ENFORCEABILITY OF ELECTRONIC CONTRACTS IN AUSTRALIA

FARISA TASNEEM
LL.M, BAL, LLB

School of Graduate School of Business and Law
College of Business
RMIT University

January 2015
Declar

ation

I certify that except where due acknowledgement has been made, the work is that of the author alone; the work has not been submitted previously, in whole or in part, to qualify for any other academic award; the content of the thesis/project is the result of work which has been carried out since the official commencement date of the approved research program; any editorial work, paid or unpaid, carried out by a third party is acknowledged; and, ethics procedures and guidelines have been followed.

Farisa Tasneem

January 2015
ACKNOWLEDGEMENTS

The completion of this thesis would not have been possible without the support of Prof. Margaret Jackson, Prof. Donald Feaver, Prof. Benedict Sheehy, Prof. Siva Muthaly and Ms Prue Lamont. I would also like to acknowledge the support, patience and encouragement provided by my family.

Finally, I acknowledge the editorial assistance provided by Dr Lisa Lines from Elite Editing and Tutoring in relation to standardization of headings, table of contents, bibliography and general editorial support.

Papers originating from the thesis:


2. **Chapter 5 and 7**: Farisa T., ELECTRONIC CONTRACTS AND CLOUD COMPUTING Published in ERA ranked (1801) Journal - *international commercial law and Technology*, Vol 9, No 2, 2014 [Contribution: 100%].


4. **Chapter 8**: Farisa T., ELECTRONIC CONTRACTS AND PRIVACY: THE BIG DATA REVELUTION accepted for publication in Refereed journal International Journal of Technology, Policy and Law

5. **Chapter 6**: Farisa T., MISTaken IDENTITY AND MOBILE COMMERCE: CURRENT AND EMERGING ISSUES making minor changes for publication in Computer Law and Security Review.
CONTENTS

DECLARATION ........................................................................................................... ii
ACKNOWLEDGEMENTS ...................................................................................... iii
CONTENTS ............................................................................................................. iv
ABSTRACT .............................................................................................................. viii

CHAPTER 1 INTRODUCTION ................................................................................... 9
  1.1 Introduction ........................................................................................................ 9
  1.2 Current Legal Position .................................................................................... 11
  1.3 Significance ...................................................................................................... 15
  1.4 Thesis and Links to the Study .......................................................................... 17
  1.5 Aim and Research Questions .......................................................................... 19
    1.5.1 Primary Research Questions .................................................................. 19
      1.5.1.1 Secondary Research Questions ......................................................... 19
  1.6 Focus of the Thesis ........................................................................................ 19
    1.6.1 Research Method and Methodology ......................................................... 20
  1.7 Structure of the Thesis .................................................................................... 20
  1.8 Limitations ...................................................................................................... 24
  1.9 Important Definitions and Meanings .............................................................. 25
    1.9.1 Definition of Electronic Commerce ........................................................ 25
    1.9.2 Electronic Signatures: Meaning ................................................................. 27
    1.9.3 Electronic Contract: Meaning ................................................................ 29

CHAPTER 2 ENFORCEABILITY OF ELECTRONIC CONTRACTS AND
DEVELOPMENT OF INTERNATIONAL NORMS ............................................. 30
  2.1 Introduction ...................................................................................................... 31
  2.2 The Internet ..................................................................................................... 32
    2.2.1 Development of the Internet .................................................................... 33
  2.3 Development of Electronic Commerce ........................................................... 34
    2.3.1 Electronic Commerce and EDI ................................................................ 35
  2.4 Legal Response: A Historic Perspective .......................................................... 37
    2.4.1 Legal Issues and Response in European Countries .................................... 37
    2.4.2 United States ............................................................................................ 40
    2.4.3 United Kingdom ....................................................................................... 46
    2.4.4 Australia .................................................................................................... 50
    2.4.5 Canada ...................................................................................................... 58
  2.5 EDI Trading Partner Agreements and International Responses ....................... 59
    2.5.1 Need of Legal Rules .................................................................................. 63
  2.6 UNCITRAL and Development of International Norms ..................................... 64
    2.6.1 UNCITRAL: Functions and Methods of Work ......................................... 65
      2.6.1.1 Composition, Functions and Methods of Work .................................. 65
    2.6.2 History and Background of Model Law on Electronic Commerce ........... 66
  2.7 Electronic Signatures and International Developments: Coordination of
    Developments among International Organisations ............................................. 75
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.1.1 Instantaneous Communication</td>
<td>162</td>
</tr>
<tr>
<td>5.2.1.2 Deemed Receipt Rule</td>
<td>166</td>
</tr>
<tr>
<td>5.3 Time and Place of Contract Formation</td>
<td>172</td>
</tr>
<tr>
<td>5.4 Electronic Transaction Legislation of Australia: Time of Contract</td>
<td>179</td>
</tr>
<tr>
<td>5.4.1 Technical Aspects and the Electronic Transactions Legislation</td>
<td>182</td>
</tr>
<tr>
<td>5.4.2 Time of Receipt: Australia</td>
<td>185</td>
</tr>
<tr>
<td>5.5 Time and Place of Contract Formation: Position in the UK</td>
<td>188</td>
</tr>
<tr>
<td>5.6 Time and Place of Contract Formation: Position in the US</td>
<td>191</td>
</tr>
<tr>
<td>5.7 Conclusion</td>
<td>195</td>
</tr>
<tr>
<td>CHAPTER 6 ENFORCEABILITY OF ELECTRONIC CONTRACTS AND</td>
<td>197</td>
</tr>
<tr>
<td>MISTAKEN IDENTITY</td>
<td></td>
</tr>
<tr>
<td>6.1 Introduction</td>
<td>197</td>
</tr>
<tr>
<td>6.2 Online Transactions and Mistaken Identity</td>
<td>197</td>
</tr>
<tr>
<td>6.3 Traditional Common Law Principles and Mistaken Identity</td>
<td>198</td>
</tr>
<tr>
<td>6.3.1 Face To Face Dealings and Transactions Carried Out by Correspondence</td>
<td>199</td>
</tr>
<tr>
<td>6.4 Authentications and Carelessness of Parties</td>
<td>202</td>
</tr>
<tr>
<td>6.5 Electronic Authentication and Australia’s Response to International Norms</td>
<td>208</td>
</tr>
<tr>
<td>6.6 Electronic Authentication and Position in the UK</td>
<td>211</td>
</tr>
<tr>
<td>6.7 Electronic Authentication and Position in the US</td>
<td>214</td>
</tr>
<tr>
<td>6.8 Conclusion</td>
<td>220</td>
</tr>
<tr>
<td>CHAPTER 7 ENFORCEABILITY OF ELECTRONIC CONTRACTS: WRITING AND SIGNATURE REQUIREMENTS</td>
<td>223</td>
</tr>
<tr>
<td>7.1 Introduction</td>
<td>223</td>
</tr>
<tr>
<td>7.2 The Validity of Electronic Contracts, Writing Requirements and Response to International Norms</td>
<td>224</td>
</tr>
<tr>
<td>7.3 The Validity of Electronic Signatures and the Effect of Electronic Signatures</td>
<td>236</td>
</tr>
<tr>
<td>7.3.1 Trust</td>
<td>238</td>
</tr>
<tr>
<td>7.3.2 Features of Electronic Signatures</td>
<td>240</td>
</tr>
<tr>
<td>7.4 Position in the US</td>
<td>260</td>
</tr>
<tr>
<td>7.5 Position in the UK</td>
<td>264</td>
</tr>
<tr>
<td>7.5.1 Electronic Signatures: UK</td>
<td>266</td>
</tr>
<tr>
<td>7.6 Conclusion</td>
<td>277</td>
</tr>
<tr>
<td>CHAPTER 8 ENFORCEABILITY OF ELECTRONIC CONTRACTS: ISSUES ASSOCIATED WITH CLICKWRAP AGREEMENTS</td>
<td>279</td>
</tr>
<tr>
<td>8.1 Introduction</td>
<td>279</td>
</tr>
<tr>
<td>8.2 Online Transactions and Impact of Privacy Concerns</td>
<td>280</td>
</tr>
<tr>
<td>8.3 Click Wrap Agreements and Privacy Terms</td>
<td>281</td>
</tr>
<tr>
<td>8.4 Click Wrap Agreements and Privacy Policies</td>
<td>289</td>
</tr>
<tr>
<td>8.5 Position in the US</td>
<td>292</td>
</tr>
<tr>
<td>8.6 Position in the UK</td>
<td>293</td>
</tr>
<tr>
<td>8.7 Conclusion</td>
<td>295</td>
</tr>
<tr>
<td>CHAPTER 9 CONCLUSION</td>
<td>296</td>
</tr>
</tbody>
</table>
9.1 Introduction ................................................................................................................................. 296
  9.1.1 Primary Question One: Has the Electronic Transaction Legislation of
  Australia Resolved the Issues? ................................................................................................. 297
    9.1.1.1 Invitation to Treat ........................................................................................................ 297
    9.1.1.2 Time of Contract Formation .................................................................................... 300
    9.1.1.3 Place of Contract Formation ................................................................................. 304
    9.1.1.4 Signatures ................................................................................................................ 306
    9.1.1.5 Writing Requirements and Storage of Contractual Terms .................................. 308
    9.1.1.6 Conclusion of Primary Research Question .......................................................... 311
  9.1.2 What Issues Arise When Traditional Contract Principles are Applied
  to Electronic Contracts? ............................................................................................................. 313
    9.1.2.1 Click Wrap Agreements .......................................................................................... 313
    9.1.2.2 Mistaken Identity .................................................................................................... 316
    9.1.2.3 Conclusion of Primary Research Question Two .................................................. 317
  9.1.3 Sub-Question One: Do Other Jurisdictions Have the Same Issues? Is it
  an International Problem? ....................................................................................................... 317
    9.1.3.1 Writing and Storage of Contractual Terms .......................................................... 319
    9.1.4.2 Time ...................................................................................................................... 321
    9.1.4.3 Place of Business ................................................................................................... 322
    9.1.4.4 Signature ............................................................................................................... 322
    9.1.4.5 Click Wrap Agreements ......................................................................................... 324
    9.1.4.6 Mistaken Identity .................................................................................................. 325
  9.1.4 Sub-Question Two: What Is the Role of International Developments
  in Addressing Issues? How Is Australia Responding to the
  International Developments? .................................................................................................. 326
  9.2 Concluding Remarks: Summary of Major Findings, Contributions of the
  Research to the Area of Electronic Contracts and Recommendations ....... 328
    9.2.1 Recommendations and Suggestions ......................................................................... 329
  9.3 Areas for Future Research .................................................................................................... 330

BIBLIOGRAPHY ............................................................................................................................. 331

JOURNAL ARTICLES, CONFERENCE PAPERS AND NEWS PAPER
ARTICLES ........................................................................................................................................ 331

TEXT BOOKS ............................................................................................................................... 364

WEB SITES ..................................................................................................................................... 368

OFFICIAL REPORTS AND STATEMENTS ............................................................................. 373

INTERNATIONAL INSTRUMENTS ............................................................................................. 380

LEGISLATION .................................................................................................................................. 381
  AUSTRALIA ............................................................................................................................... 381
  UNITED KINGDOM .................................................................................................................. 382
  SINGAPORE ............................................................................................................................. 383
  GERMANY ................................................................................................................................. 384
  OTHER COUNTRIES ............................................................................................................... 384
  EUROPEAN COMMUNITY ..................................................................................................... 384

TABLE OF CASES .......................................................................................................................... 384
Electronic contracts must be legally enforceable and certain like traditional contracts, to establish a similar legal framework in an electronic environment. The Electronic Transaction Legislation of Australia has made an attempt to strengthen legal certainty of electronic framework while ensuring law keeps pace with technological development. Despite this, the enforceability of electronic contracts is not as certain and predictable as those of traditional paper-based contracts. These problems arise due to regulatory deficiencies. Different approaches to address this issue have been adopted by jurisdictions such as the United States (US) and the United Kingdom (UK); however, the issue has not been adequately resolved in these jurisdictions.

At the international level, various organisations such as the United Nations Commission on International Trade Law (UNCITRAL), the Organisation for Economic Co-operation and Development (OECD), the International Chamber of Commerce (ICC) and are working in close cooperation to resolve uncertainty surrounding electronic contracts. International developments also present the same deficiencies as are present at the national level. This thesis examines the current laws and reviews how international norms emerged and continue to resolve the issues.
CHAPTER 1
INTRODUCTION

1.1 Introduction
1.2 Current Legal Position
1.3 Significance
1.4 Thesis and Links to the Study
1.5 Aim and Research Questions
1.5.1 Primary Research Questions
1.6.1.1 Secondary Research Questions
1.6 Focus of the Thesis
1.6.1 Research Method and Methodology
1.7 Structure of the Thesis
1.8 Limitations
1.9 Important Definitions and Meanings
1.9.1 Definition of Electronic Commerce
1.9.2 Electronic Signatures: Meaning
1.9.3 Electronic Contract: Meaning

1.1 Introduction

The emergence of the internet has brought a tremendous revolution to all walks of life including business activities. Today the impact of the internet is so huge that it is unavoidable for the overall success of any business because this can be used as the most powerful tool in conducting both business-to-business and business-to-consumer transactions. Electronic commerce has resulted in electronic contracts. It enables people to gather vital information for conducting successful business transactions and form contracts. With the help of a simple click, world-wide business is possible with no huge expenditure or investment and the desired result is seen in minutes and seconds instead of hours and days unlike olden days.¹

The internet transcends geographic boundaries, cultures and time zones. Hence, the physical location of the seller is irrelevant to the buyer or consumer who can purchase goods or services over the internet. It has extended and transformed the boundaries of seller-buyer contracts, business consumer transactions and commercial transactions far beyond the confines of traditional markets and shops. By using the internet, an offer can be transmitted instantaneously to the other person or offeree. The offeree or the other party can review the agreement (document), consent to the contents of the document and accept the offer instantaneously by resending the document electronically using the internet. Challenges regarding the applicability of traditional laws to electronic contracts arise partly due to the novelty of electronic commerce and partly due to the global framework within which they take place on the basis of domestically oriented principles. Hence, it is necessary for the internet and electronic commerce to function in a trustworthy and certain online environment.

Despite the advantages of electronic contracts, the characteristics of reliability and certainty that usually accompany paper-based contracts such as a paper document signed by the party with ink are missing in an electronic contract. Therefore, recipients of electronic messages must be in a position to trust them, so that they can act by relying on the message and without there being a need for further verification. Security concerns should be addressed because online activities generate vast amount of data and leave behind vital information which can be misused.

Innovative technologies such as cloud computing are setting the stage for an enormous change in the sector which is already fast moving. Revolutionary and fast

---

6 Cloud computing can be defined as a computing model that provides on-demand network access to a shared pool of computing resources. Through cloud computing, data can be stored on the Web and can
growing, ‘cloud technology’ allows businesses to free themselves from the usual restraints associated with traditional computing. A web based application or service offered via the internet is called cloud computing. It can include cloud based word processor, email and power point presentation. Since it is web based and not desktop based, people will no longer be tied up to a single computer located in the office as the data can be stored on the web and can be accessed from anywhere in the world. Cloud computing encompasses multiple computers, multiple servers and multiple networks. Therefore, it opens door for more easy manipulation of data.

In today’s electronic world businesses heavily rely on information technology for carrying out different transactions. Smart phones and tablets provide easy access to information. Everyday vast amount of data is being created which represents a new era in data exploration and utilization. Management of big data created like this is more than a challenge as businesses now have more valuable information within their electronic systems which needs to be protected.

The internet and its related technologies are described in greater detail in Chapter 5 where its implications in relation to time and place of contract formation is highlighted. It is also discussed in Chapter 7 and Chapter 8 in relation to mistaken identity and click wrap agreements.

1.2 Current Legal Position

In Australia, the Electronic Transaction Legislation governs electronic transactions. It aims to allow for greater certainty in electronic transactions through compliance with international legal standards and in particular with the United Nations
The Convention on the Use of Electronic Communications in International Contracts 2005 which has been acceded by Australia.\(^\text{11}\) However, the legislation is not intended to provide a comprehensive legal framework, which could offer certainty in relation to the enforceability and legal effect of electronic contracts. It only provides a broad legal framework for the formation of electronic contracts.\(^\text{12}\)

It is also not clear whether the Electronic Transaction Legislation provides an adequate framework for effective formation of electronic contracts. Electronic contracts may not always fit within the legal framework that govern traditional contracts. For instance, electronic contracts may never appear on a piece of paper, may involve minimal or no human interaction, and may not be completely instantaneous. Despite these innovative features of electronic contracts, Electronic Transaction Legislation has a very narrow focus. It merely clarifies traditional law and rephrases traditional law to accommodate electronic contracts. Instead of drastically altering the purpose and effect of the law for electronic contracts, it merely rephrases it. Therefore, it does not provide a complete solution.\(^\text{13}\) For example, the broad criteria to be met for an electronic signature to be recognised under the Electronic Transaction Legislation as a valid signature is that the signature must identify the person and must indicate a persons intention with regards to the transaction. It further states that the signature method used to identify the person and indicate the intention of the person must be reliable and appropriate for the purpose for which information was communicated.\(^\text{14}\) This approach is known as the...

---


minimalist approach, as it provides minimal legal recognition to different types of electronic signatures.\textsuperscript{15} Signatures such as a name typed at the end of an email qualifies as a binding and legally enforceable signature, despite the limited ability of the party to verify the integrity and authenticity of the electronic contract. It is uncertain whether the minimalist approach provides adequate protection to the parties entering into an electronic contract. The protection that needs to be provided to the electronic contracts must be equivalent or similar to the well defined and clear protection that is available for the traditional contract. Electronic contracts do not meet the same standards of reliability, certainty, security performed by a traditional paper-based contracts, which are formed face-to-face in the presence of the parties, at the same time and in the same place.\textsuperscript{16}

A contract may be legally effective even in the absence of a signature. However, certain transactions or contracts are governed by legislation that require a signature to be legally binding and enforceable for example, The Statute of Frauds 1677 (UK), Property Law Act 1974 (Qld), Instruments Act 1958 (Vic), Conveyancing Act 1919 (NSW) and Law of Property Act 1936 (SA). Even when a signature is not required under legislation, a signature is important because it enhances the enforceability of the contract and provides additional assurance to the other party regarding the acceptance of the terms of the contract.\textsuperscript{17} A signature in such a contract indicates that the parties have agreed to the terms of the contract. Therefore, the presence of a signature not only prevents fraudulent transactions and contracts but also enhances the validity of a contract due to the valid and enforceable signature.\textsuperscript{18}


\textsuperscript{17} McCullagh, Little and Caelli, above n 16.

Similar uncertainties in relation to the enforceability of electronic contracts are found in other jurisdictions. Further, different electronic signature laws have emerged globally, which has created a patchwork of regulation. Some laws provide legal validity to electronic signatures irrespective of technology used to create the signature. Others provide legal validity to signatures based on a specific technology or to signatures that are more inclined towards a single technology. However, recognition of a single technology or signatures that are more inclined towards a single technology have disadvantages, such as creating barriers for the development of other technologies, facing the problem of an outdated adopted technology and frustration of the growth of free market. Laws that vaguely provide validity to different technologies have their own shortcomings, such as extending recognition to all technologies and all signatures that are created electronically, irrespective of their reliability and security.

As such, there is considerable ongoing discussion and debate regarding the appropriate legal framework for electronic contract. According to some authors,
traditional contract principles can be adapted and applied to electronic contracts.\textsuperscript{25} According to others, only international developments can resolve the issues related to electronic contracts.\textsuperscript{26} A third group of authors are of the opinion that electronic contracts need new rules for issue resolution.\textsuperscript{27} There is thus uncertainty regarding an appropriate legal framework for electronic contracts.

1.3 Significance

The research is significant as it identifies the strengths and weaknesses of electronic contracts to maximise the potential of electronic commerce. The research also makes an attempt to resolve the above discussion regarding an appropriate legal framework for electronic contracts. Further, the Expert Group that recommended adoption of the Electronic Transaction Legislation in Australia identified the importance and potential of electronic commerce as follows:\textsuperscript{28}

Electronic commerce has expanded from the closed world of business to business transactions between known parties to encompass a complex web of different activities involving large numbers of individuals, many of whom will never meet each other. It has implications for many facets of economic and social life and its development is ushering in a new era of global communication and trade. It has the potential to fundamentally change the way commercial transactions, the business of government, the delivery of services and a host of other interactions are conducted, raising issues at the heart of policies directed at the regulation of traditional practices and procedures.

The importance of online environment for conducting commercial transactions was highlighted by the expert group as follows:\textsuperscript{29}

There must be confidence that the infrastructure which already exists for paper exchanges can also be established for electronic exchanges, so that: services and

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{25} S E Tuma and C R Ward, above n 24; Donnie et al, above n 3.
\item \textsuperscript{26} Mazzotta, above n 24; Endeshaw, above n 24.
\item \textsuperscript{29} Ibid para 1.9.
\end{enumerate}
\end{footnotesize}
networks are secure and reliable; transactions are safe and private; there are ways to prove the origin, receipt and integrity of information received; there are ways to identify the parties involved; and there are appropriate redress mechanisms available if something goes wrong.

Although the internet has been used as a commercial medium for nearly a decade, the enforceability and legal effect of electronic contracts is an unresolved issue. Further, the importance of trustworthy online transactions as well as the importance of electronic commerce is being highlighted by most international organisations such as the UNCITRAL, OECD, and ICC. These organisations have expressed concerns in general regarding the need for the improvement of the online environment for the continued development of electronic commerce. OECD released a report titled ‘Shaping the Policies for the Future of the Internet Economy’ in 2008, which highlighted the importance of electronic commerce as follows:

Clearly, the Internet economy is already an important and growing part of our economies and societies, but to reach its full potential in meeting economic and social objectives, a policy environment in which the Internet’s role as catalyst can be maximised is essential.

UNCITRAL has released a reference document titled ‘Promoting Confidence in Electronic Commerce: Legal Issues on International use of Electronic Authentication and Signature Methods’ in 2007. It explains the importance of a reliable online environment as follows:

Creating trust in electronic commerce is of great importance for its development. Special rules may be needed to increase certainty and security in its use. Such rules may be provided in a variety of legislative texts: international

---

legal instruments (treaties and conventions); transnational model laws; national legislation (often based on model laws); self-regulatory instruments; or contractual agreements.

ICC highlights the importance of electronic commerce for conducting commercial transactions by stating that for:\(^3^4\)

..e-commerce to reach its full potential, certainty and confidence is essential for both businesses and consumers when disputes arise between them on-line.

The scope of this thesis is narrow as it specifically looks at enforceability of electronic contracts for the continued development of electronic commerce.

