Service Level Corporation*[726] in which the court had to decide whether a party is bound to contractual terms that appear on screen of a computer whilst installing a software programme by clicking the 'I agree' option. In answering the legal question in the affirmative, the court reasoned that a click-wrap agreement could be analysed as forming a contract under UCC Section 2-204 (formation in general) in that the buyer assents to the click-wrap agreement when clinking the box 'I agree'.[727]

Norwood also explains that the court referred to the famous decision of *Pro Cd v Zeidenberg & Siken Mtn. Web Services*[728] in which the Court was of the view that the final failure to reject the terms of a shrink-wrap agreement

[724] Ibid.
[725] J E Murray, Jr and H M Flechtner op cit note 683 at 66.
[726] *Llan* op cit note 629 183 F. Supp 2d 328 (D. Mass 2002).
[727] Ibid at 16 and also see discussion in J M Norwood op cit note 668 at 443.
[728] 86 F.3d 1447 (7th Cir 1996).

was sufficient to show assent to contract terms and that the doctrine of 'money now, terms later' has application in the United States law.[729]

In the second case of *DeJohn v The TV Corporation International* [730] the vexed legal issue of jurisdiction came under the spotlight with specific reference to a forum selection clause. The court held for a party to evade being bound to a forum selection clause it must prove the following:

> 'It was the result of fraud or overreaching; the party will be deprived of his day in Court due to grave inconvenienced and unfair selection of the selected forum; the clause is against public policy of the forum state and the party may be deprived of legal remedy due to the unfairness of the chosen legal regime.'[731]

None of the factors could be proved and the clause was upheld.[732] In the case of *Sprecht v Netscape Communications Corporation*[733] attention was drawn to the effect of what the court referred to as an internet agreement which was contained far down at the bottom of the web-page under the download option for free software. The court refused to enforce an arbitration clause and stated, '[the offeree] is not bound by inconspicuous contractual provisions of which he was unaware'.[734]

The court further held that, 'downloading is hardly an unambiguous indication of assent'.[735] The primary purpose of the download is to get the product. If the party intended to be bound he surely would have clicked 'I assent'.

---

[729] Ibid and also see the case discussion of Joseph C. Wang (1998) ProCD, Inc. v. Zeidenberg and Article 2B: Finally, The Validation of Shrink-Wrap Licenses, 16 J *in Marshall J. Computer& Info. L*.at 460.
[730] 245 F.Supp. 2d 913 (N.D. ILL. 2003).
[731] 245 F.Supp. 2d 913 (N.D. ILL.2003) at 917.
[732] Ibid.
[733] 150 F supp 2d 585 (SDNY 2001).
[734] Ibid at 589.
[735] Ibid at 595.

(vi) E-jurisdiction in e-related disputes

Another vexed legal issue is e-jurisdiction. Dennis Rice explains that jurisdiction in the United States is influenced by the 3rd Restatement of Foreign Relations Law of the United States.[736] It is divided into 'jurisdiction to prescribe', 'jurisdiction to adjudicate' and 'jurisdiction to enforce'.[737] For the purposes of this discussion, it is important to look at jurisdiction to adjudicate.[738]

In this realm of internet-based e-jurisdiction, a realm in which the courts have created new jurisdictional principles for analysing electronic contacts mediated through cyberspace that depart from the traditional jurisdictional principles articulated in cases involving contacts made in real space.[739]

New considerations such as web site internet activity and target audience are essential concepts that United States courts use to determine whether to treat virtual contacts as 'minimum contacts'. The United States courts have come up with various tests to establish jurisdiction or to give it grounds to refuse to hear a matter which will be discussed below in detail.

The U.S. Supreme Court has developed an alternative test that assists in establishing jurisdiction in case of doubt called the 'effects test' or 'minimum contact test' based on the Supreme Court's decision in *Calder v*

[736] 3rd Restatement of Foreign Relations , Law of the United States, § 401.
[737] D T Rice "Recent trends in determining jurisdiction in Cyberspace", presented at "IT Meets Telecon", (2003) hosted by the Computer Law Association at the Convention Centre, Munich, Germany 13-14 November 2003 at 3.
[738] Jurisdiction to adjudicate means that the tribunal of a given country may resolve a dispute to a person or thing where the country has jurisdiction to prescribe the law that is sought to be sought and enforced which is subject to reasonableness.
[739] A B Spenser "Jurisdiction and the Internet: Returning to Traditional Principles to Analyze Network- Mediated Contracts" (2005) in *University of Illinois Law Review*, Vol. 2006 No1 at 72.

Jones.[740] In terms of this alternatives test state courts may exercise jurisdiction when a defendant intentionally harms forum residents. In the said matter, a California resident brought a suit in the California Superior Court against a Florida resident who allegedly wrote libelous matters about her in a prominent national publication. In holding that jurisdiction was proper, the court found 'the brunt of the harm, in terms of the respondent's emotional distress and the injury to her professional reputation was suffered in California'.[741]

In the case of *World-wide Volkswagen Corp v Woodson*[742] the concept of 'minimum contacts', in turn, can be seen to perform two related but distinguishable functions. It protects the defendant against the burdens of litigating in a distant or inconvenient 'forum'. It also acts to ensure that states through their courts, do not reach out beyond the limits imposed on them by their status as coequal sovereigns in a federal system.[743] The court in this case also added the requirement of plaintiff having to purposefully affiliate the defendant with the forum.[744]

In the case of *Burger King v Rudzewicz*,[745] the United States court further developed what it called the 'minimum contact test' to found jurisdiction on a defendant on the basis of the entire dealings, including 'prior negotiation and contemplated future consequences' establishing that 'the defendant purposefully established minimum contacts with the forum' and may foresee being hauled before a court in another party's jurisdiction.[746]

---

[740] 465 US 783 (1984).
[741] Ibid at *at* 789-790 *and also see* F F Wang "Obstacles and solutions to internet Jurisdiction – A comparative Analysis of the EU and US laws" (2008) in Business *and Law- Theory and Practic*e, Eds S Kierkegaard, ft 66 on p. 121.
[742] 444 U.S 286, 291-922 (1980).
[743] Ibid at p 292 and also see A B Spenser "Jurisdiction and the Internet : Returning to Traditional Principles to Analyze Network Mediated Contacts" (2005) in *University of Illinois Law Review*, Vol.2006 , No1 at 72.
[744] World-Wide Volkswagen Corp v Woodson 444 U.S 286, 297-998 (1980).
[745] 471 US , 105 S.Ct.2185, 85 Led. 2d 528 (1985).
[746] Ibid at p478-479 and also see discussion of F F Wang (2008) Obstacles and solutions to internet Jurisdiction – A comparative Analysis of the EU and US laws" *Business and Law - Theory and Practice*, Eds S Kierkegard, at 120.