1.4 Thesis and Links to the Study

Traditional contract principles have their origins in case precedents, most of them decided before the internet was developed and thus not completely equipped to deal with electronic contracts.\(^3^5\) Electronic contracts do not change the application of traditional contract law principles but traditional contract law principles require adjustments to accommodate electronic contracts effectively.\(^3^6\) For instance, in traditional paper based transactions, there are accepted customs and practices in conjunction with acceptable legal rules which determine the rights and responsibilities of the parties. These practices often include controls such as:

1) Signature to evidence agreements
2) Proofs such as time and date stamping, which provide proof of dispatch and receipt or acceptance in some cases
3) Witnesses, notaries or other trusted third parties who acknowledge and authenticate transactions.\(^3^7\)

\(^3^5\) Hillman and Rachlinski, above n 24, 429, 430; Radin, above n 27.
\(^3^6\) Squires, above n 3; Christensen, Duncan and Low, above n 16; R A Horning, ‘The Enforceability of Contracts Negotiated in Cyberspace’ (1997) 5(2) *International Journal of Law and Information Technology* 109; Hillman and Rachlinski, above n 24, 429, 431.
These controls create the necessary level of legal certainty. In order to create viable electronic equivalents to traditional contracting activities, it is necessary to develop legal mechanisms or supportable legal analogues for the innovative digital infrastructure. The electronic transactions must be at least as efficient and secure as traditional transactions without forcing users to negotiate customised terms and conditions.\(^{38}\) The Electronic Transaction Legislation of Australia, which is based on international developments, attempts to resolve perceived uncertainty regarding the application of traditional principles. Hence, the consideration of common law principles within an electronic environment must take place in the light of the legislative framework.\(^{39}\) The law applicable to electronic transactions must be certain and predictable to enhance business and consumer confidence.\(^{40}\) The thesis examines the extent to which the Electronic Transaction Legislation of Australia provides an adequate and supportive legal environment.

Electronic contracts are of international significance and international developments in relation to electronic contracts are taking place to offer national legislators a set of internationally accepted rules.\(^{41}\) Due to the international and global nature of electronic contracts and electronic signatures, international developments are considered. Soft international norms are developed and standardised by international organisations. Soft norms are non-binding international instruments such as the *Model Law on Electronic Commerce 1996*.\(^ {42}\) The role of soft and hard international law developments seen in the form of UNCITRAL *Model Law on Electronic Commerce 1996*, UNCITRAL *Model Law on Electronic Signatures 2001*, OECD Declaration on Authentication 1998, Model trading partner agreements and the UN Convention on the Use of Electronic Communications in International Contracts 2005 are examined. These international developments are analysed to assess their role and significance in resolution of issues related to electronic contracts. Given the

---

\(^{38}\) P Diwan and S Sharma, above n 37; Squires, above n 3; Christensen, Duncan and Low, above n 16.


\(^{40}\) Christensen, above n 39; Christensen, Duncan, and Low, above n 16.

\(^{41}\) Christensen, above n 39; Christensen, Duncan and Low, above n 16.

international nature of electronic contracts, although the focus of the thesis is on assessing the impact of electronic transaction legislation of Australia, an analysis of similar developments introduced in other jurisdictions such as the United States (US) and the United Kingdom (UK) is undertaken. The thesis will specifically examine the legislative initiatives in regulating electronic contracts and electronic signatures in jurisdictions such as the US and the UK. These jurisdictions have been selected as they are among the top ten two-way trading partners of Australia, according to the Department of Foreign Affairs and Trade.\(^{43}\)

1.5 Aim and Research Questions

The aim of this research is to evaluate the role of Electronic Transaction Legislation of Australia in establishing an appropriate legal framework for electronic contracts.

1.5.1 Primary Research Questions

1. What issues arise when traditional contract law is applied to electronic contracts? Has the Electronic Transaction Legislation of Australia resolved the issues?

1.5.1.1 Secondary Research Questions

1. Do other jurisdictions have same issues? Is it an International problem?
2. What is the role of international developments in addressing issues? How is Australia responding to the international developments?

1.6 Focus of the Thesis

---

This thesis demonstrates that the traditional contract principles are inadequate. While the Electronic Transaction Legislation of Australia has also fallen short of its intended aim of facilitating as well as building business and community confidence in electronic contracts. This in turn has given rise to gaps in relation to electronic contracts, which can cripple the effective development of electronic commerce.

Like the Electronic Transaction Legislation of Australia, national legislation in other countries and international developments have adopted different paths for achieving the same purpose but are inadequate.

1.6.1 Research Method and Methodology

Doctrinal legal research method was employed and document analysis was carried out. The objective of doctrinal research will be to base any statements about what the law is on primary authorities such as the cases and legislation. Document analysis was carried out to evaluate two sets of laws, traditional contract principles and the Electronic Transaction Legislation of Australia. Additional insights on issues related to electronic contracts were obtained by evaluating analogous laws of different countries and international developments on electronic contracts.

1.7 Structure of the Thesis

The thesis is divided into nine chapters. Chapter One is an introduction to the thesis and provides an overview of the nine chapters. The chapter also identifies the need for conducting research in this area. It deals with significance and limitations of the research.

Chapter Two: Enforceability of Electronic Contracts and Development of International Norms examines the manner in which international norms were developed, which ultimately resulted in the development of Model Law on Electronic Commerce 1996. It examines the issues related to electronic commerce and maps

44 Squires, above n 3; Christensen, above n 39.
how similar developments took place in different countries including Australia from an international perspective. For assessing the development of norms, the chapter provides an overview of issues related to traditional writing requirement, signature and traditional contract Law. The historic developments of internet and transformation of internet into a commercial medium, and development of electronic commerce are initially discussed. It is followed by the analysis of shortcomings of traditional laws of different countries and evaluation of international developments as seen in UN such as the Model Law on Electronic Commerce and Model Law on Electronic Signatures. International developments undertaken by ICC and OECD are also considered in this chapter. Initial attempts made to resolve the issues globally through trading partner agreements are also assessed. Analyses of national and international developments are undertaken to determine the role and significance of international developments in resolving issues related to electronic contracts and electronic signatures. Then, the nature and scope of international law and of soft international law is discussed to explain how establishment of a common international understanding of norms takes place and how it affects national laws. The chapter also examines the impact of international developments on Australia.

Chapter three: The Transformation of International Norms Into National Norms and Enforceability of Electronic Contracts examines the transformation of international norms into national norms. It analyses the manner in which the Electronic Transaction Legislation of Australia was finally introduced based on the Model Law of Electronic Commerce 1996. It assesses how the need for Electronic Transaction Legislation was realised in Australia. The impetus behind the development of the Electronic Transaction Legislation is also examined. The impact of international developments on Australia is also examined.

This chapter provides an understanding of how different issues related to electronic commerce arose in Australia, the manner in which attempts were made to resolve, how international norms ultimately became national norms, and the extent of the influence of the soft international developments on Australia. The impact of international developments on Australia is also examined. The chapter establishes that technology and fear of uncertainty provided the main impetus for the
introduction of Electronic Transaction Legislation, coupled with the influence of international developments such as UNCITRAL Model Law on Electronic Commerce 1996 and the OECD Declaration on Authentication.

Chapter Four: Enforceability of Electronic Contracts: Issues Associated With Invitation to Treat and Electronic Mistakes evaluates whether an electronic contract is valid and enforceable in the same manner as a traditional or paper-based contract. Analysis of the application of traditional principles is undertaken to understand whether traditional law can effectively accommodate electronic contracts without crippling the development of electronic commerce. Consequently, the chapter analyses the broader basic principles of contract law and assesses the nature of electronic agreements. The discussion then proceed to evaluate the effect of regulatory measures on the contact formation process. This chapter establishes that the Electronic Transaction Legislation of Australia is deficient. As a result, gaps related to invitation to treat and electronic mistakes still exist. The impact of international developments on Australia is also examined.

Chapter Five: Enforceability of Electronic Contracts: Issue of Time and Place of Contract Formation analyses the relevance of the electronic acceptance, postal acceptance rule and jurisdiction within the realm of contract formation. Chapter five explores those aspects of electronic contacts that cannot be accommodated under traditional laws. The chapter establishes that the traditional contract principles related to acceptance, time of contract formation and jurisdiction are clearly displaced and inadequate in the electronic environment. The impact of international developments on Australia is also examined. It submits that these deficiencies have given rise to gaps that can cripple the effective development of electronic commerce. The discussion then proceed to evaluate the effect of regulatory measures on the contact formation process. This chapter establishes that the Electronic Transaction Legislation of Australia is deficient. As a result, gaps related to time and place of contract formation persist.

Chapter Six Enforceability of Electronic Contracts and Mistaken Identity analyses the effect of mistaken identity issues on electronic contract formation. Chapter six
explores those aspects of mistaken identity issues that cannot be accommodated under traditional laws. The chapter establishes that the traditional contract principles related to mistaken identity are clearly displaced and inadequate in the electronic environment. The discussion then proceed to evaluate the effect of regulatory measures on the contract formation process. The impact of international developments on Australia is also examined. This chapter establishes that the Electronic Transaction Legislation of Australia is deficient. As a result, gaps related to mistaken identity exist.

Chapter Seven Enforceability of Electronic Contracts: Writing and Signature Requirements highlights the importance of electronic signatures and discusses both the technical features of electronic signatures and different types of electronic signatures. It also identifies the impact of security risks on electronic contracts. Doctrines that are being developed to validate electronic signatures are also evaluated. The impact of international developments on Australia is also examined. This chapter provides an understanding of how issues related to electronic writing and electronic signatures requirement are resolved by the Electronic Transaction Legislation. This chapter establishes that the Electronic Transaction Legislation of Australia has fallen short of its intended aim of facilitating electronic commerce and building business and community. As a result, gaps related to electronic contracts and signatures exist.

Chapter Eight Enforceability of Electronic Contracts: Issues Associated With Click wrap Agreements. They are agreements where the user is made to view the relevant terms and then click ‘I agree’ in order to enter into a contract. Click wrap Agreements continues the analysis of electronic contracts by specifically examining the issues associated with click wrap agreements. This chapter devotes special attention in examining one sided terms which are incorporated through click wrap agreements. The impact of international developments on Australia is also examined. Cases dealing with Click wrap Agreements are examined and its impact on the development of electronic commerce is evaluated in this chapter.

---

Chapter Nine concludes the thesis. It brings together the conclusions derived from the analyses of traditional laws, analysis of electronic transaction law of Australia, analysis of similar laws in other jurisdictions and international developments. The conclusion specifies the overall implications of the research.

1.8 Limitations

There are very few Australian cases specifically dealing with electronic contracts or testing the Electronic Transaction Legislation of Australia. There have been a few cases in the other jurisdictions that are discussed but they can only be considered persuasive.

The research examines the impact of Electronic Transaction Legislation of Australia. Hence, the analysis of traditional contract principles and traditional laws has been made only to the extent of assessing the impact of Electronic Transaction Legislation of Australia. This thesis deals specifically with electronic contracts; hence, the thesis only deals with the issues related to invitation to treat, electronic mistakes, time of contract formation, place of contract formation, mistaken identity, writing requirements, signature requirements and click wrap agreements.

Analysis of other jurisdictions is made only to the extent of understanding different legislative approaches adopted globally. To avoid repetition, only those provisions of other countries and international developments that differ from the Electronic Transaction Legislation of Australia are discussed.

The research specifically focuses on electronic contracts and one particular aspect of electronic contracts: electronic signatures. Digital signatures based upon Public Key Infrastructure (PKI) are a sub-set of electronic signatures. Hence, PKI and issues associated with the liabilities of certification authorities are not discussed in the thesis. The scope is further limited as the research specifically focuses on transactions conducted through computer communication utilising either an open or a closed network. Therefore, other electronic media such as telex and fax are
excluded. Issues of electronic contracts formed through mobile phones are discussed only to the extent of illustrating the intensity of the issue. Smart phones are nothing but mini computers therefore, issues of electronic contracts formed through smart phones are also discussed only to the extent of illustrating the intensity of the issue.

1.9 Important Definitions and Meanings

Some important definitions and meanings that indicate the scope of the thesis are provided in this section.

1.9.1 Definition of Electronic Commerce

Electronic commerce does not have a single widely accepted definition. The OECD provides the following definition:

Electronic Commerce refers generally to all forms of commercial transactions involving both organisations and individuals, that are based upon the electronic processing and transmission of data, including text, sound and visual images. It also refers to the effects that the electronic exchange of commercial information may have on the institutions and processes that support and govern commercial activities. These include organisational management, commercial negotiations and contracts, legal and regulatory frameworks, financial settlement arrangements, and taxation, among many others.

UNCAD takes a different approach and provides both a narrow and a broad definition of electronic commerce as follows:

The narrow definition is that electronic commerce is a commercial transaction whereby the order for a good or service is made using some form of Internet based communication. The delivery and payment may be performed off-line in the physical world.

---


49 The United Nations Conference on Trade and Development (UNCTAD) was established in 1964 to promote the integration of developing countries into the world economy in a development-friendly way. UNCTAD <http://r0.unctad.org/ecommerce/ecommerce_en/faq_en.htm>.
The broad definition includes the use of Internet and non-Internet communications systems, such as telephone ordering, interactive television and electronic messaging. The broad definition would also include privately owned electronic networks usually run by businesses and their partners for their own account. It is important that the buyer and seller do not meet physically during the order placement. Instead they use some kind of electronic communication device to close the deal.

The New Zealand Ministry of Economic Development provides a wide definition of electronic commerce. According to the New Zealand Ministry of Economic Development: 50

Electronic commerce refers to all commercial transactions based on the electronic processing and transmission of data, including text, sound and image. This includes Electronic Data Interchange (EDI), EFTPOS, electronic banking, digital cash and other electronic payment systems, but particularly refers to commerce transacted over the Internet.

The US Department of Commerce also provides a broad definition of electronic commerce. According to the US Department of Commerce: 51

Electronic commerce is a means of conducting transactions, that prior to the evolution of internet in 1995 as a business tool, would have been completed in more traditional ways.

The term electronic commerce was defined by the Australian Law Reform Commission, in the report titled ‘Legal Risk in International Transactions’ as follows: 52

In this report electronic commerce’ includes all business transactions on, or using facilities provided by, electronic networks and extends to non-transactional interchanges such as electronic mail and personal entertainment.

There has been much discussion in the last couple of years about the opportunities that are expected to be generated from electronic commerce.

The Electronic Commerce Expert Group report that considered the implementation of the UNCITRAL Model Law on Electronic Commerce 1996 in Australia states:

Electronic commerce is a broad concept that covers any commercial transaction that is effected via electronic means and would include such means as facsimile, telex, EDI, Internet, and the telephone.

However, for the purpose of the report, the Expert Group limited the application of the term ‘electronic commerce’ to ‘those trade or commercial transactions involving computer to computer communications whether utilising an open or closed network’.

This thesis adopts the definition of electronic commerce provided by the Electronic Commerce Expert Group. The term ‘electronic commerce’ is used in this thesis to refer to commercial transactions conducted through computer-to-computer communication. This definition has been adopted as the Electronic Transaction Legislation of Australia was based on the recommendations of the Expert Group.

1.9.2 Electronic Signatures: Meaning

The word ‘signature’ comes from the Latin word ‘signare’, which means ‘to sign or mark’. The Random House Unabridged Dictionary defines ‘signature’ as a ‘person’s name, or a mark representing it, as signed personally or by deputy, as in subscribing a letter or other document’. It also defines ‘signature’ as ‘the act of signing a document’. Webster’s Dictionary defines ‘signature’ as ‘the name of one as written by oneself’.

54 Ibid.
55 Ibid.
56 Webster’s New World Medical Dictionary (3rd ed, 2008).
58 Webster’s Dictionary (Webster’s II New Riverside University Dictionary, United States, 1988) 1083.
Signatures in a contract are important and well recognised in contract law, though very little is written about traditional signatures. The concept of witnessing, particularly by notaries, has been recognised establishing the importance of signatures. Traditional signatures are mainly used as evidence and they are verified only in case of a dispute. Hence, traditional signatures have forensic value and evidential value.

Electronic signatures are nothing than an electronic confirmation of authentication. Thus, the definition of electronic signatures is very broad and includes all forms of electronic identification such as informal and insecure initials at the end of an email to highly secure and formal iris scans. Digital signatures, which are a sub-set of electronic signatures, also fall under the description of electronic signatures.

Electronic signature is a term used to describe ‘signatures’, which are affixed or incorporated in electronic contracts or documents through electronic or cryptographic means. Some of the examples of electronic signatures include insertion of scanned version of the signatory or signer’s signature in an electronic transaction or typewritten name of the signer or signatory at the end of an email or electronic communication or using cryptographic technology such as digital signature or a person clicking ‘I accept’ button and the use of password. Electronic signatures may function in the same way as a handwritten signature, by identifying the person who has affixed or appended the signature to the electronic communication or document and may indicate the willingness and agreement of the signatory regarding the content of the electronic document. However, in most of the examples of electronic signatures identified above (except digital signature) the sender’s identity and the integrity of documents cannot be established. This thesis deals specifically with

electronic signatures and will focus particularly on insecure electronic signatures. Hence, PKI related to digital signatures, where a Certification Authority acts as a trusted third party will not be discussed in this thesis.

1.9.3 Electronic Contract: Meaning

An electronic contract is an agreement that is created and signed electronically. It can be described as a contract formed through electronic means such as email transactions, Electronic Data Interchange (EDI) transactions and online shopping scenarios.

---

CHAPTER 2
ENFORCEABILITY OF ELECTRONIC CONTRACTS AND DEVELOPMENT
OF INTERNATIONAL NORMS

2.1 Introduction
2.2 The Internet
2.2.1 Development of the Internet
2.3 Development of Electronic Commerce
2.3.1 Electronic Commerce and EDI
2.4 Legal Response: A Historic Perspective
2.4.1 Legal Issues and Response in European Countries
2.4.2 United States
2.4.3 United Kingdom
2.4.4 Australia
2.4.5 Canada
2.5 EDI Trading Partner Agreements and International Responses
2.5.1 Need of Legal Rules
2.6 UNCITRAL and Development of International Norms
2.6.1 UNCITRAL: Functions and Methods of Work
2.6.1.1 Composition, Functions and Methods of Work
2.6.2 History and Background of Model Law on Electronic Commerce
2.7 Electronic Signatures and International Developments: Coordination of
Developments among International Organisations
2.7.1 UNCITRAL Model Law on Electronic Signatures
2.8 Soft International Law
2.8.1 Scope of Soft International Law
2.8.2 Reasons for the Adoption of Soft Instruments and Nature of Soft Laws
2.8.3 The Difference between Hard Law and Soft Law
2.8.4 Impact of Soft Law on National Law
2.8.4.1 Common Issues of the First Two Proposals
2.8.4.2 Role of Model Laws as Guiding Principles
2.8.4.3 UN Convention and the Response of Other Countries
2.9 Conclusion
2.1 Introduction

This chapter provides a broad international picture of issues and examines the international norm generation process. Since it is impossible to analyse the traditional laws of all the countries, the analysis centres upon two major groupings: common law and civil law. This chapter only provides a brief overview of the most relevant laws of these countries.

The aim of this chapter is to examine the manner in which international norms were developed to regulate electronic commerce. This chapter will provide an overview of the development of the internet, transformation of the internet into a commercial medium, development of electronic commerce and how issues associated with electronic commerce arose internationally. UNCITRAL adopted the Model Law on Electronic Commerce in June 1996. This chapter will review some of the attempts made by model laws and model trading partner agreement to accommodate electronic commerce and the resulting impact on the law. The origin of UNCITRAL and the development of the model laws will be discussed to examine the international efforts made to regulate electronic commerce.

This chapter commences by discussing the development of internet and electronic commerce. After some preliminary explanation of internet and electronic commerce, the chapter analyses the how EDI transactions were conducted during the 1970s and the manner in which issues related to EDI transactions arose in different countries between 1982 and the late 1990s. Then, attempts made to regulate the issues through EDI trading partner agreements are analysed. Next, the first international attempt to harmonise EDI transactions through the preparation of the Uniform Rules of Conduct for Interchange of Trade Data by Tele transmission (UNCID) in 1987 and the development of model trading partner agreements by different countries is discussed. The chapter proceeds by analysing the attempts made to regulate electronic contracts

---

2 They are agreements that were used by the trading partners to negotiate customised terms and conditions. P Diwan and S Sharma, E-Commerce: A Manager’s Guide to E-Business (2005) 216–220.
and electronic signatures by UNCITRAL. The chapter also outlines and highlights the role of other international organisations such as OECD and ICC in issues resolution.

2.2 The Internet

The internet can be described as a network of networks.\(^3\) It is an open, worldwide network that enables communication and exchange of the data between computers connected to a network through a number of standardised protocols.\(^4\) The internet began in the late 1960s as a US government funded computer network equipment. In 1958, the Defence Advanced Research Projects Agency (DARPA) was established to assure that the US maintained a lead in applying technology for military capabilities. One of DARPA’s aims was to establish a communication network that would withstand military attacks.\(^5\)

The Department of Defence created a system of linked computer networks that were first called ARPANET.\(^6\) Most of the civilians who had collaborated with the Department of Defence were researchers at universities. Several academic institutions became involved as the academics found the network an efficient mode of communication. In 1973, the first international connection was established with the University College London by means of a Norwegian network. After a few years, institutions and individual users established connections to other networks such as USENET, BITNET and CSNET. Due to increasing non-military use, ARPANET split into MILNET and NSFNET.\(^7\) MILNET is the US military network.\(^8\) NSFNET

---


\(^7\) Quirk and Forder, above n 5, 6–7.

\(^8\) Military Network (MILNET) <http://www.milnet.com/milnet-history.html> 24 October 2006; Quirk and Forder, above n 5, 6–7.
was established by the US National Science Foundation. ARPANET retired in 1990 and later NSFNET became the corner stone of the internet.  

NSFNET grew and many international connections were established, which included Canada, Finland, France, Norway and Sweden. In 1989, further international connections were established such as Germany, Israel, Mexico, the Netherlands, New Zealand and the UK. In 1989, the Australian universities and the Commonwealth Scientific and Industrial Research Organisation (CSIRO) under the Australian Vice Chancellor’s Committee (AVCC) initiated a project called the Australian Academic Research Network (AARNET). The AARNET established the base of the Internet in Australia. NSFNET expanded constantly and the number of hosts on NSFNET exceeded 100,000 by 1989.

2.2.1 Development of the Internet

In 1983, Transmission Control Protocol and Internet Protocol (TCP/IP) became the communication protocol. The TCP/IP are the standard protocols that divide messages into packets of data and send it over the networks. The word ‘internet’ is named after the internet protocol, which is the standard communication protocol used by all the computers of the world. Messages are divided into packets of data and each packet carries its destination address. When the messages reach their destination they are rearranged by the TCP/IP protocols. In order to exchange email text messages and files in a particular format Simple Mail Transfer Protocol (SMTP) and File Transfer Protocol (FTP) were developed. However, in 1984, the Domain Name System (DSN) was introduced, which removed the need to make use of an IP protocol numbers as addresses.

---

9 National Science Foundation <http://www.nsf.gov/about/history/> 24 October 2004; Quirk and Forder, above n 5, 7.
10 Quirk and Forder, above n 5, 7.
12 Quirk and Forder, above n 5, 8–9; The Internet Society (ISOC) <http://www.isoc.org/internet/history> 20 July 2006.
14 Quirk and Forder, above n 5, 8–9.
15 Ibid 7–9.
In 1979, DARPA had established a committee known as the Internet Configuration Control Board. It guided the development of internet protocols. In 1983, this committee was renamed as the Internet Activities Board (IAB) when TC/IP became the standard protocol. The IAB was supported by funds from the DARPA, NSF, NASA, and the Department of Energy (DOE). The Internet Engineering Task Force (IETF) and The Internet Research Task Force (IRTF) are two coordinating task forces of IAB. IETF creates, develops and tests the internet standard protocols and the IRTF carries out research on future internet developments.\textsuperscript{16}

The next stage in the development of internet was the World Wide Web (WWW). It enhanced the capabilities of internet by providing a graphical environment.\textsuperscript{17} Later, protocols were developed to enable new internet services, such as internet relay chat.\textsuperscript{18}

2.3 Development of Electronic Commerce

Electronic commerce began with direct computer-to-computer communication by means of telephone lines or cable connections. The first electronic commerce activity began in the 1970s when banks in the US implemented the electronic funds transfer (EFT) system. Later, this technology was also adopted by other organisations that did regular business with each other. A business would fill forms electronically on their own networks and then transfer all the data in batches to each other. The term coined for this type of arrangement and transactions was known as EDI.\textsuperscript{19} In the 1970s and 1980s, businesses began to establish standard electronic forms for their common business documents via EDI and this was used by the businesses for receiving and sending purchase orders, invoices and shipping notifications.\textsuperscript{20} EDI allowed

\textsuperscript{16} Ibid 15.
\textsuperscript{18} Quirk and Forder, above n 5, 9.
\textsuperscript{20} Ibid.
companies to automate their purchasing procedures. This was done by structuring and coding the data such that the receiving computer could automatically transfer the data to accounting, inventory management and other business software.

Since the mid-1990s, the Internet has been used interestingly for commercial transactions. Initially, it was used for conducting business-to-consumer activities. Later, it was realised that the web technology is also suitable for commercial activities and exchange business information between large companies. The web pages combine multimedia and the ability to intercommunicate. This interactive nature of the web enhanced the potential of the internet as a commercial tool by enabling sellers to communicate with potential buyers.

2.3.1 Electronic Commerce and EDI

During the 1970s, EDI transactions were conducted by different industrial sectors and each sector had developed its own set of data elements and messages to meet the specific needs of a particular industry. For example, standards, such as the organisation for Data Exchange by Tele transmission (ODETTE) were developed in Europe. It is an organisation formed by the automotive industry to developed standards specifically for companies associated with the automobile industry. Similarly, TRADANET standards for retail industry in the UK. AUTOPACK

adopted by the automotive industry representing vehicle manufacturers, suppliers, telephone plus and the EDI service providers in Australia.28

Business organisations also began to conduct cross-industry trading and hence the need for national standards was realised. By the late 1970s, the need to develop EDI standards that could be used across industry sectors and across national boundaries was recognised and the work to develop the standards was initiated by standards groups and industry organisations.29 In 1979, the American National Standards Institute (ANSI) formed the Accredited Standards Committee (ASC) X12 to develop uniform standards for electronic interchange of business transactions.30 Similarly, in 1981, national standards called the Guidelines for Trade Data Interchange (GTDI) emerged in Europe.31

By the early 1980s, the integration of EDI into ongoing business practices had occurred and was expected to continue at a considerable rate. EDI transactions were expected to become the predominant method of sale contracting.32 By combining the functional capabilities of computers, companies exchanged information electronically rather than sending and receiving paper documents. By eliminating reliance upon paper as the medium through which commerce occurred traditionally,
new and different approach emerged regarding how commercial relationships were defined and maintained. The technologies of electronic commerce confronted legal barriers. Commercial parties wished to be certain that the advantages of employing the technologies are not undermined by the presence of legal obstacles or uncertainties that might erode confidence in the systems even before being installed and tested. The following section highlights these issues and concerns.

2.4 Legal Response: A Historic Perspective

Several countries expressed continued concerns regarding lack of appropriate legal rules for rapidly growing field of electronic commerce from 1980 to late 1990s at the national level. An overview and a brief summary of these issues and developments that took place in the past are discussed below.

2.4.1 Legal Issues and Response in European Countries

As early as 1982, the Nordic Legal Committee formed by the Nordic Council of Ministers conducted a survey of legal and security issues created by EDI. The survey showed that EDI transactions could give rise to security and legal issues. Security concerns were expressed and need for appropriate security procedure was identified as data in an electronic form was easily alterable unlike traditional paper-based documents.

---

33 ABA, Electronic Messaging: A Report of the Ad Hoc Sub-Committee on the Scope of the UCC 5 (1988). As a result of these changes, the ABA suggested that there was a need to re-examine the fundamental principles of contract.
36 UNCITRAL, Legal Aspects of Automatic Trade Data Interchange, Transmitted by the Delegations of Denmark, Finland, Norway and Sweden, UN Doc A/CN.9/238 (1983).
The Nordic council is a regional organisation that was established in 1952 by the governments of Denmark, Norway, Iceland and Sweden. It was also found that the EDI transactions were not satisfactorily accommodated by the legal rules, as electronic form was not contemplated by many traditional laws. For example, Article 6 of the Accounting Act 1977 of Norway specified legal requirements in terms of paper-based documents. It required records to be bound or stitched and maintained in a long-lasting manner. It was uncertain whether data stored on an electronic medium would be regarded as valid.

The report recommended an international action as EDI was widely used by many industries for conducting cross-border transactions. It proposed different international organisations to initiate work on EDI as follows:

- There is an urgent need for international action to establish rules regarding legal acceptance of trade data transmitted by telecommunications since this is essentially a problem of international trade law, the United Nations Commission for International Trade Law (UNCITRAL) would appear to be the central forum.
- The work could be undertaken in co-operation with the Customs Co-operation Council (CCC), which is actively engaged in establishing rules concerning important aspects of administrative law; with the Organisation for Economic Co-operation and Development (OECD) for aspects related to trans border data flows; and with other international organizations, such as the International Chamber of Commerce (ICC), in the commercial field, to ensure compatibility.

In 1988, the Commission of Europe began to develop the TEDIS (Trade EDI Systems) Programme. One of its purposes was the development of an appropriate legal framework for EDI in the member states of the European communities. It examined the legal issues related to the use of EDI and found that none of the

---

41 UNCTRALT, Legal Aspects of Automatic Trade Data Interchange, Transmitted by the Delegations of Denmark, Finland, Norway and Sweden, UN Doc A/CN.9/238 (1983).
42 Ibid.
European countries had appropriate legislation to facilitate EDI transaction. The TEDIS program identified the requirements for written paper-based documents and manual signatures legal requirements as the major legal impediments to the use of EDI. There were rigid requirements for signatures. Article 126, indent 1 of the German Civil Code required handwritten signature of the signatory accompanied with the name of the signatory. The term ‘document’ provided under Article 415 of the German Code of Civil Procedure required the contents to be in writing. It was uncertain whether electronic documents could satisfy the requirements of a ‘document’ prescribed under Article 415 of the German Code of Civil Procedure. Similarly, Article 1341 of the Belgian Civil Code required written evidence for agreements that exceeded the amount of BF 3000. The priority given to written documents was perceived as an obstacle to the development of electronic commerce by the TEDIS study.

After surveying the national laws of European countries, the commission in 1989 released its report. Apart from issues of data security and confidentiality, the commission identified three principal legal impediments and summarised it as follows:

(i) the obligation (where imposed) to make out, produce, send or preserve signed paper documents;
(ii) the evanescence of information sent by electronic data interchange and the consequent difficulty of adducing proof of what had been transmitted; and
(iii) the difficulty of determining the moment and place at which a transaction effected by electronic data interchange takes place.

Ibid 65.
Ibid 32.
During the 1990s, the lack of predictability and the certain legal environment was identified by the European commission as follows:\textsuperscript{49}

building trust and confidence among businesses and consumers implies the deployment of secure technologies (such as digital signatures, digital certificates and secure electronic payment mechanisms) and of a predictable legal and institutional framework to support these technologies. In order to allow for electronic commerce operators to support these technologies. In order to allow for electronic commerce operators to reap the full benefits of the Single Market, it is essential to avoid regulatory inconsistencies and to ensure a coherent legal and regulatory framework for electronic commerce at EU level. This should be based on the application of key Internal Market principles.

Regulatory responses, where appropriate, need to be addressed at every step of the business activity from the establishment of business, to the promotion and provision of electronic commerce activities, through conclusion of contracts, to making of electronic payments.

Three groups of issues arose in the Europe, the first group were those related to the evidential aspects of writing requirement and signature such as identification, attribution and integrity of contents. The second group related to recognition of electronic form of writing, signature and contract. The third group related to application of traditional contract principles in the electronic environment.

2.4.2 United States

A study of the issues from the 1980s to the 1990s indicated that similar national issues relating to electronic commerce arose in common law countries, such as the US, the UK, Australia and Canada. Continued concerns were expressed at the national level regarding these issues. An overview and a brief summary of these issues and developments that transpired in the past are discussed below.

In 1988, the American Bar Association (ABA) made a remark about the electronic data and messages by stating that the electronic messaging systems and also the EDI

were changing the way businesses entered into contracts. In 1987, an Electronic Messaging Services Task Force was formed under the patronage of the ABA to determine how well the existing contract law and contract formation provisions of the Uniform Commercial Code (UCC) accommodated the changes in business practices. In 1988, a study was initiated by the task force to determine what legal concerns existed that might impede a full scale implementation of EDI in commercial contracting, the manner in which businesses attempted to address such concerns, and to identify possible legal solutions.

A report titled ‘The Commercial Use of Electronic Data Interchange’ was released in 1990. The report discusses the legal issues related to the sales contracts under the law of the US. The Uniform Commercial Code (UCC) of the US required a contract for the sale of goods valued $500 or more, to be evidenced in writing and signed by the party against whom it is enforced as follows:

except as otherwise provided in this section a contract for the sale of goods for the price of $500 or more is not enforceable by way of action or defense unless there is some writing sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker.

The UCC defined signature as any symbol executed or adopted by a party with the present intention to authenticate writing. The UCC provided an interpretation of what constituted ‘writing’. Under the UCC, writing includes printing, typewriting or any other intentional reduction to tangible form. The limitation in this definition was intentional and identified that there must be a tangible representation of information that comprised the subject matter of the contract. The requirements of a

---

50 ABA, *Electronic Messaging: A Report of the Ad Hoc Sub-Committee on the Scope of the UCC* 5 (1988), As a result of these changes, the ABA suggested that there was a need to re-examine the fundamental principles of contract.
53 Ibid § 2–201.
54 Ibid § 1–201.
valid and enforceable contract were satisfied by any type of computer storage media that was physical, where a tangible printout of the contents of the media could be generated. The parties intended the media and any printout generated to be a representation of their contractual terms and conditions. However, ‘temporary visual picturisations’ that are represented on the screen of a computer were not specifically included within the UCC’s definition of ‘writing’ and do not take a ‘tangible form’ as was required by the UCC. Hence, it was uncertain whether electronic form would satisfy requirements of the code.\textsuperscript{56} It was also uncertain whether an electronic form of writing could attain immutability of paper-based documents to satisfy the writing requirement.\textsuperscript{57}

The report indicated that the requirement of writing and signature could raise issues as it was uncertain whether an electronic document would qualify as writing and signature as follows:\textsuperscript{58}

the issue is whether the records of EDI communication, which are increasingly relied upon by businesses themselves, are acceptable within the ’signed writing’ concepts of the Uniform Commercial Code and related case law.

The task force suggested that since EDI transactions were being used between limited trading partners with a long-term relationship, none of the uncertainties had resulted in litigation.\textsuperscript{59} However, problems could arise if EDI transactions were used


\textsuperscript{59} UNCITRAL, 23\textsuperscript{rd} sess, [256–69], UN Doc A/51/9/333 (1990), 259.
more widely by businesses in a more open environment. The report also noted that appropriate security procedures were necessary to protect EDI transactions and the application of adequate security procedures could safeguard the integrity of transmission and the reliability of EDI transaction records.

During the 1990s, acceptance of electronic signature, acceptance of writing on computer disk and the use of new technology was being extended to a large number of contracts in the US, as seen in Wikens v Iowa Insurance Commissioner and Cylburn v Allstate Insurance Company. In Wikens v Iowa Insurance Commissioner, it was held that signatures generated on a computer meet the requirement of statute and these are as good as written signatures. In this case, Wikens v Iowa Insurance Commissioner, insurance agents brought an action against an insurer alleging that the insurer failed to comply with s 515.52 of the Iowa Code because the agent, Larry Hertel, countersigned insurance policies by typing his name into the document on the computer. However, the Insurance Commissioner determined that the signatures generated on the computer did meet the requirements of the Iowa Code and the members of the Iowa Court of Appeals agreed. Section 4.1(7) of the Iowa Code, 1989 provided as follows:

the words written and in writing, may include any mode of representing words or letters in general use. A signature, when required by law, must be made by the writing or markings of the person whose signature is required. If a person is unable due to a physical handicap to make a written signature, that person may make substitution in lien of a signature required by law.

While giving the judgment of the court, Sackett J indicated that the sole issue was to prove intent, not the method itself used to affect the signature and stated as follows:

---

60 Ibid.
64 Wikens v Iowa Insurance Commissioner 457 NW 2d 1 (Iowa App 1990).
we find the fact that the signature is computer generated rather than hand signed does not defeat the purpose of the act. The issue is not how the name is placed on a sheet of paper; rather the issue is whether the person whose name is affixed intends to be bound. No one argues that the agent whose name was affixed did not intend to be bound. We find the signature requirements of the statute were met.

Similarly, a notice provided through computer disks was considered equivalent to a written notice in *Cylburn v Allstate Insurance Company*\(^6^8\), in the South Carolina case. In this case, *Cylburn v Allstate Insurance Company*.\(^6^9\) the plaintiff brought legal action against his insurer for breach of contract, when the plaintiff’s house was burnt and he had stopped paying insurance premium about 2 years earlier. The plaintiff alleged that the insurance policy had not been legally cancelled and he had been denied insurance cover. Under §38-75-730(b) of the South Carolina Code, cancellation arises when premiums are not paid and the cancellation is not effective unless the insured is provided with a written notice of cancellation not less than ten days before the proposed effective date of cancellation. The members of the jury determined at the trial that the defendant did not send the notice of cancellation of the policy to the plaintiff after he failed to pay the premium. The jury was also asked to decide if the insurance company had sent a written notice to their insurance agent, indicating that the policy was cancelled. In fact, the insurance company had sent computer disks to its agents to notify them of the changes. The members of the jury concluded that the method of providing written notice was not sufficient.\(^7^0\) However, it was decided at the appeal after a brief indication that other forms of technology, such as videotapes and tape recordings were considered writings. Thus, the computer disk sent by mail to the agent was equally acceptable. While reaching the decision, Blatt SDJ agreed that the form of technology was hardly a problem, which was based upon sound legal principles. Blatt SDJ stated as follows:\(^7^1\)

> the storage of information on tape recordings and videotapes is not that much different from that on floppy diskettes for computers, but rather is more a difference in the devices used to read the information. The information can be

---

69 Ibid.
70 Mason, above n 67, 284–6.
retrieved and printed as hard copy on paper. In today’s paperless society of computer generated information, the court is not prepared, in the absence of some legislative provision or otherwise, to find that a computer floppy diskette would not constitute a writing within the meaning of [S.C.Code 1976] § 38-75-730.

Although attempts were made during the 1990s to draw analogies between electronic signatures and traditional signatures, security of electronic communication and their ease of manipulation was still a concern.\(^{72}\) Hence, concept of authentication, which ensures that only the recipient has sent a particular message was considered to fit well only within the traditional paradigm of paper-based signatures.\(^{73}\) Security of electronic transactions was also a concern.\(^{74}\) Further, some legal commentators were also of the opinion that mailbox rule would face its demise due to the instantaneous nature of EDI and email communication.\(^{75}\) It should be noted that others opposed this view.\(^{76}\)

Due to a number of issues identified above regarding the formation of electronic contracts, electronic writing and electronic signatures, there was an uncertain and unpredictable legal environment, which was considered to be the main barrier to the development of electronic commerce.\(^{77}\) The US Department of commerce expressed...
concerns regarding the lack of predictable and definitive legal framework as follows.\(^7\)

businesses have raised three potential inhibitors to the widespread adoption of internet commerce: the lack of a predictable legal environment, concerns that government will overtax the internet, and uncertainty about the internet’s performance, reliability and security. For businesses to feel comfortable about using the internet in communications with its suppliers and customers, it needs to be sure of the identity of the party at the other end of the transaction and that any agreement made electronically is binding.

Three groups of issues arose in the US, the first group were those related to the evidential aspects of writing requirement and signature such as identification, attribution and integrity of contents. The second group related to recognition of electronic form of writing, signature and contract. The third group related to application of traditional contract principles in the electronic environment such as rules associated with and time and place of contract formation.

2.4.3 United Kingdom

As in the US, uncertainty regarding electronic contracts and signatures existed in the UK during the 1980s.\(^7\) From 1989 through to the late 1990s, various domestic bar associations such as the ABA, trade groups and government entities began to examine the legal issues associated with EDI in other common law countries.\(^8\)

Most contracts were devoid of formalities and could be concluded in writing or orally and completed either electronically or physically. The informal contracts, which included contracts of sale and lease could be concluded safely over the internet. Many contracts were required to be in writing or had some other formal

requirements, such as the attachment of a physical signature or attestation by witnesses in order to be effective. However, these formal requirements caused problems when the principles of electronic contracting were applied. The main issue was the application of the rules in cyberspace, which required the contract to be ‘written’ or ‘in writing’. The other issue was whether a digital document could fulfil the necessary formal requirements of such contracts.\(^{81}\)

When there was a requirement for writing in a contract, then reference was usually made to the \textit{Interpretation Act 1978},\(^{82}\) which defined writing as:\(^{83}\)

\begin{quote}
including typing, printing, lithography, photography and other modes of representing or reproducing words in a visible form.
\end{quote}

The above definition of writing meant that for many formal contracts, electronic contracting could not be used as digital communication. A series of electrical impulses did not have the requisite degree of visibility that was required by the definition under the \textit{Interpretation Act}. The UK aimed to become the ‘world’s best place in which to trade electronically’, but this issue became a major barrier for the development of electronic commerce.\(^{84}\)

Different forms of traditional signatures, such as rubber stamp, telex signature, faxed copy, printed name, handwritten signatures were recognised as valid under various English cases.\(^{85}\) For example, in \textit{Lobb v Stanley},\(^{86}\) Patterson J recognised the importance of affixing the name of a party as a signature and stated that a signature

\begin{thebibliography}{99}
\bibitem{interpretation} \textit{Interpretation Act 1978} (UK).
\bibitem{lobb} \textit{Lobb v Stanley} (1844) 5 QB 574; 114 ER 1366.
\end{thebibliography}
was only a mark, and held that even the printed name of the party who was required
to sign the document was sufficient to be considered a signature. In this case, Lord
Denham CJ, and Patterson, Coleridge and Wrightman JJ argued as to what could be
construed as a signature. In *Lobb v Stanley* Stanley, a certified bankrupt gave a
signed, written promise following bankruptcy. Out of the three undated letters, which
were produced by Stanley, one of the letters read that:

Mr Stanley begs to inform Mr Lobb that he will be glad to give him a
promissory note or bill for the amount of Mr Stanley’s account, payable at three
months, as Mr Stanley has of late been put to heavy expenses, and hopes this
arrangement will be satisfactory to Mr Lobb. 3 Crescent. Thursday morning.

During the trial before Lord Denham CJ and Patterson J, verdict was found for Lobb
and leave was granted to appeal. Whatley, counsel for Stanley submitted that all
previous decisions related to the concept as to what constituted signature were not
correct. Patterson J stated:

it is true that the word ‘signed’ occurs in the statute and, if this had been the
first time that we were called upon to put a construction on that word, and if the
decisions on the Statute of Frauds had not occurred, I should perhaps be slow to
say that this was a signature.

Although Lord Denham CJ agreed that the letters were not signed in one sense, the
intrinsic evidence of the documents proved the signature. Further, Lord Denham CJ
pointed out that:

It is a signature of the party when he authenticates the instrument by writing his
name in the body, Here, it is true the whole name is not written, but only ‘Mr
Stanley’. I think more is not necessary.

At the same time, Coleridge J reinforced the significance of the mechanism by which
the document was authenticated when he pointed out that:

---

87 Ibid.
88 Ibid.
89 Ibid.
90 Mason, above n 67, 49.
91 *Lobb v Stanley* (1844) 5 QB 582.
92 Ibid 582, 581.
93 Ibid 582, 582.
Is it not enough if a party, at the beginning of a document, writes his name so as to govern what follows? Does he not then use his name as a signature?

Finally, it was unanimously agreed that Stanley signed the documents, Stanley wrote the letters himself and he identified himself by surname in the body of the letters. By identifying himself in this manner, Stanley demonstrated that he intended the recipient to rely on the promise contained in the letter. Thus, the signature was his assertion because he wrote his surname and he intended that the content of the letters were to be acted upon by the recipient.94

Although in traditional cases, different types of signatures were considered valid, attribution of the message to a particular sender was considered a matter of concern as there was no clear authority dealing with the issue. Hence, requirement of signature was also considered problematic.95 A signature is a process. If that process produces sufficient evidence indicating that a person has adopted a document as his own and if that document appears to be the same document to which the process is applied, then the document can be considered signed. It is not relevant whether the result of that process is a visible mark or a symbol. So in one way, it can be said that a signature is actually evidence.96 Unlike traditional signatures, which can be attributed to a person, electronic signatures cannot create evidence, as they can be easily tampered with and suffer from limitations.