In the case *of Zippo Mfg. co. v Zippo Dot* [747] the court expanded on the minimum contact test by stating that personal jurisdiction for e-commerce companies should be dealt with on a sliding scale[748] to analyse the contacts necessary to establish jurisdiction in what this study will now the call the 'Zippo test'.[749] In determining the constitutionality of exercising jurisdiction, the court in the Zippo case focused on 'the nature and quality of commercial activity that an entity conducts over the internet'.[750] The sliding scale approach can be divided into three categories. First, active websites: for example, where a defendant enters into contracts with residents of a foreign jurisdiction that involve the repeated transmission of computer files over the internet, their conduct will fall into the active category. This is a ground for the exercise of personal jurisdiction.[751]

Secondly, passive websites: namely, those websites which merely provide information to a person visiting the site. They may be accessed by internet browsers, but do not allow interaction between the host of the website and a visitor to the site. Passive websites do not conduct business, offer goods for sale, or enable a person visiting the website to order merchandise, services, or files.[752] The court reasoned that passive websites do not meet the standard of purposeful availment established under the traditional personal jurisdiction framework.[753] The defendant has simply posted information on a passive internet website which is accessible to users in foreign jurisdictions. This is not a ground for the exercise of personal jurisdiction.[754]

---

[747] F.Supp 1119 (W.D.pa 1997).
[748] Wang op cit note 747.
[749] D T Rice supra op cite note 729 at 1.
[750] *Zippo Mfg. cow, v Zippo Dot F.Supp* 1119 (W.D.pa 1997) at 1124.
[751] Wang op cit note 747 at 121.
[752] Zippo Mfg. cow, v Zippo Dot F.Supp 1119 (W.D.pa 1997).
[753] *Bensusan Restaurant Corp. v. King*, 937 F. Supp. 295, 297 (S.D.N.Y.1996), aff'd, 126 F.3d 25 (2d Cir. 1997) also see the article of Anindita Dutta 'Zippo Manufacturing Co. v. Zippo Dot Com, Inc.,' (1998) Vol13 *Berkeley Tech. L.J.* 289 and available at: http://scholarship.law.berkeley.edu/btlj/vol13/iss1/19 (accessed on the 16 June 2014).
[754] J R Reidenberg 'Technology and Internet jurisdiction' (2005) in *University of Pennsylvania Law Review* at 1951

Thirdly, are the interactive websites that make up the middle of the sliding scale where a user can exchange information with the host computer. In this middle scale, jurisdiction should be determined by the 'level of interactivity and commercial nature of the exchange of information that occurs on their web site'.[755]

Factors such as online contracting (found on most e-commerce sites) can show a high level of interaction leading to the exercise of jurisdiction. This is the crucial point of the sliding scale analysis. If the activities occurring on a defendant`s website lean more towards the passive side of the scale, personal jurisdiction will not be applied. If, the activity slides toward the active side of the scale, personal jurisdiction will most likely be upheld.[756]

Lastly, the courts in applying the 'Zippo' and effects tests have focused on whether there was 'something more' that was required to exercise jurisdiction and developed the 'targeting test'.[757]The targeting test states that a court will have jurisdiction if, 'the defendant specifically engaged in wrongful conduct targeted at a plaintiff with the knowledge that the defendant is a resident of a forum state'.[758] The targeting test is argued to be a better test as it deals more with the intention of the parties in determining jurisdiction and is seen as a fairer approach in establishing whether a defendant could have foreseen being hauled before a court outside his/her normal jurisdiction.

The most famous decision dealing with a court's jurisdiction regarding the conduct of owners of a website is the case of *Yahoo! Inc, a Delaware Corporation v La Ligue Contre Le Racisme et L'antisemitisme a French*

[755] *Zippo Mfg. cow, v Zippo Dot* F.Supp 1119 (W.D.pa 1997) at 1124.
[756] Ibid.
[757] Reidenberg op cit note 755.
[758] *Bancroft & Master Inc v Augusta Nat'l Inc.,* 223 F. 3d 1082, 1087 (9th Cir 2000*) and World-Wide Volkwagen Corp v Woodson,* 444 US 286, 297 (1980).

Association; L'union Des Etudiants Juifs De France, a French Association[759]. In this matter Yahoo!, an American internet service provider, brought suit in federal district court in diversity against 'La Ligue Contre Le Racisme et L'Antisemitisme' (LICRA) and 'L'Union des Etudiants Juifs de France' (UEJF) seeking a declaratory judgment that two interim orders by a French court are unrecognisable and unenforceable. The court order pertained to the court ban imposed on Yahoo!! on its French website *www.yahoo.fr* prohibiting it from selling Nazi material, Nazi memorabilia or any Nazi article within the French jurisdiction. The exact wording of the Court order read:

> 'Yahoo! take all necessary measures to dissuade and render impossible any access [from French territory] via Yahoo.com to the Nazi artifact auction service and to any other site or service that may be construed as constituting an apology for Nazism or a contesting of Nazi crimes.'[760]

The court, in its reasoning, applied the effects test (also known as the 'purposeful direction' test) as formulated in the *Calder v Jones*[761] decision and the 'minimum contacts' test as set out in *Zippo Mfg. Co v Zippo Dot.*[762]

Furthermore, the court recognised that, 'the risk of a large monetary penalty would have to inevitably weigh heavily in Yahoo!'s assessment of its options', the majority tries to neutralise the risk creating a protective shield

[759] 1181, 1192 (N.D. Cal. 2001).
[760] The French court's orders are written in French. We quote from the English translation provided in the record. Counsel for LICRA and UEJF contended at oral argument that the words "all necessary measures" (underlined and italicized above) are a mistranslation of the French text. The original French for the entire phrase (italicized above) is "prendre toutes les mesures de nature à dissuader et à rendre impossible." Counsel contended that the words "toutes les mesures de nature à" are more accurately translated as "all reasonable (or available) measures."
[761] 465 U.S. 783, 104 S.Ct. 1482, 79 L.Ed.2d 804 (1984).
[762] F.Supp 1119 (W.D.pa 1997).

by invoking the doctrine that United States courts will not enforce the penal judgments of other countries. It thus assures Yahoo! that, 'even if the French court were to impose a monetary penalty against Yahoo!, it is exceedingly unlikely that any court in California or indeed elsewhere in the United States would enforce it' because it is a penal judgment.[763]

In the most recent case in the appeal of *MacDermind Inc v Jackie Deiter* [764] the United States Court of Appeal held that a foreign defendant's remote use (at the time from Canada) of a computer within the jurisdiction of Connecticut satisfied the jurisdictional requirements of both the Connecticut Long-arm Statute and due process. In finding that the district court (the court '*a quo'*) had erred by dismissing the action on lack of jurisdiction held that the district court indeed had jurisdiction to hear the dispute and it concluded that the defendant actually did 'use' the computer services in the Connecticut state as she had accessed an information system within Connecticut as contained in the Connecticut Long–arm Statute.[765]