During the 1990s, the Select Committee on Trade & Industry, Seventh Report of UK stated that there were many requirements in law for ‘documents’, ‘records’ or ‘instruments to be in ‘writing’ and often ‘signed’. The report also identified that the definitions of such words in statute and case law would not encompass digital forms of information as well as more traditional forms of ‘documents’, ‘writing’, and ‘signatures’. It also noted that it would have the effect of preventing some

94 Mason, above n 67, 49–50.
commercial transactions or dealings with government being conducted electronically or place such transactions beyond the scope of some laws.\textsuperscript{97}

Further, the Select Committee on Trade & Industry, Seventh Report identified that the government had stated that:\textsuperscript{98}

\begin{quote}
At present, there are circumstances where there is doubt about whether a requirement in law for a signature can be met legally using an electronic signature’ and that, ‘the position on requirements for information to be ‘written’ or ‘in writing’ is clearer – such a requirement cannot at present, be met using electronic means.
\end{quote}

These ‘uncertainties and limitations’ were regarded as important barriers to the development of electronic commerce and electronic governments, which had to be dealt with both at national and international levels.\textsuperscript{99}

Thus, three groups of issues arose in the UK, the first group were those related to the evidential aspects of writing requirement and signature such as identification, attribution and integrity of contents. The second group related to recognition of electronic form of writing, signature and contract. The third group related to application of traditional contract principles in the electronic environment such as rules associated with and time and place of contract formation.

2.4.4 Australia

Traditional contractual principles are displaced and inadequate in an electronic environment as discussed in the previous chapter. Traditional contractual principles evolved out of commercial practices when contracts were formed through the exchanging of letters or by offline communication. Traditional contract principles assume that most contracts will take the form of written offer, which will be communicated to the party who accepts the terms, rejects the terms or makes a

\begin{flushright}
\textsuperscript{98} Ibid.
\textsuperscript{99} Ibid.
\end{flushright}
counter offer. Hence, some legal commentators were of the opinion that the lack of specific rules relating to electronic contracts could create uncertainty regarding the application of traditional principles to electronic contracts and these changes required re-examination of fundamental contract principles.\textsuperscript{100} Further, there was also a debatable issue as to whether it is appropriate to regard email and EDI messages as instantaneous communication like telex to exclude the application of postal acceptance rule. Email and EDI could not be easily differentiated as instantaneous or non-instantaneous messages. It was argued that if email or EDI were like telex then the acceptance must be actually be received by the offeror.\textsuperscript{101}

When a contract is formed electronically, there is no requirement that the contract must be in writing. Even under the general law of contract there is no requirement for traditional, conventional or paper-based contracts to be in writing and the same rule applies to electronic contracts.\textsuperscript{102} However, in Australia, the Statute of Frauds and the equivalent legislations require certain contracts to be in writing and signed by the parties, similar to the other common law countries, such as the UK, the US and Canada.\textsuperscript{103} Requirements for written contract are found in Australian legislation such as: the \textit{Imperial Acts (Substituted Provisions) Act} 1986 (ACT); the \textit{Conveyancing Act} 1919 (NSW), s 54A; s 62 of the \textit{Law of Property Act} 2000; s 26(1) of the \textit{Law of Property Act} 1936 (SA); s136 of the \textit{Instruments Act} 1958 (Vic); s 9 of the \textit{Conveyancing Law of Property Act} 1884 (Tas) and s 4 of the \textit{Statute of Frauds} 1677 (Imp) (WA).\textsuperscript{104}

---


Writing is defined in interpretation statutes in Australia’s various states and territories. Section 36 of the *Acts Interpretation Act* 1954 (Qld) defines writing as including ‘any mode of representing or reproducing words in a visible form’. Section 21 of the *Interpretation Act* (NSW) defines writing as follows:

writing includes printing, photography, photocopying, lithography, typewriting

and any other mode of representing or reproducing words in visible form.

Similar definitions are provided under s 5 of the *Interpretation Act* 1984 (WA), s 4 of the *Acts Interpretation Act* 1915 (SA) and s 24(b) of the *Acts Interpretation Act* 1931 (Tas).

When a document exists in an electronic environment without taking a physical form, the issue is whether such an document could be considered a contract in writing as required under the Statute of Frauds. In reality, the electronic document is a series of numbers stored in the memory of the computer. The content of such an electronic document seen on the computer screen is a translation of the numbers by the computer after the application of coding convention and this ultimately appears as a form of words to the reader on the computer screen. These are understandable to a person only after appropriate coding convention translates these numbers into

---


105 Christensen, above n 104.

106 Section 5 of the *Interpretation Act* 1984 (WA) defines writing as follows: ‘Writing and expressions referring to writing include printing, photography, photocopying, lithography, typewriting and any other modes of representing or reproducing words invisible form’. According to Section 4 of the *Acts Interpretation Act* 1915 (SA), ‘writing includes any visible form in which words may be reproduced or represented’. According to Section 24(b) of the *Acts Interpretation Act* 1931 (Tas), ‘expressions referring to writing shall be construed as including references to any mode of representing or reproducing words, figures, or symbols in a visible form’.

107 Section 5 of the *Interpretation Act* 1984 (WA) defines writing as follows: ‘Writing and expressions referring to writing include printing, photography, photocopying, lithography, typewriting and any other modes of representing or reproducing words invisible form’.

108 Section 4 of the *Acts Interpretation Act* 1915 (SA) defines writing as including ‘any visible form in which words may be reproduced or represented’.

109 Section 24(b) of the *Acts Interpretation Act* 1931 (Tas) defines writing to include ‘references to any mode of representing or reproducing words, figures, or symbols in a visible form’.

110 Rees, above n 101, 9–17.
words. Therefore, an electronic contract by nature has a dual form. There are a series of stored numbers and code and the contract takes visible form as a translation of the numeric code when it is transmitted to a computer screen. It is this dual nature of the electronic contract that has led to the uncertainty as to whether an it can be regarded as a contract in writing.\textsuperscript{111}

The physical form of traditional or paper-based contracts satisfies the purpose of written contracts. The issue is whether an electronic contract that may never take a physical form but can be retained by the parties satisfies the purpose of a written contract. The term ‘in writing’ poses difficulties for electronic contracts if it is determined that it implies not only words but a physical form. The requirement of writing is satisfied and accepted by courts when a contract between the parties is reduced to a tangible form that can be considered a record of the formation of a contract and may be relied on as an evidence of bargain between the parties for a future reference. For many centuries, most parties have reduced a contract into a tangible form by creating a physical contract or some printed version of the contract on paper.\textsuperscript{112} Further, writing is defined under the interpretation statues of Australia as any mode of representing or reproduction of word in the visible form.\textsuperscript{113} The traditional definition of writing is sufficiently broad to be argued that both tangible and intangible documents may come within its scope. Since the emphasis of the Interpretation Acts in each jurisdiction is on visibility,\textsuperscript{114} it was uncertain whether an electronic document, which is a series of numbers stored in the computer’s memory,

\textsuperscript{111} C Reed, Digital Information Law: Electronic Documents And Requirements of Form (1996); Christensen, above n 104.
\textsuperscript{112} Christensen, above n 104.
\textsuperscript{113} Interpretation Act 1901 (Cth); Interpretation of Legislation Act 1984 (Vic); Interpretation Act 1984 (WA) s 5; Interpretation Act 1978 (NT) s 26; Acts Interpretation Act 1915 (SA); Interpretation Act 1931 (Tas).
\textsuperscript{114} Under Section 38 of the Interpretation of Legislation Act 1984 (Vic), writing includes all modes of representation or reproduction of words, figures or symbols in a visible form, as well as expressions referring to writing. Under Section 25 of the Interpretation Act 1901 (Cth), writing encompasses any mode of representing or reproducing words, figures, drawing or symbols in a visible form. In the Interpretation Act 1984 (WA) s 24(b), ‘expressions referring to writing shall be construed as including references to any mode of representing or reproducing words, figures, or symbols in a visible form’. Similarly, Section 4 of the Interpretation Act 1915 (SA) and Section 26 of the Interpretation Act 1978 (NT) emphasises visibility.
would qualify as writing. There was considerable doubt regarding the broad interpretation of the term ‘writing’.

The legal problem facing EDI users was that legislation such as the Statute of Frauds and the standard commercial practice required contracts for the sale of goods to be in writing and signed. The reason for the requirement of a signature or writing was to satisfy the court that the contents of the contract or document were unchanged and the information originated from its purported source. Further, the physical properties of the paper, ink marks and style of writing could be used by a forensic expert to determine the authenticity of a document. In addition, any attempt to alter the document was likely to be detected. An unsigned computer message could be tampered with and changed without a trace. In order to achieve predictability and legal certainty, it was necessary to establish that writing in an electronic form is protected to the same extent as that of a paper-based form.

Issues related to electronic signatures arose as it was uncertain whether an electronic signature would be regarded as a valid signature under contract. The law available to resolve the issue was based on legal concepts developed before the advent of electronic commerce. The issue of the validity of electronic signatures could only be assessed based on traditional legal concepts. The meaning of signatures in Australia was established as early as 1884 in *R v Moore: Ex Parte Myers* dealt with a pawnbroker's pledge ticket that was not signed by the pawnbroker in accordance with the relevant legislation but was signed by an authorised agent, even though the name of the pawnbroker was printed on the ticket. In this case, Myers was a licensed pawnbroker and manager of the Mont de Piete Company carrying on business of pawn broking in various branches licensed for the business. Under S 21

---

117 Cunliffe, above n 100; Cunliffe and McLachlan, above n 100; Clark, above n 22, 31.
120 *R v Moore: Ex parte Myers* (1884) 10 VLR 322.
121 *R v Moore: Ex parte Myers* (1884) 10 VLR 322.
of the *Pawnbrokers Statute 1865*, pledge-tickets were to be signed with the signature of the pawnbroker. Pledge-tickets were given to customers and each manager was authorised to sign the ticket under the printed words, ‘Lewis M Myers, per’.

On an appeal from being convicted by the justices at South Melbourne for not signing the tickets, Higginbotham J held that a ‘signature is only a mark’ and may ‘be impressed upon the document by a stamp engraved with a facsimile of the ordinary signature of the person signing’. He also held for the court that a statute is satisfied by proof of the making of a mark upon the document by or by the authority of the signatory.

Further, on the importance of a signature, Higginbotham J stated:

"It was observed by Patterson J in *Lobb v Stanley*, that the object if all Statutes which require a particular document to be signed by a particular person is to authenticate the genuineness of the document. A signature is only a mark, and where the Statute merely requires a document shall be signed, the Statute is satisfied by proof of the making of the mark upon the document by or by the authority of the signatory…In like manner, where the Statute does not require that the signature shall be an autograph, the printed name of the party who is required to sign the document is enough… or the signature may be impressed upon the document by a stamp engraved with a facsimile of the ordinary signature of the person signing…But proof in these cases must be given that the name printed on the stamp was affixed by the person signing, or that such signature has been recognised and brought home to him as having been done by his authority so as to appropriate it to the particular instrument."

*R v Moore* establishes three important aspects of signature. Firstly, it identifies recognition by the Australian judiciary that a person’s signature, in order to bind them to the contents of the document, does not require the physical act of the person putting pen to paper. It can be achieved via an agent or through the use of some mechanical means, such as an impress stamp bearing a facsimile of the person’s

---

122 Ibid VLR 324.
123 Ibid.
124 Ibid.
signature. A printed name was considered as valid signature in Clohesy v Maher. While in Electronic Rentals Pty Ltd v Anderson High Court held that when a document was required by statute to be made under a man’s hand or to be signed by him, then what was ordinarily meant was that he must personally sign the document with his name or his mark by a pen or by a stamp.

In Australia, the function of a traditional signature is met by any method and the ordinary meaning of signature is nothing but a mark in a written document. Signatures are important in a document and traditional signatures are not only important in a paper-based document but they are also used for evidential purpose in a contract. There are four historical policy objectives for the requirements of writing and signatures, which include evidentiary, cautionary, channelling and record keeping. Though these functions are not discreet, they are intimately connected. The requirement of signature has a protective effect, since it cautions the signatory. Further, the need for a signature can also warn the signer or signatory that the document has legal consequences and encourage the signatory to think whether he or she wants to be legally bound by affixing the signature. This function is considered an important issue in protecting the consumers. The requirements of writing and signatures are generally considered formalities but they also create durable records of the parties in a contract and identify the terms of the agreement. Signatures serve the function of channelling by clarifying the line between intent to act in a legal manner and the intent to act otherwise. Parties to a

126 See Denning L J in Lazarus Estates Ltd v Beasley (1956) 1 All ER 341 regarding company stamp and signatures.
127 Clohesy v Maher (1880) 6 VLR 357.
128 Electronic Rentals Pty Ltd v Anderson (1971) 124 CLR 27, 42.
129 S Christensen, W Duncan and R Low, ‘Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements Be Fulfilled Electronically?—A Case for Reform Based upon the Electronic Transactions (Queensland) Act 2001’ (December 2002) Centre for Commercial and Property Law, Queensland University of Technology 1, 37.
130 A signature performs a number of functions. These include the identification of the signatory, the provision of certainty regarding the personal involvement of a person in the act of signature, the association of a person with the content of the contract or document, the attestation of the intention of a person to be bound by the document or contract as well as the attestation of the authorship of the signatory regarding the document or contract. McCullagh, Little and Caelli, above n 125, 455–456.
133 Sneddon, above n 131, 334, 348.
134 Ibid.
contract are forced to use a particular form and similar agreements must use similar forms. The channelling also effects the decision as to whether a document is legally binding by reducing the need to produce evidence in the case. Thus, channelling is related to evidentiary function.\(^\text{135}\)

Affixing a signature is a formality, yet it serves the evidentiary purpose by ensuring the availability of admissible and reliable evidence. These characteristics help in preventing perjury or fraud. Signatures can perform evidentiary functions as follows.\(^\text{136}\)

\(\text{a. signature identifies the signer by name;}\)
\(\text{b. signature identifies a particular characteristic or attribute or status of the signer, rather than the name of the person;}\)
\(\text{c. signature provides evidence that the signatory has agreed to be bound by the record either by adopting or approving; and}\)
\(\text{d. Signature provides evidence that the signatory has acknowledged or witnessed or verified the record and not necessarily agreed to be bound by the contents of the document.}\)

It was argued by some commentators that electronic signatures cannot fulfil all of the functions of a traditional signature.\(^\text{137}\) It was also perceived that the absence of paper as the principle medium of communication in an electronic environment would lead to a loss of traditional safeguards when paper was removed as a medium of commercial activities.\(^\text{138}\) The Statute of Frauds and the standard business practices require contracts involving sale of goods to be in writing and signed by the parties. This practice is to ensure that the contents of the contract remain unchanged and forensic experts are able to detect any alterations made on the paper by looking into the ink marks and handwriting of the parties. It was argued that an electronic contract does not permit such detection, as a computer message may be unsigned and may be


\(^{136}\) Carter, above n 135; Sneddon, above n 131, 334, 348 339.

\(^{137}\) Sneddon, above n 131, 348; McCullagh, Little and Caelli, above n 125, 455–459.

tampered without any detection.\textsuperscript{139} The increased risk of fraud was perceived as a hurdle.\textsuperscript{140}

Thus, three groups of issues arose in Australia, the first group were those related to the evidential aspects of writing requirement and signature such as identification, attribution and integrity of contents. The second group related to recognition of electronic form of writing, signature and contract. The third group related to application of traditional contract principles in the electronic environment such as rules associated with and time and place of contract formation.

2.4.5 Canada

As in other countries, concerns regarding the lack of appropriate legal framework for EDI transactions were also expressed in Canada.\textsuperscript{141} In 1993, the Uniform Law Conference of Canada realised the need of appropriate legal framework to accommodate EDI transactions. Traditional legal rules were considered inadequate.\textsuperscript{142} During the proceedings of the Seventy Fifth Annual Meeting of Uniform Law Conference in 1993 issues were summarised as follows:\textsuperscript{143}

EDI has its impact because electronic data replace paper for keeping of records and for carrying out transactions. A host of legal rules require records to be kept in physical form and transactions to be documented in writing. In addition, electronic data can be transferred, recombined or simply examined much more easily than paper data. As a result, problems of authentication and security take on new aspects.

To sum up, three main groupings of issues were a matter of concern for businesses, traders and legal commentators. The first group were those related to the evidential aspects of writing requirement and signature, such as identification, attribution and integrity of contents the second group related to recognition of electronic form of

\textsuperscript{139} Clark, above n 22, 29–31.
\textsuperscript{141} Crawford, above n 35, 66, 72; B D Grayton, ‘Canadian Legal Issues Arising from Electronic Data Interchange’ (1993) 27 \textit{UBC Law Review} 257, 258–90; Brooks, above n 32.
\textsuperscript{143} Ibid.
writing, signature and contract. The third group related to the application of traditional contract principles in the electronic environment. Thus, from the analysis of traditional laws these three main groups of issues emerge. The next section looks at the attempts that were made to regulate these issues.

2.5 EDI Trading Partner Agreements and International Responses

In the absence of clear rules governing EDI transactions, interchange agreements were formulated by traders. Interchange agreements are contractual agreements. These agreements addressed a number of legal and technical issues associated with the use of EDIs. The agreement detailed the individual roles and legal responsibilities of the trading partners for transmitting, receiving and storing electronic messages. Various national trade facilitation bodies, bar associations and regional organisation prepared model interchange agreements.

The first international attempt to harmonise EDI transactions was the preparation of UNCID in 1987. UNCID was prepared by a special joint committee of the ICC in which various organisations, such as the UN Economic Commission for Europe (ECE), UNCAD, the OECD, the Organization for Data Exchange by Tele Transmission in Europe (ODETTE) and UNCITRAL were represented. The UNCID developed a code of conduct, which the parties would choose to apply to their EDI relationship. The UICID rules were in the form of non-mandatory rules, which EDI users and suppliers of network services could incorporate into their communications agreement.

146 Ibid 9.
147 Ibid 10.
148 Ibid.
Provisions of the code required parties to ensure transfer and the capability to receive, correct and complete EDI messages.\textsuperscript{150} The main provisions of the rules were duty of care when sending, transmitting and receiving EDI messages, in order to guarantee integrity, appropriate control of the identity of the parties involved in the transaction, notification upon request of the receipt of a document, protection of sensitive information, requirement to maintain records of the transaction to be used as evidence in courts and interchange standards.\textsuperscript{151}

After the publication of the UNCID rules, various model interchange agreements were published between 1990 and 1996. In order to resolve uncertainties associated with EDI transactions, different countries began to develop their own individual model EDI agreements. The ABA developed the model EDI trading partner agreement (ABA model agreement), The EDI Council of Canada introduced the Canada model EDI trading partner agreement, and the EDI Associations of the UK developed the UK Interchange Agreement. The TEDIS programmed produced a European model EDI agreement (TEDIS European Agreement) reflecting the best practice in the EDI community. It was prepared by the Commission of European communities. Similarly, the EDI Council of Australia released a model EDI trading partner agreement, The Model Agreement on Transfer of Data in international trade (FINPRO/CMEA Agreement) was prepared by the republic of Finland and CMEA member states. The European Model EDI Agreement was prepared in 1994 by the Commission of the European Communities and the New Zealand Electronic Data Interchange Association developed the NZ Standard Agreement.\textsuperscript{152}

The EDI agreements addressed technical aspects, such as the format in which the data must be sent and the way in which appropriate computer systems must be

\textsuperscript{151} A Mitrakas, \textit{Open EDI and Law in Europe} (1997) 170; Boss, above n 48.
maintained.\textsuperscript{153} For example, the TEDIS agreement required transmission of EDI messages according to the UN/EDIFACT standards. The ABA agreement required parties to specify the chosen version.\textsuperscript{154}

In order to ensure the reliability of EDI transactions, model agreements required the trading parties to preserve and maintain the records of all EDI messages transmitted between the parties and also required parties to preserve the transaction logs and trade data logs, which could assure the reliability of the transaction.\textsuperscript{155}

Errors or failure can arise while sending or receiving a message in an electronic environment. Hence, some agreements such as the ABA model agreement and Canadian model agreement required the recipient of the data to notify the sender that the message received was accurate. The UK Interchange Agreement imposed obligations on the sender to ensure that the data transmitted was accurate\textsuperscript{156}

Model agreements also indicated that the appropriate level of security must be implemented and maintained when information is sent electronically. Most agreements stated that the parties must use sufficiently reliable procedures to protect unauthorised transmissions and access. Some agreements such as the ABA model interchange agreement, NZ Standard Agreement and Canadian agreement specifically allowed the parties to agree upon what security would be reasonable. The UK and FINPRO agreements required a code and crypto key to be used as a security device.\textsuperscript{157}

\textsuperscript{153} Boss, above n 149, 45–6.
\textsuperscript{154} ABA, \textit{Electronic Messaging: A Report of the Ad Hoc Sub-Committee on the Scope of the UCC 5} (1988); UNCTAD, above n 1; Boss, above n 149, 46.
\textsuperscript{155} Canada Interchange Agreement Article 7.04; NZ Interchange Agreement Article 7, TEDIS European Agreement Article 8; UK Interchange Agreement Article 7; FINPRO Model Agreement Article 6; \textit{Legal Issues of Electronic Data Interchange: Report of the Secretary-General, UNCITRAL}, [392], UN Doc A/CN.9/350 (1991); Boss, above n 149, 50.
\textsuperscript{157} Boss, above n 149, 54.
Model agreements also defined electronic transmission in terms of writing and signature.\(^{158}\) For example, Article 6.04 of the Canada Interchange Agreement indicated that electronic transmission can constitute writing and signature as follows:\(^{159}\)

the parties agree that as between then each document that is received by the receiver shall be deemed to constitute a memorandum in writing signed and delivered by or on behalf of the sender thereof for the purposes of any statute or rule of law that requires a contract to be evidenced by written memorandum or be in writing, or requires any such written memorandum to be signed and/or delivered.

Similarly, Article 3.3.2 of the ABA Model Agreement stated that electronic form can satisfy the legal requirements of writing and signature follows:\(^{160}\)

any document properly transmitted pursuant to this agreement shall be considered….to be a ‘writing’ or ‘in writing’, and any such document when containing, or to which there is affixed, a signature ('signature documents’) shall be deemed for all purposes (a) to have been ‘signed’ and (b) to constitute an ‘original’ when printed from electronic files or records established and maintained in the normal course of business.

The model agreement of Australia made several references to paper-based documents:\(^{161}\)

3.3 Any message received pursuant to this Agreement containing, or to which is affixed, a Signature [the signature can be electronically embedded in the message] and of which the receipt has been confirmed shall be deemed for all purposes;
(1) to be ‘written’ or ‘in writing’
(2) to have been ‘signed’; and


\(^{159}\) *Model Electronic Data Interchange Trading Partner Agreement and Commentary*, EDI Council of Canada (1990).


(3) to constitute an ‘original’ when printed form electronic file or records
established and maintained in the normal course of business.

Although the model agreements did not specifically deal with contract formation
issues, the TEDIS European Agreement specified exactly when a message will be
deemed as received by the other party. Article 10.2 of the TEDIS European
Agreement stated: 162

as far as the formation of a contract is concerned, a contract by EDI is deemed
to be concluded at the time and place where the EDI message constituting the
acceptance of an offer is made available to the information system of the
recipient (reception rule).

Article 3.1 of the European model EDI agreement required the parties to waive their
right to contest the validity or enforceability of EDI messages as follows: 163

The parties, intending to be legally bound by the Agreement, expressly waive
any rights to contest the validity of a contract effected by the use of EDI in
accordance with the terms and conditions of the Agreement on the sole ground
that it was effected by EDI.

During the early 1990s, various EDI committees were formed in Asia to promote the
use of EDI transactions. The Japan EDIFACT Committee and the Singapore EDI
Committee were formed in 1990. The Korea EDIFACT Committee, the Taiwan
Taipei EDIFACT Committee and the China EDIFACT Committee were formed in
1991. The Malaysia EDIFACT Committee and the India Ministry of Commerce were
formed in 1992. The Thailand EDI Council and the Philippines EDIFACT
Committee were formed in 1994. 164

2.5.1 Need of Legal Rules

164 UNECE, Electronic Data Interchange—A Management Overview (Electronic Commerce
Initiatives) submitted by Economic and Social Commission for Asia and the Pacific (1996)
The interchange agreements were merely agreements that were formed between private transacting parties and did not change the mandatory legal rules.\textsuperscript{165} Electronic commerce expanded from a limited range of business-to-business transactions between parties in existing or ongoing relationships, to a broad range of different activities. The electronic commerce activities, which were limited to business-to-business transactions on a closed proprietary network, gradually expanded into a complex web of commercial activities that were transacted on a global scale. These transactions were being conducted between increasing numbers of participants, including companies and individuals both known and unknown, on global open networks, such as the internet.\textsuperscript{166} EDI transactions were conducted over a closed network together with standard format documents.\textsuperscript{167} Hence an international and generalised effort for law reform was required to facilitate global electronic commerce.

2.6 UNCITRAL and Development of International Norms

The international community realised the need to facilitate electronic commerce and to resolve legal issues and concerns that arose from the commercial use of electric technologies. The rapid expansion of EDI in particular created considerable momentum for addressing the legal issues.\textsuperscript{168} As early as 1985, UNCITRAL examined the impact of national legal systems on the increasing use of electronic communication in international trade. Initially, the focus of UNCITRAL was on EDI. However, the use of electronic commerce was gaining momentum and the commercial use of the internet began.\textsuperscript{169} Until a very late stage in its preparation, the title of the draft model law was referred to as ‘Legal Aspects of the Electronic Data Interchange and Related Means of Communication’. However, use of the term

\begin{thebibliography}{99}
\bibitem{boss} Boss, above n 149, 66.
\bibitem{ritter} Ritter, above n 34.
\end{thebibliography}
‘electronic commerce’ was considered the most appropriate way to describe the broad range of communication techniques covered by the model law. 170

2.6.1 UNCTRAL: Functions and Methods of Work

International commerce may be hindered by several factors such as the lack of a predictable legal environment or outdated laws, which are unsuitable for commercial transactions. UNCTRAL identifies issues that arise in international trade and then provides solutions that are acceptable to states having different legal systems. 171

2.6.1.1 Composition, Functions and Methods of Work

UNCTRAL consists of 60 member states. It was initially composed of 29 states, it expanded to 36 in 1973 and was further extended to 60 in 2004. The members are elected for a term of six years and the term of half of the members expires once every three years. 172 The members represent various geographic regions of the world as well as principal economic and legal systems. 173 There are five regional groups represented, which include African states, Eastern European and Asian states, Latin American and Caribbean states, Western European states, and other states. 174

In 1966, the UN General Assembly established UNCTRAL, with the mandate to further the progressive harmonisation of the international trade law by coordinating the work of organisations active in the field. 175 Harmonisation is the process through which domestic laws are modified to enhance predictability in cross-border commercial transactions. Unification implies the adoption of a common legal standard by states governing certain aspects of international business transactions. A model law is the example of a text that is drafted to harmonise domestic law. It is a

172 Ibid.
173 Ibid.
174 Ibid.
suggestive pattern created for law makers of national governments to consider adopting as part of their domestic legislation.\textsuperscript{176}

UNCITRAL carries out its work at annual sessions held alternatively at the UN Headquarters in New York and at the Vienna International Centre on alternate years. It establishes working groups to perform the preparatory work on the topics, which are included in its program of work. In addition to the member states, non-member states and other interested organisations are also invited to attend sessions.\textsuperscript{177} UNCITRAL takes decisions by consensus instead of voting in order to address all the concerns raised so that the final text is acceptable to all.\textsuperscript{178}


2.6.2 History and Background of Model Law on Electronic Commerce

The UNCITRAL Model Law on Electronic Commerce was prepared in response to the major changes brought about by the use of computerised and other modern techniques of doing business and was adopted by UNCITRAL in 1996 to promote the harmonisation and unification of international trade law. The model law attempts to remove obstacles to international trade caused by the inadequacies and

\textsuperscript{177} Ibid.
\textsuperscript{178} Ibid.
\textsuperscript{179} Ibid.
\textsuperscript{180} Ibid.
divergences in the laws affecting trade. Changes brought about by the electronic commerce challenged the traditional regulatory structures. Work on model law was undertaken in recognition of the fact that in most situations national legislations did not contemplate electronic commerce. It was also recognised that the national legislations restrict the use of electronic commerce by including requirements that do not easily translate traditional concepts such as writing, signature or original into an electronic environment.\textsuperscript{181}

In 1984, UNCITRAL received a report from the Secretary General entitled Legal Aspects of Automatic Data Processing. The report identified several legal issues associated with the legal value of computer records, such as the requirement of writing, authentication and liability for errors.\textsuperscript{182} UNCITRAL also considered the report of the trade facilitation group and decided to place the subject of legal implications of automatic data process on its priority list.\textsuperscript{183} In 1985, UNCITRAL recommended that the member governments review their legal rules affecting the use of computer records as evidence and traditional legal obstacles that were arising due to writing and signature requirements.\textsuperscript{184}

In 1988, UNCITRAL noted that there was no refined legal structure for the rapidly growing field of electronic contracts. UNCITRAL decided to conduct a preliminary study on the principles of electronic contracts. In 1990, the report entitled ‘Preliminary study of legal issues related to the formation of contracts by electronic means’ was released. It found that most national laws included provisions that required certain transactions to be in writing or evidenced in writing. The requirement of these being in writing was made for a number of reasons. If it was required as a condition of validity of contracts, then failure to comply with the requirement rendered the transaction null and void.\textsuperscript{185}

\begin{flushleft}
\textsuperscript{183} UNCTAD, Electronic Commerce: Legal Considerations, UN Doc UNCTAD/SDTE/BFB/1 (1998).
\textsuperscript{185} Ibid.
\end{flushleft}
UNCITRAL noted that the national laws often refer to ‘Writing’ or ‘Document’ without providing a definition of the terms. In such a case, it was assumed that a written paper-based document was required by the drafters as that was the only form available during that time. Legislators generally expected writing to be on a piece of paper or some tangible physical modicum that could permit the words to be read directly.\(^{186}\) It further noted that while the rule relating to admissibility of evidence were flexible in certain jurisdictions, there were legal systems that had a strict approach to the admissibility of electronic messages and excluded electronic messages as acceptable evidence.\(^{187}\)

It also dealt with other issues that had been identified as arising in the formation of contracts by electronic means and noted the model EDI communication agreements had been formed to overcome these problems.\(^{188}\) Further, the report summarised the work that had been undertaken in the European Communities and in the US on the requirements of writing, this included the review of the report of the ABA on electronic messaging and work undertaken by TEDIS project. UNCITRAL decided to prepare a report regarding the model EDI agreements that were being made in different countries in order to determine whether a worldwide model agreement was needed.\(^{189}\)

In 1991, UNCITRAL examined the report entitled ‘Electronic Data Interchange’.\(^{190}\) It described the activities of different organisations dealing with the legal issues of EDI. It analysed the contents of the standard agreements developed by different countries and noted that those agreements varied significantly as per the needs of different category of users. It argued that disparity of contractual agreements was hindering the development of satisfactory framework for the business use of electronic commerce. It was realised that the existing contractual framework used for EDI was inappropriate for international trade as those rules were based upon the

---

187 Ibid.
189 Ibid.
190 Ibid.
structures of local laws. The report suggested that there was need for a general framework that could identify the issues and provide basic legal rules governing EDI communication.

At the twenty-fourth session, the Working Group recommended that UNCITRAL establish uniform legal rules on electronic commerce. It was agreed that the goals of such rules should be to facilitate the use of electronic commerce. In 1992, UNCITRAL endorsed the recommendations contained in the report of the working group and entrusted the preparation of legal rules on electronic commerce. The working group on international payments was renamed the working group on EDI. The group prepared legal rules applicable to EDI and other related modern means of communications from twenty fifth to twenty eight sessions. The text of the Draft model law was sent to governments and international organisations for comments. At the twenty-ninth session in 1996, the Model Law on Electronic Commerce was adopted.

The Model Law on Electronic Commerce was adopted by UNCITRAL on 12 June 1996 after its 605th meeting, which was in turn adopted by the General Assembly under Resolution 51/162 at its 85th Plenary Meeting held on 16 December 1996. It also includes an additional Article 5 bis as adopted by the Commission at its 31st Meeting held in June 1998. UNCITRAL adopted the Model Law on Electronic Signatures on 5 July 2001 at its 727th Meeting. The Introduction to the Model Law, Part A, paragraph 1-6 sets out its objectives in the accompanying Guide as follows:

(a) To provide a set of rules acceptable to the international community relating to electronic communications.

191 Ibid.
192 Ibid.
193 Ibid.
195 Ibid.
(b) To illustrate how obstacles to electronic commerce can be removed by national legislators, such as rules relating the use of ‘written’, ‘signed’ or ‘original’ documents and to help create legal certainty in the electronic environment.

(c) To help remedy any disadvantages because inadequate legislation creates obstacles to international trade.

(d) To act as a tool for interpreting existing international conventions and other instruments that may create legal obstacles when using electronic commerce.

(e) To foster efficiency in international trade.

The model law is based upon the recognition that most legal requirements in electronic commerce and electronic signatures are based upon the recognition of paper-based documents. In order to address the differences between paper-based documents and electronic data, new rules and approach has been established. The new approach is called as the ‘functional equivalent approach’, which is based upon the analysis of the purposes and functions of paper-based documents. The functions of paper or paper-based documents are provided in the Introduction to the model law, Part B, paragraph 16 and include the following:

(a) Document is legible to all;
(b) Document remains unaltered over time;
(c) Allows for the reproduction of the document so that any party may hold a copy of the document;
(d) Allows for authentication of data by means of a signature and
(e) Document remains in a form that is acceptable to the public authorities as well as the courts.

Article 1 of the model law states that it applicable to any type of data message used for conducting commercial transactions. Under Article 2(a) of the model law, the term ‘data message’ is defined as:

Data message’ means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telexcopy;

In the model law, Chapter I, Part One deals with electronic commerce in general and Chapter II deals with the legal requirements regarding data messages. Article 5 of the model law deals with the legal recognition of data messages and states as follows: 202

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 5 bis: Incorporation by reference (as adopted by the United Nations Commission on International Trade Law in June 1998 at its thirty-first session)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

From the above provisions of Article 5, it is clear that electronic data should not be treated any different from that of paper documents because of its electronic form. Further, Article 5 bis provides guidance while referring to other documents in the text of another document as seen frequently in paper-based documents and the aim is to ensure that the paper-based documents are effective in electronic environment also. Hence, the commentary in Paragraph 46-2 to the Guide to Enactment identifies the advantage of the ability to have links to databases, code lists or glossaries. In addition, the Guide to Enactment, Paragraph 46-5 refers to the use of embedded uniform resource locators that direct a reader to referenced document through hypertext link, thereby facilitating reference to related documents. An example of this reference may be seen when an individual or legal entity uses a particular identity certificate provided by the certification authority. This certificate is a signed structured message that proves the existence of an association between a particular set of data that identifies a key holder with a particular key. 203 The certificate authority may incorporate terms and conditions in these individual identity certificates to limit their liability. It is important to note that there are different

classes of certificates and it is not clear as to how the certification authorities distinguish between different types of certificates.\textsuperscript{204}

The purpose of the model law was not only to facilitate electronic communications but also to serve as a reference aid for interpreting existing international conventions in order to avoid impediments to electronic commerce. Under Article 1, the law ‘applies to any kind of information in the form of data message used in the context of commercial activities’ and it also allows for exceptions that can be made by individual countries.\textsuperscript{205}

Article 9 of the model law facilitates admissibility of electronic documents as evidence.\textsuperscript{206} Article 9 indicates it as follows:\textsuperscript{207}

\begin{enumerate}
  \item In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:
    \begin{enumerate}
      \item on the sole ground that it is a data message; or,
      \item if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
    \end{enumerate}
\end{enumerate}

Under Article 11, the model law recognises contracts formed in an electronic medium.\textsuperscript{208} Article 11 states:\textsuperscript{209}

\begin{quote}
In the context of contract formation, 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, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.
\end{quote}


\textsuperscript{206} Overby, above n 204, 223–224.


\textsuperscript{208} Diedrich, above n 200.

Article 11 of the Model Law on Electronic Commerce only states that an offer, an acceptance and contract can be made electronically. By stating this it only recognises offers, acceptances and contract made in an electronic form. It does not deal with the legal effect of electronic offers, acceptance and contracts.\(^{210}\)

The Guide to the Model Law on Electronic Commerce explains the scope of Article 11 as follows:\(^{211}\)

> It deals not only with the issue of contract formation but also with the form in which an offer and an acceptance may be expressed. In certain countries, a provision along the lines of paragraph (1) might be regarded as merely stating the obvious, namely that an offer and an acceptance, as any other expression of will, can be communicated by any means, including data messages. However, the provision is needed in view of the remaining uncertainties in a considerable number of countries as to whether contracts can validly be concluded by electronic means. Such uncertainties may stem from the fact that, in certain cases, the data messages expressing offer and acceptance are generated by computers without immediate human intervention, thus raising doubts as to the expression of intent by the parties. Another reason for such uncertainties is inherent in the mode of communication and results from the absence of a paper document.

Article 15 provide rules regarding time and place of dispatch and receipt of messages. These rules help in determining when and where information was received. Article 14 deals with acknowledgement of receipt. It focuses on whether or not a data message was received as follows:\(^{212}\)

1. Paragraphs (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.
2. 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

---

\(^{210}\) Ibid.


\(^{212}\) Sorieul, Clift and Estrella-Faria, above n 211.
(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.

(3) 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.

(4) Where the originator has not stated that the data message is conditional on
receipt of the acknowledgement, and the acknowledgement 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.

Due to large-scale use of internet, many countries have legislation that governs
communication and storage of information, which is either inadequate or
outdated. In order to promote international trade and contracts UNCITRAL has
introduced the Draft Model Law on Legal Aspects of Electronic Data Interchange
and other means of communication. The Draft has been adopted by a number of
countries including the US and Australia and it facilitates incorporation of latest
developments of communication technology into the domestic law of the member
States. Further, such incorporation is done without the removal of paper-based
requirements or legal concepts.

The Model Law on Electronic Commerce is acceptable due to its flexibility and it
has influenced many countries regarding electronic commerce legislations including
Canada and the US. Similarly, the Electronic Commerce Directive and the Electronic
Signatures Directive in the European Union (EU) were also influenced by the Model
Law and Draft Rules. Despite the popularity of Model Law on Electronic Commerce
and Model Law on Electronic Signatures, harmonisation has not been achieved and it

2.7 Electronic Signatures and International Developments: Coordination of Developments among International Organisations

After the preparation of the Model Law on Electronic Commerce in 1996, it was sent to various organisations and governments for opinion and views. Countries such as Singapore and Poland and organisations such as the International Maritime Union were of the opinion that the model law on electronic commerce must provide detailed criteria regarding the use of signature method and identification of parties. They believed that the criteria provided by model law on electronic commerce should be further strengthened and elaborated.\footnote{Draft Model Law on Electronic Data Interchange (EDI) and Related Means of Communication, Compilation of Comments by Governments and International Organisations, UNCITRAL (1995).}

During mid-1990s when the Model Law on Electronic Commerce was being developed, different states of the US began to introduce their own electronic signature laws. These states took different approaches that resulted in inconsistency in approaches adopted. For example, Utah was the first state that introduced electronic signature legislation based on digital signatures.\footnote{L Brazell, Electronic Signatures Law and Regulation (2004); M Wang, ‘Electronic Signatures: Do the Regulations on Electronic Signatures Facilitate International Electronic Commerce? A Critical Review’ (2007) 23 Computer Law & Security Report 32, 32.} Later, other states, such as Minnesota, Mississippi, Missouri and New Mexico, also developed digital signatures legislations and adopted a technology-specific approach. However, other states such as California, Alabama, Arizona, Colorado, Connecticut, Delaware and Georgia followed a completely different approach and based their legislations on a technology-neutral approach. Some states combined these two approaches and based their legislation on a hybrid criteria. By 1997, various technology-specific and hybrid...
legislations were being developed, for example the Digital Signature Law 1997 in Germany, and the Electronic Transactions Act 1998 of Singapore.\footnote{Christensen, above n 104; Wang, above n 217.} 

OECD has focused solely on the economic and social impact of electronic commerce.\footnote{UNCTAD, Electronic Commerce: Legal Considerations, UN Doc UNCTAD/SDTE/BFB/1 (1998) 7.} Initially, OECD began its work on authentication as part of its general work on electronic commerce.\footnote{OECD, OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, (2007) 15.} As early as 1997, a conference entitled Dismantling the Barriers to Global Electronic Commerce was organised in 1997 by OECD at Finland.\footnote{OECD, Dismantling the Barriers to Global Electronic Commerce, DSTI/ICCP(98)13/FINAL (1997); T L Yarbrough, ‘Connecting the World: the Development of Global Information Infrastructure’ (2001) 52 (2) Federal Communications Law Journal 315, 319–20.} Broad areas were identified where the involvement of governments as well as international organisations was considered necessary to reduce barriers and uncertainties that could hinder the development of electronic commerce. The broad areas identified included building user and consumer trust in information systems and electronic transactions, ensuring access to the information infrastructure and minimising regulatory uncertainty in electronic environment.\footnote{OECD, Dismantling the Barriers to Global Electronic Commerce (1997) <http://cordis.europa.eu/infowin/acts/ienm/newsclips/arch1997/971008no.html> 8 September 2007.}

In 1998, OECD assessed the economic and social impact of electronic commerce and release a report entitled The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda.\footnote{OECD, The Economic and Social Impacts of Electronic Commerce: Preliminary Findings and Research Agenda, (1999); UNCTAD Secretariat, Legal Dimensions of Electronic Commerce, UN Doc TD/B/COM.3/EM.8/2 (1999).} The report noted that electronic commerce can have a significant effect on global markets and increase interactivity among different countries. Hence, OECD realised the need to create a global framework for electronic commerce.\footnote{Ibid.} In 1998, a follow-up conference was organised in Canada. In October 1998, OECD along with the Government of Canada organised a Ministerial Conference called ‘A Borderless World: Realising the
Potential of Global Electronic Commerce,’ which is also known as the Ottawa Conference.225

In relation to legal frameworks, the Ottawa Conference concluded that electronic commerce requires a consistent and predictable legal framework.226 At the end of the conference, declarations were adopted on protection of privacy in global networks, consumer protection in the context of electronic commerce and authentication for electronic commerce.227 The Declaration on Authentication for Electronic commerce required member countries to adopt a non-discriminatory approach to electronic authentication from other countries and to amendments technology-specific laws or policies that may impede electronic commerce. It also recommended member countries to give favourable consideration to the provisions of the UNCITRAL Model Law on Electronic Commerce.228

The declaration outlined a number of actions to promote the development and use of electronic authentication technologies and mechanisms.229 The Declaration stated that member countries should:230

1. Take a non discriminatory approach to electronic authentication from other countries.
2. Encourage efforts to develop authentication technologies and mechanisms and facilitate the use of those technologies and mechanisms for electronic commerce.
3. Amend wherever appropriate technology or media specific requirements in current laws or policies that may impede the use of information and

228 Ibid.
229 Ibid.
communication technologies and electronic authentication mechanisms, giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by UNCITRAL.

(4) Proceed with the application of electronic authentication technologies to enhance the delivery of government services and

(5) Continue the work at international level together with business and industry and user representatives concerning authentication mechanism to facilitate electronic commerce.

The declaration adopted by OECD was complimentary to UNCITRAL’s work as it recommended countries to giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by UNCITRAL.\(^\text{231}\) Similarly, in 1997, like the UNCID rules ICC developed best practices related to digital signatures.\(^\text{232}\) It was a complimentary work to Model Law on Electronic Commerce. ICC explains it as follows:\(^\text{233}\)

> The Model Law does not specify what method of signing a data message might be appropriate under what circumstances. The Draft Guide to the Model law does indicate, however, that it may be useful in the context of data messages, to ‘develop functional equivalents for the various types and levels of signature requirements in existence’. The GUIDEC attempts to build upon the Model Law in this regard, by defining requirements for signatures used in international commerce, in particular digital signatures, in which there is the additional requirement of certification.

It provides best practices for creating a secure message, principles for safeguarding a message, roles and responsibilities of a signatory and certification authorities, secure means of dealing with digital signatures.\(^\text{234}\)

---

\(^{231}\) Annotated Provisional Agenda, UNCITRAL, UN Doc A/CN.9/WG.IV/WP.109 (2004).
\(^{233}\) ICC, General Usage for International Digitally Ensured Commerce (GUIDEC), 1997.
\(^{234}\) Ibid.
During the late 1990s, UNCITRAL coordinated the developments by initiating work on electronic signatures and certification authorities. UNCITRAL Model Law on Electronic Signatures was adopted by UNCITRAL in 2001. The purpose of the Model Law is to harmonise of laws related to electronic signatures and certification authorities. It adopts a technology-neutral approach. It builds upon the Model Law on Electronic Commerce signature provisions to provide greater legal certainty about the use of certain types of electronic signatures, it provides conduct rules for various parties dealing with electronic signatures and it provides basic standards for the recognition of electronic signatures from other jurisdictions. During the development of Model Law on Electronic Signatures the developments of other organisations were considered by UNCITRAL.  


Article 7 of the Model Law on Electronic Signatures 2001 allows the enacting state to specify techniques that satisfy the reliability test prescribed under law. It also allows legislatures to establish a mechanism through which electronic signatures meeting objective criteria of technical reliability may benefit from predetermined legal reliability. The intention of Article 7 of the Model Law on Electronic

---

Signatures 2001 is not to exclude other types of technologies that meet the reliability requirements of the Model Law Electronic Commerce 1996 and the Model Law on Electronic Signatures 2001, but to offer predictability in these requirements. Once an electronic signature is specified by a government to be reliable under Article 7 of the Model Law on Electronic Signatures 2001 then, the electronic signature automatically meets the reliability requirements of both Article 7 of the Model Law on Electronic Commerce 1996 and Article 6 of the Model Law on Electronic Signatures 2001. Though both the Model Law on Electronic Commerce 1996 and the Model Law on Electronic Signatures 2001 maintain technology-neutral approach, the Model Law on Electronic Signatures 2001 was specifically drafted with a focus on the PKI. Therefore, the Model Law on Electronic Signatures 2001 defines the duties and the standard of care for the entities in the regime of the PKI such as the signatories and the certification authorities.