Secondly, the appeal court held due proceeds was followed because that the defendant had ''minimum contacts' with the State of Connecticut Court as the previous decisions of *Calder v Jones*[766] and *World-wide Volkswagen Corp v Woodson*[767] The court further referred to the case of *Burger King v Rudzewicz*[768] and held that she had 'purposefully directed her conduct' at the information system in Connecticut.[769]

In holding that the jurisdiction was reasonable the court referred to the case of *Asashi Metal Industries Company v Superior Court,* [770]based on the following five factors: namely, (a) the burden on the defendant; (b) the

[763] Ibid at par 235.
[764] 702 F.3d 725.
[765] Ibid. at 7-8.
[766] 465 US 783 (1984).
[767] 444 U.S 286, 291-922 (1980) .
[768] 471 US , 105 S.Ct.2185, 85 Led. 2d 528 (1985).
[769] Ibid.
[770] 480 US 113-114 (1987).

interest if the forum state; (c) the plaintiff's interest in obtaining relief; (d) interest of the interstate judicial system and shared interests of the two states.

(d) Conclusion

United States legislation primarily deals with the functional equivalence of electronic data to the old traditional paper-based methods. The UCITA has proven not to be as effective and has not been widely adopted by states. This is partly due to the fact that it does not only cover e-commerce issues, but other IT related problems. The UETA has in its scope excluded a number of legal acts that one may perform using data messages. This approach is contrary to the UNCITRAL Model Law.

The UETA is deemed to be a facilitating Act, that does not require any one to perform any act relating to electronic transactions.[771] Section 7 of the UETA gives effect to Articles 5 and 6 of the Model Law on E-commerce on the aspect of validity and recognition of electronic data messages.[772] Section 7 also gives a wide recognition to electronic signatures and shows a shift closer to the UNCITRAL Model Law of E-signatures.

The UCITA seems to follow the model law with regard to time and receipt as contained by Article 15. The .UETA, which is more widely accepted, is silent on the issue and legal writers also do not have general consensus on the issue. The United States common law seems to be a leader in establishing jurisdictions and it appears that many jurisdictions seek for answers from the United States law in formulating their own tests when dealing with cross-border issues of the internet.

[771] § 6 of the UETA.
[772] T Pistorius op cit note 720 at 292.

CHAPTER VII: CONCLUSION

This dissertation shows clearly that the South African ECT Act adequately caters for paperless contracts or better said, electronic contracts (e-contracts). In this conclusion, the most important provisions in the ECT Act will be compared to the UNECIC, UNCITRAL Model Laws, the AU Convention on Cyber Security and United States law with a view to making recommendations regarding the current South African legal position on e-contracts.

(a) Formation and validity of e-contracts

The South African law of contract allows contracts to be formed in any manner, i.e. orally, telephonically, by written documentation, fax or through the conduct of the parties. This is consistent with the party autonomy principle as envisaged by the UNICITRAL Model Law and as is contained therein. An offer and an acceptance can be made on a website, in e-mail messages, and in a chat-room or any other new social media platform.

Section 11(1) and Section 22(1) of the South African ECT Act reiterate the principles allowing for contracts to be negotiated and concluded in different electronic ways by providing respectively that, 'information is not without legal force merely on the grounds that it is wholly or partly in a data message'. The above provisions follow the principles as laid down by Article 5 and Article 6 of the Model Law, Section 107 of the UCITA, and section 7 of the UETA and reconfirmed in Article 8 of the UNECIC. Section 21 of the ECT Act on the other hand, guarantees and re-affirms that, 'an agreement may be formed where an electronic agent performs an action required by law for the agreement formation'.

There might be only one ambiguous issue regarding whether an electronic message or a website is an invitation to treat or it is a valid offer. It has been argued in this dissertation that this will fall under one of the instances where an advertisement may constitute an offer from the common law perspective. In this regard, businesses can avoid ambiguity by making clear in their e-mail pricelist or website catalogue that it is either an invitation to treat or to make a firm offer.

(b) Time and place of formation of contract

Section 22 and 23 of the ECT Act provide clarity as to the existing South African contract law in determining the exact time and place of dispatch and the receipt of data messages. In summary, an offer or acceptance made in the form of a data message is deemed to have been sent when it enters an information system outside the control of the originator in terms of Section 22 of the ECT Act. It is deemed to have been sent at the place of business of the originator and is deemed to have been received when the complete data message enters an information system of the addressee and it is capable of being retrieved. It is submitted that the ECT Act could be amended to follow the UCITA rule that an e-mail must be sent to the correct address. It should be noted this also addresses the uncertainty that occurs when a data message is sent to a non-designated information system.

Section 23 of the ECT Act and Section 203(4) of the UCITA, unlike the Section 8 of the UETA or E-Sign law, actually specify when a contract is concluded which is seen as a progressive step in the ECT Act. These provisions are partially in line with the Model Law's Article 15 and confirm that the contract is concluded on receipt of the message by the addressee but go a step further by also confirming as to when the contract is concluded, unlike the Model Law and Article 10 of the UNECIC. It must be noted that in Section 23 of the ECT Act is more stringent in that it requires that the complete data message must have entered the information system of the

recipient. This additional requirement is not included in the Model Law, the UNECIC, or the UCITA. It is submitted that, although stringent, it creates more legal certainty in the event where the full data message has not been received by the addressee.

(c) Automated transactions

Section 20(a)–(c) of the ECT Act relates to automated transaction which extends to web-wrap and click-wrap agreements. This section re-states the common law position to some extent and instead of using the subjective actual consensus criterion when looking at validity of agreements, a more objective criterion, namely, reliance is applied to automated contracts.

Section 20 confirms the validity of automated transactions as previously stated by Pistorius.[773] Although the Model Law on E-commerce by way of implication confirms the validity of automated agreements, the UNECIC provides that these are now an acceptable form of contract negotiation in Article 12. Section 20(d) of the ECT Act has new important consequences in that it gives the party contracting with an electronic agent the right to review the transaction, failing which the party will not be bound. Section 20 (e) also specifies the procedure to be followed in the case where a party has made a material error and wishes not to be bound to the agreement. This provision although pre-dating the UNECIC is very similar to the provision of the UNECIC on this legal issue and shows that the drafters on the ECT Act had a very progressive intention while drafting it.

773 T Pistorius) "Formation of internet contracts: Contractual and security issues" in *SA Mercantile Law Journal* (1999) (11) at 292.

(d) Writing and signature requirement

South African law allows most contracts to be concluded informally, but in the case where writing and signatures are required by the parties, our courts have adopted a very lenient and progressive approach. In this regard, Section 12 and Section 13 of the ECT Act recognise data messages as the functional equivalent of a written document and signature.

Section 12 of the ECT Act unlike the Model Law, the UNECIC, UETA, UCITA and E-sign laws add an additional dimension which requires that the data messages must be accessible and usable for subsequent use. It is interesting to note that Section 8 of the UETA specifically states that an originator may not inhibit the printing or the subsequent use of the data message, which seems to be fulfilling a similar function as the additional requirement in Section 12 of the ECT Act although the non-inhibiting provision goes beyond the functional equivalence principle. The above provision, save were deviation has been noted, seems to follow both the international and United States trends.

Section 13 of the ECT Act also recognises the use of electronic signatures. It should also be noted that in the instance where the law requires such a signature, such a requirement will only be satisfied if one uses an advanced electronic signature.[774] There is a shift from technologically neutral electronic signatures as contained in Article 7 of the Model law as well as Article 6 of the Model Law on Electronic Signatures. A more stringent standardised security level has been adopted in South Africa which is seen as a two-tiered approach. Some electronic signatures are valid without advanced levels of security and for others the law requires a signature to follow a more prescriptive approach. The UCITA and E-sign

[774] S L Gerda (2004) 'The Electronic Communications and Transactions Act' in *Telecommunications Law.* L Thornton Eds, at 270.

law seem to follow a technologically neutral regime but some states have adopted stringent regimes such as that of South Africa.

It is submitted that the two-tier approach, as envisaged in Section 13, is ideal in that it does not unnecessarily place any specific requirements or formalities in the course of normal business contracting so making the minimalist approach the ideal approach.

The face-to-face registration required for the prescriptive advanced e-signature can have many benefits, and the said signature can also be used for other functions as it is linked and verified by the Department of Home Affairs.

(e) Jurisdiction in e-contracts

In this researcher's opinion, the ECT Act should be reviewed every second year in order to cater for new technological advances as per the technology neutrality principle. Most electronic contracts usually contain clauses stipulating that the transaction in question will be governed by a particular law; the Model laws, the ECT Act and United States pieces of legislation appear to be silent on this important international law issue. It is suggested here that a jurisdiction clause can create certainty in the event of a dispute arising as to the conclusion and performance of the contract.

A jurisdiction clause, although not absolute, can deal with any uncertainty in the agreement as to which forum will have jurisdiction and what law may apply in the case of pre-litigation and litigation.

The UNECIC also has affirmed the recognition of international cross-border electronic contracts and attempts to curb all the common law legal

problems created by the principle of jurisdiction and the implication of the conflict of laws as per Article 10 of the UNECIC.

(f) Recommendations

As discussed earlier, the South African ECT Act is mainly based upon the UNCITRAL Model Laws on E-Commerce. It is disturbing that the principles of technological neutrality with regard to electronic signatures have not been followed, but perhaps this was done as a cautionary measure. The slow uptake of advanced electronic signatures is a factor inhibiting the growth of e-commerce in South Africa.

It is also suggested that the SAAA follow a technological method when accrediting both foreign and local electronic signatures in order to relax the stringent requirement of an advanced e-signature. Section 13 of the ECT Act may be seen as inhibiting electronic commerce by not fully observing the media neutrality of electronic signatures but it could be relaxed by the implementation of less stringent rules on accreditation of advanced e-signatures since the two-tier approach has shown this to be useful. Should this not be possible, the legislature will have to look at amending Section 13 to follow the international trend of technological neutrality as envisaged by the Model law on Electronic Signatures.

It is also suggested that Section 23 of the ECT Act be amended to add that an e-mail must have been sent to the correct e-mail address as contained in the United States provisions in Section 15 of the UETA. The sending to a non-designated information system should also be addressed.

It is also submitted that the ECT Act requirement that a full data message must enter the information system of the addressee could also be relaxed as an interruption in a data connection may result in an incomplete data message being received by an addressee and may prejudice the sender

despite him/her having sent the data message. Perhaps the reception theory may not be the most appropriate theory regulating when a message is deemed received it has, unlike the United States Law, created some legal certainty.

The alignment of the South African law with international and regional law instruments such as the UNECIC and the African Union convention will also ensure regional and global legal compliance. The adoption of useful legal principles from other jurisdictions such as the United States and the EU (to some extent) which have a wide body of jurisprudence of cyber law related matters may be the way forward. Lessons learned from the US case law studies show that the old rigid approach to jurisdiction must evolve with the advent of the internet and will need to be further address by our courts. Legislative amendments are deemed appropriate.

South Africa in its current ICT Review and review of the ECT Act in the Amendment Bill of 2014 needs to take cognizance of development in technology and observe international best practice in order to fully address any current legal issues that may inhibit or create uncertainty when contracting electronically.

BIBLIOGRAPHY

Books

A

Alhadeff A & Cohen M 'Functionality of value-added network service and their liability' in R Buys (ed) *Cyberlaw @ SA II: The Law of the Internet in South Africa* (2004).

B

Benzine and Garland *Accessing the Internet* (2000).

Brazell L *Electronic Signatures Law and Regulation* (2004).

Buys R (ed) *Cyberlaw @ SA: The Law of the Internet in South Africa* (2000).

C

Christie R H *The Law of Contract* 4 ed (2001).

D

Davies A 'The development of laws on electronic documents and e-commerce transactions' (2000) *Library of Parliament (Canada)* 1. PRB-00-12.

E

Eiselen S 'E-commerce' D van der Merwe (ed) *Information and Communications Technology Law* (2008).

Eiselen S 'Principles of the UNECIC' in *Sharing International Commercial Law across National Boundaries* (2008).

F

Ferreira G R *Cyberlaw: Texts and Cases, USA* (2004).

Forder J & Quirk P *Electronic Commerce and the Law* (2001).

G

Gerda S L 'The Electronic Communications and Transactions Act' in L Thornton (ed) *Telecommunications Law* (2004).

K

Kahn E *et al , Ellison Kahn Contract and Mercantile Law* 2 ed (1989).

Kobrin S J 'Economic governance in an electronically networked global economy' in R Hall & T Biersteker (eds) *The Emergence of Private Authority: Forms of Private Authority and their Implications for Global Governance* (2002) Cambridge University Press. (Also available at *http://www.management.wharton.upenn.edu/kobrin/Research/revision%201.pdf*) (accessed May 2007).

L

Lord R A ‘Electronic signatures and transactions under the UETA in Williston (eds) *Williston on Contracts* (2008).

Meiring R ‘Electronic Transactions’ in *Cyberlaw @ SA II: The Law of the Internet in South Africa,* (2004) R Buys (ed).

Murray J E Jr. & Flechtner H M *Sales, Leases and Electronic Commerce* (2001).

N

Nagel *et al Commercial Law* (2000).

O

Oxford English Dictionary (1989).