The Model Law on Electronic Signatures is intended to serve as a model law for Member States while enacting legislation related to electronic signatures. Thailand has already adopted the legislation based on the UNCITRAL Model Law on Electronic Signatures.\(^{239}\)

Model Law on Electronic Signatures is based upon Article 7 of the Model Law on Electronic Commerce. According to the Model Law on Electronic Signatures, there exists a presumption that where certain criteria of technical reliability are met, the electronic signatures shall be treated as equivalent to the handwritten signatures. The Model Law on Electronic Signatures contain basic rules of conduct that deal with the responsibilities and liabilities that may bind upon the various parties involved in the process of electronic signatures, such as the signatory, the trusted third party and the relying party. The Model Law on Electronic Signatures follows the two tier approach regarding authentication.\(^{240}\) Article 7 of the UNCITRAL Model Law on Electronic Commerce recognises any electronic signature method that is applied for the purpose of signing a data message or electronic data as fulfilling the requirements of a signature that is handwritten, which is sufficiently reliable in all circumstances. The


\(^{240}\) Ibid.
Model Law on Electronic Signatures creates the second and the narrower regime. It identifies methods of electronic signature that is recognised by a State authority or private accredited entity or the concerned parties as meeting the criteria of technical reliability as set out in Article 6 of the UNCITRAL Model Law on Electronic Signatures. Article 2 of the UNCITRAL Model Law on Electronic Signatures defines ‘electronic signature’ as ‘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’.  

Article 6(3) of the UNCITRAL Model Law on Electronic Signatures identifies certain criteria to be satisfied by an electronic signature to be considered reliable, which are as follows:

i. The signature creation data are linked to the signatory and to no other person.

Under Article 2(d) of the UNCITRAL Model Law on Electronic Signatures, the signatory is a person that holds signature creation data and acts either on its own or on behalf of the person it represents. The linkage between the data used for the creation of the signature and the signatory is important. Though the signature creation data may be shared by different users, the signature creation data must be capable of identifying unambiguously, one user in relation to the electronic signature. The Model Law on Electronic Signatures does not define the ‘signature creation data’. However, according to the Guide to Enactment, the ‘signature creation data’ covers those core elements that should be kept confidential in order to ensure the quality of the process of signature.  

Regarding electronic signatures (excluding digital signatures), the term ‘signature creation data’ is intended to designate secret keys, codes or other elements in the process of creating an electronic signature, which is used to provide a secure link between the resulting electronic signature and the person of the signatory. For example, in case of electronic signatures based upon the biometrics indicator such as fingerprint or retina scan data, the link is established between the electronic signature and the person of the signatory. However, in case of

\[\text{241} \text{ Ibid.} \]
\[\text{242} \text{ Model Law on Electronic Signatures with Guide to Enactment, UNCITRAL, [para 97], (2001).} \]
digital signatures relying on asymmetric cryptography, the operative element that is said to be linked to the signatory is the cryptographic key pair such as the private and the public keys but only the private key is covered by the description of signature creation data.\footnote{S Christensen, W Duncan and R Low, ‘The Statute of Frauds in the Digital Age: Maintaining the Integrity of Signatures’ (2003) 10(4) \textit{E Law: Murdoch University Electronic Journal} \url{http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html} 22 July 2007.} In addition, the text being signed electronically is also not covered under this description.\footnote{Model Law on Electronic Signatures with Guide to Enactment, UNCITRAL, [para 97], (2001).} At the time of signing, the signature creating data was under the control of the signatory and no other person. In order to satisfy the criteria for an electronic signature to be reliable, the signature creation data must be under the sole control of the signatory at the time of signing. This is similar to the provisions in the Electronic Signatures Directive but the Electronic Signatures Directive refers to the method used to create the electronic signature and also states that the signatory must maintain the signature creation data under the sole control of the signatory. The Guide to Enactment provides example of a situation where the signature creation data is available on a network and it is capable of being used by a large number of persons. However, if the signature creation data is widely available on the network, then it must not be covered by the model law.\footnote{Model Law on Electronic Signatures with Guide to Enactment, UNCITRAL, [para 126], (2001).}

ii. Any alteration made to the electronic signature after it is signed must be detectable

In order to establish the integrity of an electronic signature, any alteration made to the electronic signature after the signature has been affixed must be detectable. Once this criteria is met, then the electronic signature is said to be reliable in order to satisfy the requirement of legislation for a valid signature.

iii. Where the purpose of the legal requirement for a signature is to provide assurance regarding the integrity of the information, then any alteration made in the information after it has been signed must be detectable.

In order to establish the integrity of the information that is signed electronically, any alteration made to the information after the information has been signed must be capable of detection.\footnote{Christensen, Duncan and Low, above n 243.} According to the Guide to the Enactment, this criteria is intended to be used by those countries where, existing legal rules governing the use
of handwritten signatures cannot accommodate a distinction between integrity of the signature and integrity of the information that is being signed.\(^{247}\)

However, one disadvantage with the model law is that the conditions listed in Article 6(3) are not the only conditions for establishing reliability of an electronic signature and Article 6(4) (a) provides the reliability may be established in any other way. Accordingly, under Article 6(4):\(^{248}\)

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.

Paragraph 4 of the Guide to Enactment intends to:\(^{249}\)

Provide a legal basis for the commercial practice under which many commercial parties would regulate by contract their relationships regarding the use of electronic signatures.

However, the other ways of establishing reliability have not been explained under the Model Law on Electronic Signatures. Article 8 of the *Model Law on Electronic Signatures 2001* provides guidelines regarding the conduct of the signatory.\(^{250}\) According to Article 8(1) (a) where signature creation data can be used to create a legally binding signature, the signatory must exercise reasonable care to avoid unauthorised use of its signature creation data and under Article 8(1)(b) the signatory must notify any person who may rely on that signature if the signatory knows it has been compromised.\(^{251}\)

Articles 9 and 10 of the *Model Law on Electronic Signatures 2001* deal with the conduct and trustworthiness of certification service providers and these requirements are similar to those adopted by the EU Electronic Signatures Directive. According to Article 9(1)(c), a certification service provider must provide reasonably accessible means that enables a relying party to ascertain from a certificate the identity of the


\(^{248}\) Ibid; Christensen, Duncan and Low, above n 243.


\(^{250}\) Fitzeiland et al, above n 238, 554–5.

certification service provider and the validity of the signature creation data. Further, under Article 9(1)(f), the certification service provider must also use trustworthy systems, procedure and human resources and the certification service provider must bear the legal consequences of any failure on its part to satisfy this requirement. The conduct of relying party is dealt in Article 11 and Article 2(f) defines relying party as ‘a person that may act on the basis of a certificate or an electronic signature’. 252 According to Article 11, a relying party must bear the legal consequences of his or her own conduct including any failure to take reasonable steps to verify the reliability of an electronic signature or revocation of a certificate that supports electronic signature. 253 As seen above, the combination of Articles 8, 9 and 11 has the effect of placing responsibilities on all parties in the electronic regime. Accordingly, a signatory must take reasonable care to ensure that there is no unauthorised use of signature creation data and where a certificate is used to support his or her electronic signature, then the signatory must ensure accuracy and completeness of the information in that certificate. At the same time, it is the responsibility of the relying party to verify the reliability and validity of the electronic signature. Finally, under Article 12, while determining the validity of a certificate or electronic signature, it is not necessary to consider a number of factors such as geographic location where the signature is used or created or the geographic location of the place of business of the signatory as explained in Article 12(1). 254 In addition, Article 12 provides that an electronic signature created or used outside the enacting state shall have the same legal effect as a signature that is created in that enacting state if the electronic signature offers a substantially equivalent level of reliability. 255

2.8 Soft International Law

Soft International Law International organisations create and implement various international commitments, some of which are contained in non-binding legal instruments. 256 Although states collectively deal with problems and issues at the

252 Fitzeland et al, above n 238, 554–5.
254 Fitzeland et al, above n 238 554–5.
international level, they avoid legal obligations in the form of soft laws.\textsuperscript{257} Soft law is used to describe rules of international law that do not provide concrete rights or obligations. They provide rules that are very vague and flexible. For example, Article 2 of the Convention on Economic, Social and Cultural Rights 1966 requires parties:

\begin{quote}
258
to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.
\end{quote}

The obligation in such instruments is vague in what it requires states to do in order to avoid international responsibility, unlike customary international law that obligates states appropriate compensation following an expropriation of foreign owned property.\textsuperscript{259}

There is no single accepted definition of soft international law.\textsuperscript{260} Some commentators use the term soft international law to include all those instruments that are not hard laws. Others use it to refer morally binding instruments.\textsuperscript{261} It has also been referred as international instrument other than a treaty that contains principles, norms, standards or other statements of accepted behaviour.\textsuperscript{262} Professor Baxter defines soft law and describes their non-binding nature as follows:\textsuperscript{263}

\begin{quote}
Norms of various degree of cogency, persuasiveness and consensus which are incorporated in agreements between states but do not create enforceable rights and duties.
\end{quote}

\begin{flushright}
\textsuperscript{259} M Dixon, Text Book on International Law (3rd ed, 1996) 44.
\textsuperscript{260} Shelton, above n 256, 322.
\textsuperscript{262} Shelton, above n 256, 319.
\end{flushright}
Similarly, Edward Kwakwa defines soft law as a term: 264

Used to refer to certain categories of norms, technically non-binding in nature that states nonetheless follow in practice or to which they at least subscribe.

Dinah Shelton describes soft law in terms of flexible and vaguer nature of a binding instrument and provides the following definition: 265

The term soft law is also sometimes employed to refer to the weak, vague or poorly drafted content of a binding instrument.

Pierre-Marie Dupuy talks about soft law as a form of multilateral cooperation among the members of international community as follows: 266

Soft law is not merely a new term for an old (customary) process, it is both a sign and product of the permanent state of multilateral cooperation and competition among heterogeneous members of the contemporary world community.

Steven Ratner explains soft law as norms formulated by international organisation and offers the following definition: 267

Precepts emanating from international bodies that conform in some sense to expectations of required behaviour but are not binding on states.

2.8.1 Scope of Soft International Law

The most common examples of soft law instruments are the UNCITRAL Model Law on International Commercial Arbitration 1985. Soft law instruments related to electronic contracts and electronic signatures that are discussed in Chapter Three of this thesis are the UNCITRAL Model Law on Electronic Commerce 1996, the UNCITRAL Model Law on Electronic Signatures 2001, the 1998 OECD Declaration on Authentication for Electronic Commerce, and guidelines related to digital

265 Shelton, above n 256, 321.
signatures developed by ICC in 1997 titled General Usage for International Digitally Ensured Commerce (GUIDEC).

The legal effect of different soft law instruments may not necessarily be the same but they are carefully negotiated and drafted statements that in some cases are intended to have normative significance despite of their non-binding nature and form. Soft law instruments can either be concluded at a high level of abstraction and generality while some times they may even include greater degree of specificity.

2.8.2 Reasons for the Adoption of Soft Instruments and Nature of Soft Laws

Soft law is preferred to hard law to avoid complex domestic ratification process. The use of non-binding instruments enable states to agree on more precise provisions as their legal commitment and consequences for non-compliance are limited. Soft laws are preferred as they provide immediate evidence of international support. Soft laws are also adopted as certain international organisations do not have the power to adopt binding legal instruments.

Non-binding instruments that are in the form of declarations and resolutions set goals to be achieved in the future. They are general in nature rather than specific rules or laws. Non-binding instruments are suitable for technical matters particularly when the subject matter is not ripe for the formation of a treaty due to scientific uncertainty regarding the subject matter. Pierre-Marie Dupuy talks about the transformative nature of international law and soft law and the growing need of soft laws as follows:

271 Ibid.
272 Ibid.
273 Shelton, above n 256, 321.
274 Pierre-Marie, above n 266, 435.
275 Ibid.
276 Pierre-Marie, above n 266, 428–9.
277 Shelton, above n 256, 322.
278 Pierre-Marie, above n 266, 420–1.
Rapid evolution of the international economy and the growing phenomenon of global interdependence, combined with progress in science and technology, is creating a need for new branches of international law.

Similarly, Professor Christine Chinkine describes the evolutionary nature of soft laws and international law as follows: 277

The International legal order is an evolving one that requires a wide range of modalities for change and development, especially into new subject areas. They must draw upon the entire continuum of mechanisms arranging from the traditional international legal forms to the soft law instruments.

Legal instruments related to electronic commerce, electronic contracts and electronic signatures are also developing in an evolutionary manner. UNCITRAL developed the Model Law on Electronic Commerce in 1996 to regulate electronic commerce, in 2001 the Model Law on Electronic Signatures was developed to regulate electronic signatures. Both the model laws are in the form of soft legal instruments. In 2005, convention on electronic contracts was developed to address electronic contract formation issues.

Helen Keller describes the nature and their growing importance of soft laws in regulation international activities as follows: 278

Soft law has long existed in international public life, yet it is in the context of new global governance challenges that soft law arrangement challenges have gained significant salience and flourished across the international stage.

Many international issues many be new, complex and novel. The underlying problem may not be clear and apparent. In such cases, states cannot anticipate all possible consequences of a hard law. Hence, in such situations states prefer to leave agreements imprecise. Soft law provides the framework within which states can

277 Chinkin, above n 269, 866–7.
change their arrangements according to the changing circumstances and adopt hard law though further negotiations.\textsuperscript{279}

2.8.3 The Difference between Hard Law and Soft Law

Soft law may be differentiated from hard law, which is binding. Hard law is identified through rules stating clear and specific commitments; conversely, norms or principles that are general in wording are identified as soft laws.\textsuperscript{280} Hard law is also distinguishing from soft law through the method of enforcement. Hard enforcement is specified though hard obligations such as compulsory settlement of disputes. For example, the 1982 convention on law of sea represents a hard obligation by specifying compulsory settlement of disputes involving ICJ, international tribunal as well as various forms of arbitrations. Whereas in soft enforcement, problems are referred to non-binding conciliation.\textsuperscript{281}

Kenneth, Abbott and Snidal Duncan define hard law as legally binding and precise in nature as follows:\textsuperscript{282}

Legally binding obligations that are precise (or can be made precise through adjudication or the issuance of detailed regulations) and that delegate authority for interpreting and implementing the law.

They define soft law and the realm of soft law as follows:\textsuperscript{283}

The realm of ‘soft law’ begins once legal arrangements are weakened along one or more of the dimensions of obligation, precision, and delegation. This softening can occur in varying degrees along each dimension and in different combinations across’ dimensions.

Helen Keller describes the scope of soft law and differentiates soft law from hard law as follows:\textsuperscript{284}

\begin{flushleft}
\textsuperscript{280} Boyle, above n 268, 901–2.  
\textsuperscript{281} Ibid 901, 909.  
\textsuperscript{282} Abbott and Duncan, above n 279, 421.  
\textsuperscript{283} Ibid 422.  
\textsuperscript{284} Keller, above n 278, 249.  
\end{flushleft}
Soft law is a very vague concept, rooted in the international law theory. Drawing on the dichotomy between hard and soft law, one might conceive soft law as a normative realm encompassing everything that is not hard law, or apply it with a more bounded degree of definitional freedom.

Treaties are usually regarded as hard law and binding. However, the distinction between treaties and soft law is not always clear. Treaties may be both hard and soft. A legal instrument that is in the form a treaty does not itself becomes hard law. A treaty may be regarded as hard law if it specifically states the right and obligations provided. If it provides general goals or express obligations in vague terms, rather than clear and concrete terms it is soft. The 1963 Moscow Treaty can be said to be an example of obligation where a part has the right to withdraw from the treaty if it decides that extraordinary events, related to the subject matters of the treaty have jeopardised the supreme interests of its country.


2.8.4 Impact of Soft Law on National Law

The regulation of electronic commerce took place in the form of model law that established an international model for different countries. This section examines the process of internationalisation of soft norms and its impact on national legislation. According to Professor Baxter, once a matter becomes the subject of a soft norm, the matter can no longer be asserted to be within the domestic jurisdiction of the state. It will establish presumptions, indicate the prevailing trend of opinion, and provide a guiding principle that may have a certain inherent appeal for the parties and channel

---

285 Boyle, above n 268, 901–2.
286 Ibid.
287 Chinkin, above n 269, 851.
negotiation and settlement into legal and orderly path.\textsuperscript{289} Similarly, according to Dinah Shelton, the adoption of non-binding normative instruments can lead to the codification of similar virtually identical norms in subsequent binding instruments.\textsuperscript{290} According to Boyle, soft laws are used as authoritative interpretations of the obligations contained in treaty provisions.\textsuperscript{291}

Helen Keller highlights the role of soft law in influencing the conduct of states as follows:\textsuperscript{292}

> Soft law is a generic term referring to category of social norms that are not legally binding per se as a matter of law but with nevertheless have a certain legal relevance in influencing the conduct and decision of states and non state actors.

Similarly, Gruchalla Wesierski talks about the legal and political effect of soft laws on states as follows:\textsuperscript{293}

> These instruments are characterized by the relatively large amount of discretion which is left to the party bound by the obligation. Although soft norms are discretionary in nature there are not without important legal and political effect

Klabbers provides a similar description of soft law in terms of their legal effect in spite of their for soft nature:\textsuperscript{294}

> Those instruments which are to be considered giving rise to legal effects, but do not (or not yet, perhaps) amount to real law.

Similarly, Jonathan L Charney talks about the effect of soft law on international community as follows:\textsuperscript{295}

> Predetermined generalized norms of behaviour, that while non binding as law, attract compliance by targeted members of international community

\textsuperscript{289} Baxter, above n 263, 565.
\textsuperscript{290} Shelton, above n 256, 321.
\textsuperscript{291} Boyle, above n 268, 901–5.
\textsuperscript{292} Keller, above n 278, 248.
\textsuperscript{293} Gruchalla-Wesierki, above n 247, 37.
\textsuperscript{294} Klabbers, above n 261.
According to Pierre-Marie Dupuy, soft law impacts on national legislatures as reference models that anticipate internationally grounded state obligations. Pierre-Marie Dupuy also describes the process through which establishment of a common international understanding takes place as follows:

cross-references from one institution to another, the recalling of guidelines adopted by other apparently concurrent international authorities, recurrent invocation of the same rules formulated in one way or another at the universal, regional or more restricted level, all tend progressively to develop and establish a common international understanding.

Similar cross-referencing was made from one institution to other apparently concurrent international authorities in relation to electronic commerce. For example, the declaration adopted by OECD in 1998 was complimentary to UNCITRAL’s Model Law on Electronic Commerce that was developed in 1996. It recommended countries to giving favourable consideration to the relevant provisions of the Model Law on Electronic Commerce adopted by UNCITRAL.

Professor H.H Koh describes how domestic obedience to internationalised global law occurs. He explains the process of norm internationalisation as follows:

One might distinguish among social, political and legal internationalization. Social internationalization occurs when a norm acquires so much public legitimacy that there is widespread general obedience to it. Political internationalization occurs when political elite accepts an international norm and adopts it as a matter of government policy. Legal internationalization occurs when as international norm is incorporated into the domestic legal system through executive action, judicial interpretation, legislative action or some combination of the three.

The development of international soft law in the form of UNCITRAL Model Law on Electronic Commerce and later as domestic legislation explains the process of norm internationalisation. The development of Model Law on Electronic Commerce

---

296 Pierre-Marie, above n 266, 434–5.
297 Ibid 420–421.
provided an international framework and established a model for the development of domestic legislation.

The UNCITRAL model law has been so popular that it has been adopted by a number of jurisdictions in addition to Australia, including as the Uniform Electronic Transactions Act in the US, the Electronic Commerce Security Act in Illinois and the Electronic Records and Signatures Act 1997 in Massachusetts.²⁹⁹

The UNCITRAL Model Law on Electronic Contracts 1996 was very influential around the world in providing a broad legal basis for electronic communications. Following the development of Model Law on Electronic Commerce, UNCITRAL developed the Model Law on Electronic Signatures 2001 to provide certainty to electronic signatures. Soon after the development of Model Law on Electronic Signatures,³⁰⁰ UNCITRAL at its thirty third session held between 17 June and 7 July 2000 in New York, considered proposals for future work in electronic commerce. Three suggested topics for discussion included electronic contracts (considered from the perspective of the UN Sales Convention), online dispute settlement and dematerialisation of documents of title, particularly in the transport industry.³⁰¹

The proposal to carry out work on existing traditional international instruments and to bring them in line with electronic commerce was made by the Centre for the Facilitation of Procedures and Practices for Administration, Commerce, and Transport (CEFACT), which is a branch of the UN’s Economic Commission for Europe. Traditional conventions were drafted before electronic communications were

developed; hence, their provisions and concepts appeared to require paper-based documents.  

The proposal was made to take necessary action to ensure that the references made to writing, signature and document in the traditional conventions and agreements relating to international trade, allowed for electronic equivalents.

In response to the proposal of CEFACET, the secretariat of UNCITRAL undertook a survey of existing conventions. The survey indicated that the provisions of traditional conventions hindered electronic commerce. For example, the definition of the term ‘writing’ provided by the Convention on Limitation period in the international Sale of Goods 1974, included ‘telegram and telex’, but it did not expressly recognise electronic communications. A note prepared by the secretariat of UNCITRAL described it as follows:  

Various provisions in the Convention refer to communications that need to be made ‘in writing’….The definition of ‘writing’ in article 1, paragraph 3 (g), which includes ‘telegram and telex’, may not prima facie include electronic communications.

Thus, UNCITRAL decided to carry out work on the removal of obstacles to electronic commerce found under traditional conventions and international instruments. However, it also considered other proposals that were on the future work agenda simultaneously. The second topic identified by UNCITRAL for future work was development of a convention on electronic contracts. A proposal to develop a Convention based upon the principles of Model Law on Electronic Commerce was made by US in 1998. The Model Law on Electronic Contracts

---

304 Ibid.
305 UNCITRAL, Legal Aspects of Electronic Commerce—Legal Barriers to the Development of Electronic Commerce in International Instruments Relating to International Trade, [7], UN Doc A/CN.9/WG.IV/WP.94 (2002).
306 UNCITRAL, Proposal by the United States of America, UN Doc A/CN.9/WG.IV/WP.77 (1998); George, above n 300, 313; A H Boss, Electronic Commerce: Globalization of Domestic Law or Domestication of Globalized Law? (Paper presented at the Association of American Law Schools Conference (AASL) on Commercial Law at the Crossroads, Canada, 17 June 2005); Report of the
validates the formation of electronic contracts by stating ‘where a data message is used for the formation of contact, that contact shall not be denied validity or enforceability on the sole grounds that a data message was used for that purpose’. UNCITRAL had recommended all the member states to adopt that provision. However, regional versions were proposed within Latin America and for the Commonwealth of Nations. Most of the legislation that implemented Model Law on Electronic Commerce had adopted that provision. Hence, undertaking work on this aspect had generated some controversy.\(^{307}\) Countries that had adopted the model law had done it inconsistently; hence, international transaction still faced a pack work of legal framework for international transactions.\(^{308}\) In the favour of preparation of a convention it was believed that a convention would contribute to increasing the legal certainty and predictability in electronic business transaction along with model laws.