Orji U J *Cybersecurity Law and Regulation* (2012).

P

Papadopoulus S & Snail S ‘Electronic contracts in South Africa (e-contracts)’ in Papadopoulus and Snail (ed) *Cyberlaw @ SA III: The Law of the Internet in South Africa* (2012).

R

Rainey J S *United States* (2004).

S

Schneider G *Electronic Commerce* (2006).

Shim J, Qureshi A A, Siegel J G & Siegel R M *The International Handbook of Electronic Commerce* (2000).

Smith G *Smith's Guide to the Internet* (2000).

U

United Nations Commission on International Trade Law Yearbook (1985).

UNCITRAL 'Recommendation on the Legal Value of Computer Records'. Resolution 40/71 adopted by 40th General Assembly (11th December, 1985) in *United Nations Commission on International Trade Law Yearbook,* (1985).

V

Van Aswegen *et al General Principles of the Law of Contract* (1999).

Vogel H J 'E-commerce: Directives of the European Union and implementation in German law' in D Campbell & S Woodley (eds) *E-commerce: Law & Jurisdiction* (2003).

W

Wang F F 'Obstacles and solutions to internet jurisdiction: A Comparative Analysis of the EU and US Laws' in S Kierkegaard (ed) *Business and Law – Theory and Practice* (2008).

Journal articles

A

AUCLCS. 'Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa' (version - 1/01.2011), available at: *http://www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf* .

Abhilash C M 'E-commerce Law in Developing Countries: An Indian Perspective' (2002) 11(3) *Information & Communication Technology Law* 270-80.

Ahmad F 'Electronic commerce: An Indian Perspective' (2001) 9 (2) *International Journal of Law and Information Technology* 133-170

Andrade D 'Is the Pen Mightier than the Electronic Signature?' (2005) (30 October 2005) *(<http://www.derebus.org.za/nxt/gateway.dll/bsxha/uei9/7okka/eqkka/svbua>*.

Angel J 'Why use Digital Signatures for Electronic Commerce?' (1999) *The Journal of Information Law and Technology Law* 2-4.

B

Baker & McKenzie 'Singapore E- Commerce Legislation and Regulations' *Global E-Commerce Law*, available at *www.bmck.co/ecommerce/malysia.html*.

Blyth S E 'Digital Signature Lawof the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-commerce with Enhanced Security' (2005) 11 *Richmond Journal of Law & Technology* 2 1, available at *http://law.richmond.edu/jolt/v11i2/article6.pdf*.

Brand R A 'A global Convention on Choice of Court Agreement' (2004) 10 *Journal of International & Comparative Law* 345 .

C

Christianson G and Mostert W 'Digital Signatures' (May 2000) 28 *De Rebus* (2000) 34

Chong K W & Chao J 'United Nations Convention on the Use of Electronic Communications in International Contracts – a New Global Standard' (2006) 18 *Singapore Academy of Law Journal* 116.

Coetzee J 'The Electronic Communication and Transactions Act 25 of 2002: Facilitating Electronic Commerce' (2004) 3 *Stellenbosch Law Review* 501.

Coetzee J 'The Convention on the use of Electronic Communications in International Contracts: Creating an International Legal Framework for Electronic Contracting' (2006) *South African Mercantile Law Journal* (18) 245.

Colliers D 'E-mail and SMS contracts' (2008) 16 *Juta Business Law* 1 (21) 20

Connolly C & Ravindra P 'First UN Convention on E-commerce Finalised' (2006) 22 *Computer and Security Report* 31.

Cornelius S ‘Condonation of Electronic Documents in terms of Section 2 (3) of the Wills Act’ (2003) in *Tydskrif vir Suid Afrikaanse Reg* 210.

D

Dean O ‘Stalking the Sleeping Lion’ (July 2006) *De Rebus* 21.

E

Edelstein S ‘Litigation in cyberspace: Contracts on the internet (commercial litigation) ‘. (1996) Retrieved from University of Pretoria in May 2004 (Legal Track, Trial, v32 n10 p16 (7).

Eiselen S ‘E-commerce and the GISG Formation, Formalities and Validity’ (2002) 6 *Vindobona Journal of International Commercial Law and Arbitration* 305.

Eiselen S ‘The UNECIC: International trade in the digital era’ (2007) Vol. (2) *Potchefstroom Electronic Review* 11- 49.

F

Faria J ‘E-commerce and International Legal Harmonisation: Time to go beyond the Functional Equivalence?’ (2004) *South African Mercantile Law Journal* 529.

G

Gillies L ‘Addressing the Cyberspace Fallacy: Targeting the Jurisdiction of an Electronic Consumer Contract’ (2008) 16 *International Journal of Law and Information Technology* (3) 242.

Glatt C ‘Comparative Issues in the Formation of Electronic Contracts’ (1998) 1 in *International Journal of Law and Information Technology* 6.

Gregory J D ‘Solving legal issues in electronic commerce’ (1999) Vol 32 *Canadian Business Law Journal* 84.

H

Hoffman J ‘The Meaning of Exclusions in Section 4 of the ECT, Act 25 of 2002’ (2007) *South African Law Journal* 261.

J

Jacobs W ‘Sale of Medicine over the Internet’ (2005) 11 *South African Mercantile Law Journal* 17.

K

Kidd D Jr & Daughtery W Jr 'Adapting Contract Law to accommodate Electronic Contracts' (2000) 26 *Rutgers Computer and Technology Law Journal* 215.

Koger J L 'You Sign, E-sign, We all Fall Down: Why the United States should not Crown the Marketplace as Primary Legislator of Electronic Signatures' (2001) 11 *Transnational Law & Contemporary Problems* 498.

Kuczerawy A & Killian W 'United Nations convention on the use of communications in international contracts'in *CBKE – e – Biuletyn* (2007) (1) 7.

L

Loetz D J & Du Plessis C 'Electroniese Koopkontrakte: 'n Tegnologiese Hemel of Hel' (Deel-1) (2004) *De Jure* 1 (20) 224.

M

Mason S 'Electronic Signatures: The Technical and Legal Ramifications' (1999) *Computer and Law* 37.

Mason S 'Electronic Signatures in Practice' (2006) 2 *The Journal of Information Law and Technology Law* 148.

Morel F & Jones R 'De-mystifying Electronic Signature and Electronic Signature Law from a European Union perspective' (2002) 7 *Communication Law* (6) 174.

Morrison D 'The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?' (1992) Vol 14 *George Mason UL Review* 637.

N

Norwood J M 'Summary of Statutory and Case Law associated with Contracting in the Electronic Universe' (2006) *De Paul Business & Commercial Law Journal* 415.

P

Pacini C, Andrews C & Hilson W 'Contracting in Cyberspace (the CPA and the Computer)' (2002) 65 *New York State Society of Public Accountants CPA Journal* (3) 72.