Further, the Model Law on Electronic Commerce was developed to facilitate electronic commerce and to deal with various obstacles such as formation of contracts, use of signatures and requirement for paper-based documents, which hindered electronic commerce.\(^{309}\) An attempt was not made to develop comprehensive and detail provisions to regulate electronic contracts, instead an attempt was made to support and encourage the overall development of electronic commerce. This was done on the basis of a number of general principles such as the minimalist approach, based on which only those changes were made that were absolutely necessary to accommodate electronic commerce. The drafters wanted to provide a broad and general legal framework to facilitate electronic commerce and to validate electronic transactions.\(^{310}\) Moreover, based on functional equivalence and technology neutrality principles no discrimination was made between the types of technology used to facilitate electronic commerce. This approach was taken to preserve flexibility and to permit the development of new technologies.\(^{311}\)

\(^{307}\) George, above n 300, 316–7.
\(^{308}\) Ibid 317–318.
\(^{310}\) Boss, above n 306.
Although the provisions of the model law facilitate legal recognition of electronic communication and signature, they do not deal comprehensively with the issues of electronic contracts. They only provide a basic enabling framework that facilitates the formation of contracts in an electronic medium and removes barriers to electronic commerce.\(^{312}\) Though it facilitates formation of electronic contracts, it does not deal with various aspects related to the formation of electronic contracts such as the effect of errors in electronic medium, jurisdiction and difference between electronic offer and invitation to treat.\(^{313}\)

The third topic identified for future work was on electronic transport documents such as bills of landing. This proposal was made by the UK and Northern Ireland. UNCTRAL noted the problems related with electronic form of bills of landing and described it as follows:\(^{314}\)

The functions of bills of landing that might be effected by the use of EDI communication included those of serving: (1) as a receipt for the cargo by the carrier; (2) as evidence of the contract of carriage with regard to its general terms and the particular details of vessel, loading and discharge ports, and nature, quantity and conditions of the cargo; and (3) as a document giving the holder a number of rights, including the right to claim and receive delivery of the goods at the port of discharge and the right to dispose of the goods in transit. The first two functions could be easily performed by EDI since the receipt for the cargo and information about the contract of carriage could be given by means of data message such as the UN/EDIFACT message. However, the third function (as document of title) raised difficulties in an EDI environment since, in the absence of single piece of paper, it was difficult to establish the identity of the exclusive holder to whom the carrier could deliver the goods without running the risk of being faced with a claim by another party for misdelivery.

---


\(^{313}\) George, above n 300, 318.

However, this third topic proposed for future work relating to carriage of goods overlapped with a project of another UNCITRAL’s working group that was dealing with transport law. Hence, UNCITRAL did not go ahead with the particular topic.315

2.8.4.1 Common Issues of the First Two Proposals

The working group on electronic commerce finally decided to carry out work on the development of a convention on electronic contracts and to remove obstacles to electronic commerce in existing international instruments. Members of the working group on electronic commerce found that the preparation of an international instrument dealing with issues of electronic contracting and the consideration of appropriate ways for removing obstacles to electronic commerce in existing international instruments were not mutually exclusive.316 The working group agreed that it should attempt to identify the common elements between removing legal barriers to electronic commerce in the existing international instruments and a possible international convention on electronic contracts.317

The prevailing view was that although the Model Law on Electronic Commerce provided a basis for modernising domestic legislation or interpreting international instruments, the legal barriers posed to the development of electronic commerce by the pre-existing international conventions and treaties required special attention.318 In favour of development of convention it was said that a convention would increase legal certainty and legal predictability of electronic transactions along with the Model Law on Electronic Commerce.319 Finally, the working group on electronic commerce decided to continue work on development of a convention on electronic contracts that could harmonise the principles of the Model Law on Electronic Commerce as well as modernise the contract formation provisions of pre-existing trade related instruments.320

315 George, above n 300, 314–5.
317 Ibid.
318 Ibid.
319 George, above n 300, 317.
2.8.4.2 Role of Model Laws as Guiding Principles

This section of the chapter examines how the *Model Law on Electronic Commerce 1996* and the *Model Law on Electronic Signatures 2001* acted as guiding principles for the development of UNCITRAL Convention on Electronic Communication 2005. The nature and theories of soft international law were examined previously. The theories of soft law state that if some sort of soft norm has been consented by the state, the future course of discussion, negotiation and even agreement will not be the same as they would have been in the absence of the norm. The norm will establish presumptions, indicate the prevailing trend of opinion, and provide a guiding principle that may have a certain inherent appeal for the parties and channel negotiations and settlements into legal and orderly paths. This section will examine these aspects of model laws and their role as a guiding principle for the development of convention.\(^\text{321}\)

The Working Group on Electronic Commerce continued work on the convention to facilitate the use of electronic communications in international contracting. The provisions of the preliminary draft convention on electronic communications were part of deliberations and discussion over various sessions between 2001 and 2005. The working group of electronic commerce was composed of all the members of UNCITRAL and the sessions were attended by other international organisations and state delegations.

Like the model laws, it was decided to base the convention on the principle of functional equivalence and technology neutrality. The preliminary draft convention reproduced the criteria contained under Article 6 of the Model Law on Electronic Commerce for the legal recognition of data messages as writing. One of the fundamental objectives of the preliminary draft convention was to enable the formation of electronic contracts. It contained provision on the formation of contract that mirrored Article 11 of Model Law on Electronic Commerce. The preliminary

\(^{321}\) Baxer, above n 263, 565.
daft convention also contained provision on time of receipt and dispatch of electronic message that were similar to Article 15 of Model Law on Electronic Commerce.\textsuperscript{322}

Further, regarding the signature requirement, the working group considered whether the new convention should limit itself to a general provision on the recognition of signatures like Model Law on Electronic Commerce or whether it should state conditions for the legal recognition of electronic signatures in detail like model law on electronic signature. Thus, the preliminary draft convention contained two options

variant A of the preliminary draft convention were provided along the lines of Article 7 paragraph (1) of the model law on electronic commerce.

Variant B provided under the preliminary draft convention reflected Article 6 paragraph (3) of the Model Law on Electronic Signatures.\textsuperscript{323} Thus, Article 13 of the draft convention dealt with form requirement provided variant A and B. Variant A stated that:\textsuperscript{324}

Where the law requires that a contract to which this convention applies should be signed, 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 generate or communicated in the light of all the circumstances, including any relevant agreement.

Variant B stated that:\textsuperscript{325}

(3) Where the law requires that a contract to which this convention applies should be signed, or provide consequences for the absence of a signature, that requiem is met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated in the light of all circumstances, including any relevant agreement


\textsuperscript{323} Ibid 21.

\textsuperscript{324} Ibid 32–33.

\textsuperscript{325} Ibid.
(4) An electronic signature is considered to be reliable for all purposes of satisfying the requirement referred in paragraph 3 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 no other person.
(c) Any alternations to the electronic signature, made after the time of signing, is detectable; and
(d) Where the 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 so signing is detectable.

(5) Paragraph 4 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 3, the reliability of an electronic signature.
(b) To adduce evidence of the non-reliability of an electronic signature.

However, the earlier version of the draft convention discussed above was changed later. Only the Variation A based on the Model Law on Electronic Commerce was retained, by designating the earlier Model Law on Electronic Commerce as sub-paragraph (b)(i) and adding a new sub-paragraph (b)(ii). By borrowing the ‘particular reliability’ method test from the Model Law on Electronic Signatures, Paragraph (b)(ii) seeks to permit the determination of signature reliability prior to a contract dispute, which cannot be overturned subsequently by a judge or other trier of fact.

The signature requirement of the convention states it as follows:

Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
(a) A method is used to identify the party and to indicate that party’s intention in respect of the information contained in the electronic communication;
And
(b) The method used is either:

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant Agreement; or
(ii) Proven in fact to have fulfilled the functions described in Subparagraph (a) above, by itself or together with further Evidence.

Thus, based on the above deliberations and discussion regarding the provisions of the preliminary draft convention that took place between 2001 and 2005, it can be said that Model Law on Electronic Commerce and Model Law on Electronic Signatures channelled negotiations, discussions and acted as guiding principles for the development of some of the provisions of the UNCITRAL Convention on Electronic Communications.

2.8.4.3 UN Convention and the Response of Other Countries

In Singapore, the government called for public consultation to review cyber legislation. The scope of the review included the Electronic Transactions Act and the Electronic Transactions (Certification Authority) Regulations. The objective of the review was to update the legislation and regulations in order to address the changing environment and internationals developments since the enactment of the original enactment. The consultation was conducted in three stages through consultation papers that were issued by the Non Development Authority of Singapore and the Attorney-General’s Chambers. The first stage dealt with electronic contracting issues and the second stage dealt with electronic signatures and certification authorities. In the first stage, which dealt with electronic contracting issues in the ETA, feedback was sought on the following six areas:

i) The first area related to party autonomy and the issues considered were, whether the law must compel parties to accept offers and acceptances in electronic form and whether there must be certain mandatory requirements in electronic contracting that were not open to variation by the parties;

ii) The second area related to the recognition of electronic signatures. The issue considered whether UNCITRAL requirements in relation to function and reliability were consistent with the current provisions;

iii) The third area related to the formation of contracts. The issues considered included whether there must be a provision related to when offer and acceptance in the electronic form must take effect and whether a proposal to enter an electronic contract made to the world at large must be considered an invitation to make an offer;

iv) The fourth area related to the rules on time and place of dispatch and receipt. The issue reviewed was whether the present rules must be amended to be consistent with UNCITRAL, which was related to the control over the electronic message and the capability to retrieve messages rather than the information system that was being used;

v) The fifth area related to automated systems. The issue considered was the status of electronic contracts that resulted from the interaction with automated systems and also issues related to errors made by a person in communication with an automated system; and

vi) The sixth area dealt with miscellaneous issues such as the validity of incorporation of terms and conditions by reference to electronic communication, the manner in which originality of an electronic document was likely to be addressed and whether legislation related to the sale of goods in the physical world applied to electronic goods.

The IDA proposes amendments to make section 47 the central provision in the ETA on government use of electronic records. IDA also proposes amendments to section 9 regarding retention of electronic records in order to provide as a default position subject to express opt-out. Thus, the government agencies would accept retention of documents in electronic form. A new section 9A regarding acceptance of electronic originals was also proposed. These provisions would also apply to non-government transactions. On 26 April 2010 Electronic Transactions Bill (Sig) was introduced.

in the Parliament. It was passed on 19 May 2010. The Act came into force on 1 July 2010. It mirrors UN Convention on Electronic Contracts.\textsuperscript{330}

Section 5 of the \textit{Electronic Transactions Act 2010} (Sing) deals with consent requirements. It states that the parties have a right to decide whether or not to conduct transactions electronically.\textsuperscript{331} Section 9 of the Act allows retention of information in electronic form subject to certain safeguards. Section 13 Deals with receipt and dispatch of electronic communication. The new rules modify the rules provided in the old Act and better suit electronic commerce. The new rules make reference to new modes of communications unlike the old rules.\textsuperscript{332} Section 14 of the Act deal with invitation to treat and state that the information made available through websites are invitation to treat and not offers. Part IV of the \textit{Electronic Transactions Act 2010} is also technologically neutral. Technology specific provisions which were based on digital signatures under the old Act have been moved to the third schedule of the Act.\textsuperscript{333}

In the US, the ABA recommended adoption of the convention. It highlighted the importance of the convention in establishing a certain legal environment as follows:\textsuperscript{334}

In addition to the legal certainty and predictability that will flow from widespread adoption of the E-Contracting Convention, it offers U.S companies an additional advantage. It adopts a model similar to that which they are already familiar with, and have effectively used in U.S domestic transactions for the past several years. This will provide familiar and predictable legal framework, even for transactions not governed by U.S law. To the extend it is widely adopted, it will provide for businesses an internationally endorsed alternative to other countries and regional rules of a more regulatory nature.

The American Bar Association urged the US government to become a adopt the convention.\textsuperscript{335} Thus far, only some of the countries have adopted this Convention,

\textsuperscript{331} Ibid.
\textsuperscript{332} Ibid.
\textsuperscript{333} Ibid.
such as China, Central African Republic, Lebanon, Senegal, Sri Lanka, Singapore, Sierra Leone Colombia, Honduras, Iran, Lebanon, Panama, Montenegro, Madagascar Philippines, Senegal, Saudi Arabia, Russian Federation, Paraguay and Republic of Korea.\textsuperscript{336}

2.9 Conclusion

This chapter sought to explain that three main grouping of issues have been a matter of concern of businesses, traders and legal commentators since the 1970s internationally in Australia and in other countries. The first group were those related to the evidential aspects of writing requirement and signature such as identification, attribution and integrity of contents. The second group related to recognition of electronic form of writing, signature and contract. The third group related to application of traditional contract principles in the electronic environment.

Further, this chapter presented a broader inquiry into how different countries expressed concerns regarding these issues related to electronic commerce between 1970s and the late 1990s. It was found that in the wake of these issues need of global regulation was realised. More specifically, it was illustrated that from 1980 onwards UNCITRAL initiated work on electronic commerce and made efforts to regulate it. Other organisations such as OECD and ICC also played an important role by developing guidelines and declarations. For example, the UNCID rules were developed by ICC, which provided a general basis during the development of Model Law on Electronic Commerce.

In addition, the analysis indicated that the 1998 OECD Declaration on Authentication for Electronic Commerce and ICC’s GUIDEC were complimentary to Model Law on Electronic Commerce. They in turn became part of the development during the preparation of Model Law on Electronic Signatures. Thus, coordination of developments among organisations active in the field of electronic commerce played

\textsuperscript{335} Ibid.
a significant role in the entire norm generation process and in harmonising law related to electronic commerce.

This chapter has also demonstrated that the international developments that were undertaken by different organisations such as OECD, ICC and UNCITRAL were complimentary in nature. Based on Pierre-Marie Dupuy’s theory, it was also highlighted how cross-referencing was made from one institution to other apparently concurrent international authorities in relation to electronic commerce, which all tend progressively to develop and establish a common international understanding of norms. Thus, international organisations contributed jointly towards the making of international norms.

This chapter confronted the deficiencies of traditional law as well as examined the manner in which global norms were developed to address those problems. The next chapter analyses how those global norms were transformed into national norms. Consequently, the next chapter narrows the analysis and examines how the electronic transaction legislation of Australia was ultimately developed based on international norms.
CHAPTER 3
THE TRANSFORMATION OF INTERNATIONAL NORMS INTO NATIONAL NORMS AND ENFORCEABILITY OF ELECTRONIC CONTRACTS

3.1 Introduction

3.2 Development of Internet and Concerns Expressed by Trade Group, Advisory Bodies between and Law Reform Commission from 1990 to 1997

3.3 Electronic Commerce Expert Groups Report and Need for Legislation

3.3.1 Significant Features of Model Law Adopted in Australia

3.3.2 Options for the Resolution of Issues

3.4 Adoption of Existing Regulations that Cover Electronic Transactions

3.5 Implementation of the Convention

3.5.1 Nature of the Changes Needed to Adopt the Convention

3.6 Conclusion

3.1 Introduction

The previous chapter revealed how issues related to electronic commerce arose in Australia and other countries during the 1980s. It showed how concerns of businesses and traders led to the development of Model Law on Electronic Commerce in 1996. This chapter illustrates the developments that took place within Australia from the 1990s onwards and how the Electronic Transaction Legislation was ultimately introduced based on the Model Law of Electronic Commerce. Consequently, this chapter focuses on the discussion that led to the development of Electronic Transaction Legislation.

The aim of this chapter is to provide an overview of issues and developments related to electronic commerce that took place in Australia from 1990 onwards and how Electronic Transaction Legislation was finally introduced.

3.2 Development of Internet and Concerns Expressed by Trade Group, Advisory Bodies between and Law Reform Commission from 1990 to 1997
In the 1990s, the development of the internet created opportunities for consumers to access goods and services offered by traders from all the parts of the world and opened new avenues for conducting commercial transactions. The internet provided a means to conduct business-to-consumer transactions in addition to business-to-business transactions. Commercial transactions over the internet could take place between people who had not met before and who did not have any pre-existing contractual relationship.

In the 1990s, the most common use of electronic commerce was for retail consumer purchases such as CD or book though sites on the internet. It allowed for a wide range of activities such as ordering products locally or from overseas, dealing with after sale service inquiries, 24-hour shopping, advertising, inventory control, ordering, invoicing. The services could be conducted through a graphical user interface on the internet or through a simple email message. According to the Australian Bureau of Statistics, about five per cent of businesses had home pages on websites during June 1997 and only one per cent of businesses used the internet for selling or purchasing goods or services. Further, between June 1997 and May 1998, three per cent of adults used internet to make one or more private purchases.

The Broadband Services Expert Group (BSEG) was established by the government in 1993 to examine and advise the government on the technical, economic and commercial preconditions for the widespread delivery of broadband services to...


5 Australian Bureau of Statistics, Year Book of Australia 1999, ABS Catalogue No 1301.01.
businesses, homes and schools in Australia. It was required to examine various factors such as demand for broadband services, industry development opportunities, the extent to which the industry will be able to take the advantage of the opportunities presented, the customer demand for these services, the reasons people might use electronic services rather than more traditional forms of communication and information exchange, potential benefits and its impact on the Australian community.6

BSEG undertook an extensive public consultation program. Consultations were also undertaken to examine potential demand for new services. An intermediate report was published in 1994 and the final report at the end of the year. The report saw Australia entering a period of significant changes due to the emerging communication services that also presented significant challenges. BSEF recommended the government to establish a National Information Services Council (NISC) to pursue public objectives and to advise both government and industry on future issues related to its development.7

In 1995, the NISC was established as a high level discussion forum for broad policy issues associated with the development of information superhighway. It provided information about the views on marketplace developments, technical issues, community views on the opportunities and challenges posed by electronic commerce. The membership included representatives from a broad range of areas such as community, industry, academia and government to encourage a comprehensive examination and wide-ranging discussion on the issues. In 1995, the NISC published an agenda paper as a means of raising ideas and promoting discussion on responding to developments in information and telecommunication technologies.8

The NISC also released a discussion paper on legal issues that were confronted by the community and the businesses sector. The aim of the paper was to identify the legal issues that community and businesses were confronted with in establishing information the superhighway, to promote discussion regarding the inadequacy of any law dealing with the challenges created by the new technology and to suggest specific areas that needed reform, review or adaptation to overcome actual potential legal challenges. The terms ‘information super-highway’ or ‘global information infrastructure’ refer to the trend of convergence of communications networks, media and computing systems into one system. The discussion paper emphasised that some review and adjustment to the traditional laws was necessary to facilitate electronic commerce. It stated that the there was a need for uniform and predictable laws that could facilitate electronic commerce.

Thus, as discussed above the developments leading to the introduction of electronic transaction legislation of Australia that have occurred from 1990 onwards represent two main concerns. The first is that the failure to follow international trends such as the development of electronic transaction legislation would adversely affect Australian businesses in their international transactions. Second, there was also a growing concern regarding how the electronic transactions, which are relatively new, are to be conducted effectively.

In 1995, the federal Attorney-General Michael Lavarch asked the Australian Law Reform Commission to conduct an inquiry and review the civil remedies available under the Australian law and under international instruments. The terms of reference were as follows: 11

The COMMISSION shall consider, among other matters:

(a) the impact of Australia's participation in international trade and international financial markets on the types of civil and commercial claims that may arise,

---


10 NISC, above n 8.

(b) the impact of Australia's participation in international trade and international financial markets on the types of civil and commercial claims that may arise, 
(c) the extra-territorial application of relevant Australian laws, 
(d) jurisdictional limits, including issues relating to service of process and anticipatory injunctions, and 
(e) the application of Commonwealth law in Australia's external territories.

Accordingly, the ALRC conducted the inquiry in 1995. It noted that there was a lack of an appropriate legal framework for electronic commerce and identified the need for law reform as follows:12

5.56 The cross border character and potential of electronic commerce means that legal issues of this kind are of common concern internationally. They are faced by all countries whose firms are involved in electronic commerce. They will be addressed partly through local law making and partly through international initiatives, such as UNCITRAL's work on EDI and the European Union's Data Protection Directive. To ensure that the Australian legal system develops in line with Australian goals, Australia must be fully involved in the relevant international initiatives and must take them into account in its domestic law making. At the same time it will be important to keep Australian law as consistent with international practices as possible.

5.57 At a domestic level Australian laws, both federal and State, need to be thoroughly reviewed to identify aspects which impede or restrict the adoption of efficient electronic practices. Impediments can arise in various ways including lack of recognition or validity of electronic transactions, requirements for written instruments or records, and a lack of uniformity in State and Territory laws that discourages efficient electronic practices.

ALRC identified the need for an appropriate framework for electronic commerce and recommended adoption of appropriate laws as follows:13

it is recommended that the Attorney-General should commission a comprehensive review of the legal implications of electronic commerce, including a review of the implications of electronic commerce for federal laws,

uniformity of State and Territory laws and relevant international legal and non-legal options. The Commission notes that preparatory work on some parts of this review has already been commenced in the Attorney-General's Department (recommendation 35).

To provide quicker and more flexible legal support for particular electronic commerce opportunities, it is recommended that the Treasurer and the Attorney-General should jointly establish a working group to design and test a safe haven model for the development of on-line electronic trading and investment facilities in Australia. The model would be supplementary to existing law reform and regulatory initiatives on electronic commerce. The project should be completed within 18 months (recommendation 36).


Doing business on-line provides new opportunities in the nature of business and new business opportunities. It also provides new one-to-one, as well as the more traditional one-to-many, customer relationships and greater opportunities for customer-supplier interaction.

Similarly, the report released by the Department of Foreign Affairs and Trade in 1997, ‘The Emerging Digital Economy’, considered the export opportunities created by electronic commerce for Australian business by providing means to access international markets. 15 The report of IITF recognised that it may be necessary for the government to encourage electronic commerce by coordinating industry developments. 16

Also in 1997, The Australian Competition and Consumer Commission (ACCC) released a discussion paper in August 1997 that illustrated the ease with which consumers conducting online commercial transactions could be deceived and made

---

16 IITF, above n 14, 66; De Zwart, above n 4;
to believe that they were dealing with legitimate businesses. The discussion paper dealt with issues related to the protection of consumers in the global market place. 17

In addition to the various specific working groups, the government established the National Office for The Information Economy (NOIE) to develop, coordinate and provide broad policy overview regarding activities such as establishing the regulatory, legal and physical infrastructure environment for online activities and facilitating electronic commerce. 18

Thus, from 1990 onwards, bodies such as NISC and ACCC expressed concerns regarding how electronic transactions, which are relatively new, are to be conducted effectively. However, different advisory bodies and ALRC were of the opinion that failure to follow international trend and international path such as development of electronic transaction legislation would adversely affect Australian businesses in their international transactions. Hence finally Expert Group report was formed to consider the development of electronic transaction legislation based on international developments.