Papadopoulos S 'Short message Services and E-contracting - *Jafta v Ezimvelo KZN Wildlife [2008] 10 BLLR 954 (LC)*' (2010) *Obiter* 188.

Phang A & Seng D 'The Singapore Electronic Transactions Act 1998 and the Proposed Article 2B of the Uniform Commercial Code' (1999) 7 *International Journal of Law and Information Technology* 2 103.

Pistorius T 'Formation of Internet Contracts: Contractual and Security issues' (1999) 11 *South African Mercantile Law Journal* 292.

Pistorius T 'Click Wrap and Web Wrap Agreements' (2004) *South African Mercantile Law Journal* 16.

Pistorius T 'From Snail Mail to E-ail – A South African Perspective on the Web of Conflicting Rules on the Time of E-ontracting' (2006) 39 *CILSA* 179.

Pistorius T 'Monitoring, Interception and Big Boss in the Workplace: Is the devil in the details?' (2009) *Potchestroon Electronic Review*

Pitiyasak S 'Electronic Contracts: Contract law of Thailand, England and UNCITRAL Compared' (2003) *Computer and Telecommunications Law Review*, available from WESTLAW (COMPTLR 9 (1) 16.

R

Reidenberg J R 'Technology and Internet Jurisdiction' (2005) *University of Pennsylvania Law Review* 1951.

S

Snail S 'The Validity and Enforceability of Electronic Wills' (2006) *De Rebus* August 2006 51.

Snail S & Hall N 'Electronic Wills in South Africa' (2010) Vol 7 *Digital Evidence and Electronic Signature Law Review* 67.

Stelzner S 'Contracts Over the Ether' (2008) *Without Prejudice* October Edition 41.

T

Towle H K 'Legal Developments in Electronic Contracting' (2000) *PLI Fourth Annual Internet Law Institute* 93.

Watnick V 'The Electronic Formation of Contract and the Common Law Mailbox Rule' (2002) 56 *Baylor Law Review* 196.

Theses

Archbold A *Are Contracts Concluded on the Internet Valid and Enforceable?: An Analysis of the Law applicable to Contracting on the Internet* (Unpublished LLM thesis, University of Cape Town, 1999).

Nagalingam S G *The Enforceability of Computer Contracts* (Unpublished LLB dissertation, University of Pretoria, 2000).

Conference, Convention and Workshop papers

AUCLCS 'The African Union Convention on the Establishment of a Credible Legal Draft Framework for Cyber Security in Africa (AUCLCS) 14th AU 2010 summit 'Information and communication technologies in Africa : Challenges and prospect for development' on 31 January 2010 – 2 February 2010, Addis Ababa, Ethiopia.

Eiselen S 'Contracting On-line'. Paper presented at 3rd Annual Conference on 'World Wide Web Applications' on 5 - 7 September 2001, available at *http://general.rau.ac.za/infosci/www2001/abstracts/eiselen.html*,(accessed on 5 October 2008).

Forster J S 'Electronic Contracts and Digital Signatures – the Future is Closer than You Think' (2000) available at *http://www.corinball.com/articles/art-digitalcontracts.html,* (accessed on 12 February, 2009.)

Gregory S , 'The UNICITRAL Draft Convention on Electronic Communications in International Contracting' (2004) 1 -13.

Hermann G 'Establishing a legal Framework for Electronic Commerce: The work of the United Nations Commission on International Trade (undated).

Lodder A 'Electronic Contract and Signatures: National Civil Law in the EU will Change Drastically Soon' (2000). Paper presented at the 15th BILETA Conference on 'Electronic Datasets and Access to Legal Information' 14 April 2000, University of Warwick England.

Mazotta F G 'Notes on the United Nations Conventions on the Effect of Electronic Communications in International Contracts and Its Effects on the United Nations Conventions on Contracts for the international sale of goods' (2007) *Rutgers Computer & Technology Law Journal* available at *http://www.entrepeneur.com/tradejournals/article/print/1698761139.html*, *(*accessed on 6 October 2008).

Murungi M 'Comments on The Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa' (2012) (version -1/01.2011) at 4-11, available at *http:// michaelmurungi.blogspot.com/2012/08/comments-on-draft-african-union.html* ,(accessed on 22 November 2012).

Patrikios A 'Resolution of Cross-border E-business Disputes by Arbitration Tribunals on the Basis of Transnational Substantive Rules of Law and E-business Usages: The Emergence of the Lex Informatica' (2006). Paper presented at the 21st BILETA Conference on 'Globalisation and Harmonisation in Technology Law' April 2006 Malta.

Pistorius T 'Contract Formation: A ComparativeStudy of Legislative Initiatives on Select Aspects of Electronic Commerce' (2002) 25 *CILSA* 130-31. Also available at *http://www.signelec.com/content/se/Articles_html*, (accessed on the 24th December 2007).

Pistorius T 'A comparative Study of Legislative Initiatives on Select Aspects of Electronic Commerce' (2007) available at *http://www.signelec.com/content/se/Articles_html*, (accessed on 24 December 2007).

Pistorius T 'The Legal Effect of Input Errors in Automated Transactions: The South African matrix' (2008) *Journal of Information, Law and Technology* 2 (8), available at *http://go.warwick.ac.za/jilt/2008_2/pistorius2*, (accessed on 14 February 2008).

Rheeders B 'Managing E-business: A Business Approach to Legal Aspects' (2006). Paper presented at a workshop on the 'Legal Ramifications in Information Technology & Cyberspace' 27-28 July 2006 Melrose, Johannesburg.

Rice D T 'Recent Trends in Determining Jurisdiction in Cyberspace' (2003). Paper presented at the 'IT Meets Telecon' conference hosted by the Computer Law Association at the Convention Centre 13-14 November 2003 Munich, Germany.

Shulze C 'The 2005 Hague Convention on Choice of Court Agreements' (2006). Paper presented at the conference on 'Regulating South African Commercial Law in a Globalised Environment' at the Nedbank Professional and UNISA Centre for Business Law 17 August 2006, Johannesburg.

Sibanda O 'Civil Jurisdiction in International E-disputes in the South African Magistrates' Courts: A Case of Gaps and Complexities' (2008). Paper presented at the Convention on 'Lex Informatica: The Law on Electronic Communications, Electronic Commerce and Information Technology' 2008. Pretoria.

Snail S 'Electronic Contracts in South Africa: Comparative perspectives'(2006). Paper presented at a workshop on 'Legal Ramifications in Information Technology and Cyberspace' 27 - 28 July 2006 , Melrose, Johannesburg and at South Africa's First Cyberlaw Conference, at the Innovation Hub, Pretoria.

Snail S L 'Electronic Contracts in South Africa - A Comparative Analysis' (2008) 2 *Journal of Information Law and Technology Law* available at *http://go.warwick.ac.uk/jilt/2008_2/snail*, (accessed on 13 January 2009).

Thurlow W H 'Electronic contracts in the United States and the European Union' (2001) *Electronic Journal of Comparative Law* Nov 2001 available at *http://wwe.ejcl.org/53/art53-1.html (accessed September 2010)*

UNCITRAL 'Electronic Commerce and International Legal Harmonisation: Time to go Beyond the Functional Equivalence?' (2003). Paper presented on 'ICT and E-Business Strategies for Development' at the High-level Regional Conference for Transition Economies 20-21 October 2003 Geneva.

UNCITRAL'. Paper presented at WIPO International Conference on 'Electronic Commerce and Intellectual Property' (1999) 14 – 16 September 1999, Geneva.

Wang M ‘Review of the Signature Regulations: Do they Facilitate or Impede Intentional Electronic Commerce?’ (2006). Paper presented at the ICEC August 14 -16, 2006 , Fredericton Canada.

Yankey A ‘The AU Draft Convention on Cybersecurity and E-transactions: Cooperation against Cybercrime’ (2012) Paper presented at 6 – 8 June 2012, Strasbourg – France.

CASE LAW

South Africa

Aird v Hockley 1936 EDL 117.

Allen v Sixteen Stirling Investments (Pty) Ltd 1974 4 SA164 (D) 172.

Back and Others NNO v Master of the Supreme Court 1996 2 All SA 161 *(C).*

Balzan v O'Hara & Others 1964 (3) SA (T).

Bisonboard Ltd v K Braun Woodworking Machinery 1990 ZASCA 86.

Bloom v The American Swiss Company 1915 AD 100.

Brand v Spies 1960 (4) SA 14.

Cape Explosives Works v Lever Brothers SA Ltd 1921 CPD 244.

Cape Explosives Works v SA Oil and Fat Industries 1921 CPD 24

Cinema City (Pty) Ltd v Morgenstern Family Estate 1980 1 SA 796

Collen v Rietfontein Engineering Works 1948 (1) S 413 (A).

Conrade v Rossouw 1919 AD 287.

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

Crawley v Rex 1909 TS 1105.

Dietrichsen v Dietrichsen 1911 TPD 486.

Durban's Water Wonder Land v Botha 1999 1 All SA 411 (A).

Estate Breet v Peri-Urban Areas Health Board 1955 3 SA 523 (A).

Efroiken v Simon 1927 CPD 367

Ex parte Maurice 1995 (2) SA 713.

Ewing McDonald & Co v M & M Products Co 1991 (1) SA 252 (A).

Federated Insurance Co Ltd v Malawana 1986 (1) 751 (A).

Goldblatt v Freemantle 1920 AD 123.

Greenberg v Washke 1991 WLD 1 7.

Hendrik Van der Merwe v Master of the High Court 2010 (605/09) ZASCA 99.

Hersch v Nel 1948 SA 686.

Humphreys v Casells 1923 TPD 280.

Hirshowitz v Moolman 1985 3 SA.

Jafta v Ezemvelo KZN Wildlife [2008] 10 BLLR 954 (LC).

Jamieson v Sabingo 2002 4 SA 49 (SCA).

Leobowitz t/a Lee Finance v Mhlana 2006 (6) SA 80 (SCA)18.

Letsekga v The Master & Others 1995 (4) SA 731 (W).

Kantor v Kantor 1962 (3) SA 207.

Kempstone Hire v Snyman (1988) (4) SA 465 (T) at 468 H.

Keregeulen Sealing & Whaling Co Ltd v Commissioner of Inland Revenue 1939 D 487.

MacDonald v The Master 2002 5 (SA) O 697.

Mafika Sihlali v SABC [2010] ZALC 1; (2010) and 31 ILJ 1477 (LC)).

Murray v Murray 1959 (3) SA 84 (W).

Nino Bonino v De lange 1906 TS 120.

Ramlal v Ramdhani 2002 (2) SA 643 (N).

Reid Bros v Fischer Bearings Ltd 1943 AD 232.

Rex v Nel 1921 AD 339.

Saambou-Nasionale Bouvereiniging v Friedman 1979 (3) SA 978 (A).

Sierhout v Minister of Justice 1926 AD 99.

Smeiman v Volkerz 1954 (4) SA 170 (C**).**

Sonop Petroleum v Papadogianis 1992 (3) SA 234 (A).

Spring Forest Trading 599 CC v Wilberry (Pty) Ltd TA Ecowash and Another – SCA Case No 72513

Swart v Vosloo 1965 1SA 100 (A).

South African Telkom SA Limited v *Napa Maepe, South Africa Telecommunications Regulatory Authority and The Internet Service Providers' Association (TPD) unreported case,* case number 258940/97.

Thirion v Die Meester En Endere 2001 (4) SA 1078.

Veneta Mineraria Spa v Carolina Colleries (Pty) Ltd (In Liquidation) 1987 (4) SA 883 (A)

Wilken v Kohler 1913 AD 135.

Wellness International Network v MV Navigator 2004 5 SA10.
Yates v Dalton 1938 EDL 177.

United States

Bancroft & Master Inc v Augusta Nat'l Inc 223 F. 3d 1082, 1087 (9th Cir 2000).
Beatty v First Exploration Fund 1987 and Another 25 BCLR 2d.377 (1988).
Corporation v Hasbro Inc No 02-2486, 314 F.3d.289.
Ellis Canning Co v Bernstein 348 F. supp 1212 (D.Colo.1972).
Franklin County Coop v MFC Services 441 So.2d 1376 (Miss. 1983).
Howley v Whipple 48 N.H.487, 488 (1869) C 98-20064 (N.D. Cal , April, 20 1998.)
Hines v Davidowitz 312U.S. 52, 67 (1941).
International Casings Group Inc v Premium Standard Firm Inc 358 F Supp 2d 863, 56 U.C.C Rp. Rv. 2d 736 (W.M. Mo. 2005).
Jonathan P Shattuck v David K Kolzenbach et al Barbara Kolzenbach, 01-1109A
Joseph Denzunzio Fruit v Cran, 79 F Supp.177 (S.D. Cal 1948).
Kohlmeyr & Co v Bowen 192 S.2d 400 (Ga. Ct App.1972).
Llan Systems v Netscout Service Level Corporation 183 F Supp 2d 328 (D mass 2002).
MacMillian v Weimer Drilling & Eng. Co. 512 So. 2d 14 (Ala.1986).
Michigan Canners & Freezers Assoc Inc v Agricultural Marketing & Bargaining Board 467 U.S. 461, 469 (1984).
North American System Shops 68 ALR 145 (Can QB 1989) .
Richard S Berger v Piranha Inc Civil Action No 3:-01-CV 2223-D.
Pro Cd v Zeidenberg & Siken Mtn. Web Services 86 F.3d 1447 (7th Cir 1996).
Shaw v Delta Air Lines Inc 463 US 85, 95-96 (1983)
Save–On Carpet of Arizona Inc 545 F.2d 1239 (9th Cir, 1976).
Selma Savings Bank v Webster County Bank 206 S.W. 870 (Ky. 1918).

Sprecht v Netscape Communications Corporation 150 F Supp 2d 585 (SDNY 2001).
US v Butler 297 U.S 1 (1936).

English

Adams v Lindsell [1818] EWHC KB J59.
Brinkibon Ltd v Stahag Stahl und Stahwarenhandelsgesellschaft GmbH 1 All ER 293.
Carlill v Carbolic Smoke Ball Company [1893] 1 QB 256 (CA) 268-269.
Entores Ltd v Miles Far East Corporation Ltd [1955] 2 QB327.
Henthorn v Fraser [1892] 2 Ch 27.

LEGISLATION

South Africa

Accreditation Regulation Government Gazette GN - NO. 29995 of 2007.
Alienation of Land Act 68 of 1981.
Basic Conditions of Employment Act 3 of 1997.
Bills of Exchange Act 7 of 1953.
Computer Evidence Act 57 of 1983.
Constitution, South Africa Act 108 of 1996.
Green paper on Electronic Commerce, November 2000.
Electronic Communications and Transactions Act 25 of 2002.
Interpretation Act 33 of 1957.
Labour Relations Act 28 of 1956 Land Alienation Act 68 of 1957.
Supreme CourtAct 59 of 1959.
Wills Act 43 of 1964.

United States

Uniform Computer Information Transaction Act (2002).
Uniform Electronic Transactions Act (1999).
Electronic Signatures in Global and the National Commerce Act, 15 USCA §§7001 – (2005).
Presidential Directive on Electronic Commerce, 1 July 1997.
Second Restatement of Contract No 22 (1974).
United States of America Constitution.

International Instruments and Officuial Documents

Africa

Green paper on e-commerce. Press release at http://www.polity.org.za/polity/govdocs/pr/2000/pr1119a.html (accessed on 12 October 2015).

Southern African Development Community (SADC Model Law of ElectronicCommerce), available at http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf. (accessed on 7 March 2013).

European Union

'EU Commission Directive on the Protection of Consumers in Respect of Distance Contracts' (Directive 97/7).

UNCITRAL

UNCITRAL. 'Recommendation on the Legal Value of Computer Records' (1985). Resolution 40/71 adopted at the 40th session of the General Assembly (11th December, 1985).

UNCITRAL. 'UNCITRAL Model Law on Electronic Commerce with Guide to Enactment Part I' (1996). Resolution 51/162 adopted by 85th session of the General Assembly at a plenary meeting (December 1996) available at *http://www.UNCITRAL.org/en-index.html* .

UNCITRAL. 'UNCITRAL Model Law on Electronic Signatures' (2001). Resolution 56/80 adopted at the 87th plenary meeting of the General Assembly (December 2001) available at

http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html .

UNCITRAL 'United Nations Convention on the use of Electronic Communications in International Contracts with Guide to Enactment' (2001). Resolution 51/162 adopted by 87th session of the General Assembly at a plenary meeting (December 1996) available at *http://www.UNCITRAL.org/en-index.html*, (accessed on 15 September 2008).

UNCITRAL 'Promoting confidence in electronic commerce: Legal issues on international use of electronic authentication and signature methods' (2009). Available at *http://www.uncitral.org/uncitral* (accessed on 7 March 2009).

UNCITRAL.'Convention on the Use of Electronic Communications in International Contracts. Resolution 60/21 adopted at the 60th session of the General Assembly (December 2005) . available at *http://www.UNCITRAL.org/en-index.html* (accessed on 7 March 2009).

UNCITRAL. The UNECIC in 'International Contracts Entered (2005) into force on 1 March 2013' – UNCITRAL press statement available at *http://www.uncitral.org* (accessed on 9 April 2013).

UNCITRAL. 'United Nations Convention on the use of Electronic Communications in International Contracts' (2005). Resolution 60/21 adopted at the 60th session of the General Assembly (December 2005) available at *http://www.UNCITRAL.org/en-index.html*.

Internet resources and websites

East African Community (EAC1 and EACII) available at http://www.eac.int/index.php?option=com_docman&task=doc_view&gid=632&Itemid=148 (accessed on 12 March 2013).

Erdle M 'On-line contracts: Electronic Creation of Effective contracts' (link cannot be recalled nor recovered).

Ghosh R 'The contractual validity of E-contract: An overview' available at *http://www.legalserviceindia.com/articles/econtracts.html*, (accessed on 12 February 2009).

LAWtrust *http://www.saaa.gov.za/accreditation_ProductsServices.htm/* (accessed 14 January 2013).

Mactaggart M 'Introduction to Cryptography Part 2: Symmetric Cryptography' (2001) available at *http:// www.ibm.com/developerworks/library/s-crypt02.html* (accessed on 12 February 2009).

Mactaggart M 'Introduction to Cryptography Part 3: Asymmetric cryptography' (2001) available at *http://www.ibm.com/developerworks/library/s-crypt03.html* (accessed on 12 February 2001).

Poznak Law Firm Ltd (2000) Internet Guide available at *www.poznaklw.com/articles/cyberjuris.html (*accessed 20 September 2003).

Smendinghoff T J & Hill R 'Electronic Signature Legislation' (1999) at 6, available from *http://library.findlaw.com/1999/Jan/1/241481.html,* (accessed on 6 October 2006).

Snail S L 'Legal Ramifications of the Use of Information Technology Devices at the Workplace' (2005) available at *http://www.bbatt.de*, (accesed June 2006).

South African Accreditation Authority (SAAA) Accreditation Regulations in Government Gazette No 2995 on 20 June 2007. available at *www.saaa.gov.za* (accessed on 3 March 2009)

South African Post Office Trust Centre available at *http://www.trustcentre.co.za/personal_certificates.php* (accessed 28 December 2013) and also see *http://www.saaa.gov.za/accreditation_ProductsServices.htm/* (accessed 28 December 2013).

Staude K 'Acceptance by SMS' (2008) available at *http://www.webberwentzel.com/wwb/view/wwb/en/page1873?oid=19142&sn=Detail* , (accessed on 7 January 2011).

Werksmans Inc 'Business Guide to Electronic Commerce and the Law' (2005) available at *http://www.werksman.co.za* (accessed on 22 September 2006).

Wheeler D A 'The Most iImportant Software Innovations' (2008) available at *http://www.dwheeler.com/innovation/innovation.html*, (accessed on 10 February 2009).

Zanger L M 'Electronic Contracts – Some of the Basics' (2000) 2 available at *http://www.mbc.com*, (accessed on 6 October 2006).