3.3 Electronic Commerce Expert Groups Report and Need for Legislation

Recognising the importance of electronic commerce and the need to consider legal issues to facilitate further development, the Attorney-General, the Honourable Daryl Williams, in July 1997 established an Advisory Group to consider the legal issues arising from the development of electronic commerce. The Advisory Group was required to report the Attorney-General on the form and scope of the appropriate arrangements for regulation of electronic commerce. 19 The Expert Group focused on a number of key objectives including the need to increase the overall efficiency of electronic commerce transactions, the need to resolve legal uncertainties in the

---

17 ACCC, above n 3, 9.
The adoption of electronic and the appropriate means to updating law to account for technological change. The membership of the Expert Group included representatives from industry, business, legal profession and government.\textsuperscript{20}

The Expert Group on Electronic Commerce submitted its final report in 1998. One of its key recommendation was that Australia should adopt the UNCITRAL model law. This Report considered the model law in detail The Expert Group used the model law as its basis because the internationally accepted set of rules are provided by the UN model law.\textsuperscript{21}

The Expert Group was of the opinion that while traditional contract law principles could be stretched to apply to electronic contracts on a case-by-case basis, this approach would give rise to piecemeal results. The Expert Group explained this as follows:\textsuperscript{22}

\begin{quote}
Many commercial and individual players are engaging in electronic commerce in the absence of what might be termed an appropriate legal framework, recognising that electronic commerce in many instances is as reliable and safe as paper and justifies the risk inherent in the legal uncertainty. We are not aware of any court cases in Australia dealing with the issues indicated above and it could be concluded that parties so far have adopted appropriate contractual means of preventing such problems arising. When and as they do arise, disputes could be left to the courts to resolve in the individual cases. One of the disadvantages of this approach is that while certainty will be achieved in respect of particular factual situations, it will be only after litigation, the results of litigation are likely to be piecemeal and may not be able to be applied uniformly. While the courts play a significant role in interpreting the law and adapting it to change, such as recognising the increased use of faxes in forming contracts, the widespread scale and impact of the electronic environment will make it very difficult for the issues to be addressed on a case by case basis. Where existing law mandates paper-based concepts, the courts may find it very
\end{quote}


\textsuperscript{21} Electronic Commerce Expert Group, above n 19, Executive Summary.

\textsuperscript{22} Ibid [4.2.6].
difficult to make the extensions necessary to accommodate electronic communications. After all, while a fax can be characterised as a different form of paper-based communication, a data message clearly is not.

The Expert Group not only identified legal problems but also broad policy options to resolve these problems based upon two important principles stated as follows:23

(1) Achieving functional equivalence, which means that, as far as possible, paper based commerce and electronic commerce should be treated equally by the law and

(2) The related principle of ensuring technology neutrality, which means that the law should not discriminate between forms of technology.

While suggesting the enactment of Commonwealth electronic commerce legislation, the Expert Group believed that it was recommending the minimum legislative requirements that create a scheme of national application that reduces uncertainty regarding the use of electronic commerce and remove the existing legal obstacles to its use, thereby resolving problems related to electronic commerce.24

3.3.1 Significant Features of Model Law Adopted in Australia

The Expert Group Report has deviated from the total acceptance of the UNCITRAL model law in areas of attribution and acknowledgment of receipt of data messages.25 Accordingly, the Expert Group Report at para 4.5.77 states as follows:

It is our view that, in general, legislation should not create rules which either prefer or disadvantage electronic commerce compared with paper-based commerce. The use of signatures on paper for commerce at a distance (by mail or facsimile) involves the risk of forged or unauthorised signatures. However, there is no general legislative rule that entitles an addressee to presume that a signature is the genuine signature of the apparent signer.

...The presence of the apparent signer’s name or letterhead or other indicia of authority will usually be good evidence that the signature is genuine. But the

23 Ibid Executive Summary.
24 Ibid.
25 Electronic Commerce Expert Group, above n 19, [4.5.77].
apparent signer is free to adduce evidence of forgery or unauthorised use and, in general, the addressee takes the risk that the signature was a forgery and therefore not binding on the apparent signer.

According to the UNCITRAL Guide to Enactment, the general principles on which the model law is based includes: 26
1. Facilitating electronic commerce among and within nations;
2. Validating transactions entered into by means of new information technologies to promote and encourage implementation of new information technologies;
3. Promoting the uniformity of law and
4. Supporting commercial practice.

the Expert Group recommended the introduction of Commonwealth Electronic Commerce legislation that would deal with the following issues: 27

1. Introduction of technology-neutral legislation;
2. Application of legislation to ‘data messages’ used in trade or commerce or with government; Data message is defined in Article 2 of the UNCITRAL Model Law on Electronic Commerce, with Guide to Enactment, UN (New York, 1997) as: 28
   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 telescopy.

1. Careful consideration to be provided to any exceptions made to the legislative framework regarding particular instruments or transactions;
2. Variation of terms prescribed by the legislation and these must be permitted by agreement between the parties. However, any variation must be subject to a reasonable test similar to that prescribed under s 68A(3) of the Trade Practices Act 1974 (Cth);

27 Connolly, above n 26; De Zwart, above n 4.
3. Specific acknowledgment that information, records, signatures must not be denied legal effect solely because they are in electronic form;

4. If there is a requirement of ‘writing’ under law, then it must be satisfied by a data message;\(^{29}\)

5. If there is a requirement of a signature or a signed document, then electronic signatures must be given legal effect, subject to minimum standards related to authentication technology providing equivalence to traditional signatures;

6. The legal requirements of originality under the statute or common law must be satisfied with reference to information integrity or authenticity;

7. The legislation may consider and look at the already existing Commonwealth and New South Wales Evidence Acts such as *Evidence Act 1995* (Cth) and *Evidence Act 1995* (NSW) to provide an appropriate model with respect to the admissibility and evidentiary value of electronic documents and data messages;

8. Equivalence of record retention requirements for both the paper-based and electronic commerce;

9. Clarification and certainty regarding the conclusion of a valid contract through transmission of data messages;

10. Default provisions regarding attribution must provide that a person purporting to be the originator of a message must only be bound only if the person in fact sent that message or authorised sending of such a message. The onus of proving this matter must remain with the addressee. However, the rules of attribution must be determined by agreement between the parties;

11. Legislation is not required to deal with acknowledgment of receipt;

12. Provisions regarding time and place of receipt must be developed;

13. Specific action is not required regarding electronic sea carriage documentation; and

14. International approach to these issues must be recognised.

The Expert Group suggested that legislation for electronic signature was not required. According to the group, consideration of legal issues raised by electronic commerce was sometimes complicated by the discussion of the term electronic

\(^{29}\) Electronic Commerce Expert Group, above n 19, [4.5.38–4.5.42].
signatures, that referred to a range of technologies intended to ensure the security and certainty of electronic commerce and in particular the digital signatures that formed one of the technologies. The group also recognised in Chapter 3 of its report that the legislative regimes regarding electronic signatures go beyond ensuring the legal effect of electronic signatures and their functional equivalence with the paper-based signatures. According to the Expert Group, enactment of legislation on electronic signatures is exposed to risk.  

3.3.2 Options for the Resolution of Issues

The report identified three broad options for resolving the legal issues, which are as follows:  

(a) encouraging parties to resolve the issues by contract;  
(b) taking no action at this stage and leaving it up to the courts to determine how existing law will apply to new technologies; or  
(c) enacting legislation to update the law.

The Expert Group report explained the disadvantages of (a) as follows:  

In the Internet or open system context, while contract will govern the terms of individual transactions between the parties, generally there will be no contract which governs the ongoing rights and responsibilities of the parties more broadly in the sense that a trading partner agreement does. In many instances it would be impractical to enter into a series of such contracts where what you are dealing with is isolated or one-off transaction. Securing transactions which occur over this infrastructure is of particular importance, and cannot be realized only by contractual means. A more generally applicable legal approach is needed.

According to the Expert Group, though option (b) could be equated with the minimisation of regulatory burdens upon the government and business, potential benefits were likely to be outweighed by the level of uncertainty and the need of resolving these issues through the courts. Thus, the resolution of disputes by the

31 Electronic Commerce Expert Group, above n 19, Executive Summary.  
32 Ibid [4.2.4].
courts in individual cases could achieve certainty only in particular situations and the solutions achieved through litigation would not be applied uniformly. In addition the large-scale impact of electronic environment would make it very difficult to address the issues on a case-by-case basis. Therefore, according to the Expert Group the merits option (c) were as follows: 33

(a) directly remove legal impediments to the implementation of electronic commerce;
(b) ensure certainty as to the application of the law to electronic commerce and enhance business and consumer trust and confidence;
(c) minimise costs and litigation;
(d) be applied to a wide range of transactions, facilitating both related and unrelated transactions;
(e) satisfy the objective of minimising regulatory burdens upon government and business by adopting a minimal approach and simply ensuring functional equivalence between paper-based and electronic transactions;
(f) provide a vehicle for the harmonisation of laws governing electronic commerce across Australia; and
(g) facilitate the cross-border recognition and enforcement of electronic transactions and signatures.

After considering the above merits and advantages of legislation, the Expert Group recommended (Recommendation 1) that the legislation was the best option for removing the legal uncertainties related to electronic commerce. 34

3.4 Adoption of Existing Regulations that Cover Electronic Transactions

As a result of the recommendations of the Expert Group, the Electronic Transactions Act 1999 (Cth) is an adaptation of the UNCITRAL Model Law

33 Ibid Executive Summary.
34 Ibid Recommendation 1.
on Electronic Commerce.\textsuperscript{35} It was enacted on 25 November 1999. The purpose of the Act as identified in the preamble is to facilitate electronic transactions.\textsuperscript{36}

In 1997, the Victorian Minister for Multimedia established the Electronic Business Framework Group within the Office of Multi Media in the Department of State Development in Victoria. This group proposed that Victoria enact an *Electronic Commerce Framework Bill (ECFB).*\textsuperscript{37}

The contents of the bill were made available to the public as a discussion paper in July 1998. The intention of the bill was to provide that electronic signatures satisfy legal form requirements. The discussion paper also indicated the government’s intention to establish, outside the framework of the bill, an Electronic Signature Recognition Body that would provide guidance to courts and participants in electronic commerce as to acceptable standards of systems and methods of authentication. However, such a specific recognition body was not established ultimately.\textsuperscript{38}

On 16 May 2000, the Victorian Parliament enacted the *Electronic Transactions Act 2000* (Victoria) Act No.20/2000. This Act became effective on 1 September 2000. The *Electronic Transactions Act 2000* (Victoria) is based on the Commonwealth Act,\textsuperscript{39} that is the *Electronic Transactions Act 1999* (Cth), \textsuperscript{40} Similarly, all the other States and Territory of Australia

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{38}Ibid.
\end{itemize}
\end{footnotesize}
have their own Electronic Transactions Act. They too mirror the Commonwealth Electronic Transactions Act.\(^{41}\)

The United Nations adopted the United Nations Convention on the Use of Electronic Communications in International Contracts on 23 November 2005, at 53\(^{rd}\) meeting of its 60\(^{th}\) Session as seen in the previous chapter.\(^{42}\) The Convention aims at enhancing the certainty of electronic contracts in international transactions. It deals specifically with performance as well as formation of contracts in electronic media. Hence, scope of this convention is narrower than that Model Law on Electronic Commerce.

This convention is important because of its role in modernising old and pre-existing conventions, which further facilitates global electronic commerce and brings digital technologies within the scope of old conventions. The convention has also confirmed important principles of technology neutrality and functional equivalence. While the United Nations Convention is based on well establish principles of the model law, it also takes into account the technological developments of electronic commerce.\(^{43}\)

3.5 Implementation of the Convention

Australia has acceded to this Convention. According to Attorney-General Hon Robert McClelland, the intention of adopting this Convention is to increase technology potential and promotion of business by removing obstacles. In order to achieve the goal, there is a necessity for removal of obstacles, which are of uncertain and legal nature. This can be achieved by adopting the United Nations convention. Originally, Australia adopted the Electronic Transactions Act 1999 (Cth), which was based on the 1996 Model law. In order to update 1996 Model Law, United Nations adopted the Convention in the year 2005. The Convention on Electronic

\(^{41}\) Electronic Transactions Act 2000 (NSW); Electronic Transactions Act 2001 (NT); Electronic Transactions Act 2001 (Qld); Electronic Transactions Act 2000 (SA); Electronic Transactions Act 2000 (Tas); Electronic Transactions Act 2003 (WA); Attorney General’s Department, <http://www.ag.gov.au> 2 May 2011.


Communications is based on greater understanding of the use of internet with respect to electronic transactions. Therefore, according to the Attorney-General, Australia must adopt latest electronic commerce law meeting international standard, in order to facilitate electronic contracts in a better way.  

The Attorney-General also expressed that before accession to the Convention, Australia must make changes to the existing domestic electronic transactions laws. This is being done to transform the international law into national law. UNCITRAL finalised this convention in the year 2005, which aimed towards improvement of global and international electronic contract by enhancing certainty of law and business predictions. It is important to note that the UN Convention is the first one to address the legal issues that arise from digital economy. Accession to UN Convention is being considered by Attorney-General.  

The convention updates most core provisions of Model Law adopted in 1996 and it applies to international contracts. However, before adoption of this Convention, countries and governments must decide if they want to apply these rules to a contract made domestically to prevent duplication of law.  

Important aspects of Electronic Transactions Acts’ in Australia as seen in the United Nations convention are as follows:  

(i) A general rule is established confirming the validity of electronic transactions. The Convention provides for similar legal recognition specifically in respect in respect of contracts (article 8.1).  

(ii) Legal requirements or permissions, generally required by statute, for transactions to be in writing or to be signed, or to produce, retain or to record information are met by electronic communications where certain minimum criteria are met. The criteria are directed to establishing functional equivalence between a requirement in traditional paper

---

46 Ibid.  
format and an electronic communication. The Convention establishes similar forms requirements (Article 9).

(iii) For the purposes of a law of each jurisdiction, rules are provided addressing attribution and the time and place of dispatch and receipt of electronic communications. Those rules apply in default when agreement has not otherwise been made by the originator and addressee of the communication. The Convention establishes similar rules addressing time and place of dispatch and receipt (article 10), but does not make provision for attribution.

Though the convention focuses on commercial contract made internationally, Electronic Transactions Acts are widely focussed on the removal of barriers in the use of communication made electronically in governmental and commercial contracts. Thus, Electronic Transactions Acts’ in Australia are applicable in two situations which are as follows:48

i) Domestic contracts that are regulated statutorily and

ii) Contracts regulated under common law.

According to the Attorney-General’s Department adoption of the UN convention needed only minor amendments to the existing Electronic Transaction Acts in Australia in order to update the electronic transactions regime and also for avoiding overlapping with Model Law. However, additional rules that clarify traditional principles of contracts will provide legal certainty.49

The main changes that are proposed before accession to the Convention are as follows:50

i) Minor amendments to the electronic signature provisions and other form requirements,

ii) New rules that recognise the use of automated message systems.

3.5.1 Nature of the Changes Needed to Adopt the Convention

48 Ibid 10.
49 Ibid 10.
50 Ibid 13.
The Attorney-General’s Department is of the opinion that only minor amendments to the Electronic Transactions Laws are required to update the electronic transaction regime. However, additional rules that clarify traditional principles of contracts will provide legal certainty.

Thus, consistent with objectives of the Acts regarding Electronic Commerce, implementation of the convention serves the following purposes:51

(1) Modernise Australia’s law on e-commerce so that it reflects internationally recognised legal standards,
(2) Enhance cross-border online commerce,
(3) Increase certainty for international trade by electronic means and thereby encourage further growth of electronic contracting, and
(4) Confirm Australia’s commitment to facilitating electronic communications in international trade transactions as reflected in Free Trade Agreements.

In Australia, the Electronic Transactions (Victoria) Amendment Act 2011 has become one of the significant pieces of legislation that deals with the latest electronic transactions. This Act commenced on 1 December 201152 and made amendments to the Electronic Transactions (Victoria) Act 2000 (the principal Act). The main purpose and intention of the Act is to amend the Electronic Transactions (Victoria) Act 2000, which was introduced a decade ago. The Electronic Transactions (Victoria) Amendment Act 2011 is expected to bring the current legislation into line with the international standards and to allow for greater certainty in electronic transactions through compliance with international legal standards and in particular with the United Nations Convention on the Use of Electronic Communications in International Contracts 2005.53 Similar amendments have also been made by all the

51 Ibid 10
other states and territories of Australia. Queensland is the only state which has not amended its electronic transaction legislation yet.\textsuperscript{54}

3.6 Conclusion

The developments leading to the introduction of electronic transaction legislation of Australia that have occurred from 1990 onwards represent two main concerns. The first is that the failure to follow international trends such as the development of electronic transaction legislation would adversely affect Australian businesses in their international transactions. Second, there was also a growing concern regarding how the electronic transactions, which are relatively new, are to be conducted effectively.

From 1990 onwards, bodies such as NISC and ACCC expressed concerns regarding how the electronic transactions are to be conducted effectively. Different advisory bodies and ALRC were of the opinion that failure to follow international trends such as development of electronic transaction legislation would adversely affect Australian businesses in their international transactions. Hence, finally the Expert Group was formed to consider development of electronic transaction legislation based on international developments. The next chapter examines the effect of this development and assesses the adequacy of the Electronic Transaction Legislation of Australia.

\textsuperscript{54} Electronic Transactions Amendment Act (NSW) 2010; Electronic Transactions Amendment Act (Tas) 2010; Electronic Transactions Amendment Act (Cth) 2011; Electronic Transactions Amendment Act (NT) 2011; Electronic Transactions Amendment Act (WA) 2011; Electronic Transactions Amendment Act (SA) 2011; Electronic Transactions Amendment Act (ACT) 2012.
CHAPTER 4
ENFORCEABILITY OF ELECTRONIC CONTRACTS: ISSUES ASSOCIATED WITH INVITATION TO TREAT AND ELECTRONIC MISTAKES

4.1 Introduction
4.2 Formation of an Electronic Contract
4.2.1 Methods of Formation of an Electronic Contract
4.3 Basic Elements of Written or Oral Contracts
4.3.1 Offer and Invitation to Treat
4.3.1.1 Electronic Mistakes
4.3.1.2 Electronic Transaction Legislation of Australia: Invitation to treat and Australia’s response to international norms
4.3.1.3 Electronic Transaction Legislation of Australia: Errors and Australia’s response to international norms
4.4 Position in the UK and Invitation to Treat
4.4.1 Position in the UK and Errors
4.5 Position in the US and Invitation to Treat
4.5.1 Position in the US and Errors
4.6 Conclusion

4.1 Introduction

Chapter two looked at the issues that arose under the traditional laws that led to the development of international norms. While, Chapter three looked at the manner in which those norms transformed into national law and how the Electronic Transaction Legislation of Australia was finally introduced. This chapter advances the argument of these two chapter by evaluating what issues arise when traditional contract principles and the Electronic Transaction Legislation of Australia are applied to
electronic contracts. The chapter also assess the manner in which Australia has responded to the international developments examined in chapter two and three.

The aim of this chapter is to evaluate the consequences of applying existing common law principles and the Electronic Transaction Legislation of Australia to electronic contracts. The chapter also aims to evaluate the extent to which Australian electronic transaction legislation mirrors the international principles dealing with electronic contracts.

This chapter specifically focuses on issues dealing with invitation to treat and mistakes. Before evaluating the impact of the Electronic Transaction Legislation of Australia it is necessary to examine the general principles of contract law. Therefore, the chapter first discusses the application of general principles of contract law to electronic contracts. The basic elements of a contract such as offer, invitation to treat and contractual mistakes are examined. The discussion then proceeds to evaluate the effect of regulatory measures on the contract formation process. It specifically examines the effect of the Electronic Transaction Legislation of Australia. This thesis focuses specifically on Australian law. The Laws of the US and the UK is carried out only to gain addition insights.

4.2 Formation of an Electronic Contract

Contract law was developed to deal with paper-based contracts; however, contracts can also be formed electronically. It is the introduction of the internet that now allows people to enter into agreements, regardless of geographical locations, international national borders and time differences.\(^1\) Examples of electronic contracts include buying and selling goods, booking airline tickets and banking transactions. Almost any transaction or contract that can occur face-to-face can now occur electronically.\(^2\)

---


A contract is an agreement under which parties assume obligations to each other for a valuable consideration. A contract is governed by the law of the country or jurisdiction as agreed between the parties or by the law of the country or jurisdiction as imposed by the courts. The law of contract identifies the general elements of a binding contract but it does not require a contract to be formed in a particular manner or method or format.

Most every day contracts do not require formalities. There is no statutory requirement for the contract to be in writing except for the requirement under the Statute of Frauds. An electronic contract may be formed through an email or by completion of the contract on the internet. Two broad categories of electronic contracts include:

i. Sale of Goods. Goods may be ordered and sold over the internet with the payment made through the internet by means of credit card.

ii. Sale of Digitised Products. Goods such as computer software, videos and books may be ordered online and paid for and delivered online. When these contracts are formed electronically the digital products can be downloaded directly from the particular websites.

4.2.1 Methods of Formation of an Electronic Contract

The simplest way of forming an electronic contract is by the exchange of text documents, which could be transmitted through electronic communications such as

---

6 Christensen, above n 4.
email. Parties can use email for business or commerce in several ways. The content or text of an email can include information relating to negotiations, offers and acceptance. Further, it can also include the draft of a contract itself. Contracts can be formed completely through email communication alone or through a combination of other forms of communications such as fax, paper based documents or by means of the telephone. In the case of an email, the offer is made by an offeror and the offeree in turn sends the message. Generally, acceptance is communicated to the offeror, only when the offeror ‘logs’ into the system, which may be compared to the opening of a letter.

Websites enable buyers to order goods generally through electronic order forms and shopping carts. Shopping carts graphically represent a shopping basket or shopping cart of a supermarket. Usually, the purchase of online products is facilitated by click wrap contracts. The terms of such contracts should be accessible to the buyers or customers prior to concluding the contract. These agreements, which contain

standardised electronic forms completed by the buyers or customers, are generally based on the seller’s terms and conditions.17

4.3 Basic Elements of Written or Oral Contracts

All enforceable contracts consist of basic elements such as offer, acceptance, consideration, intention, mutuality, capacity and legality. In order to be valid, electronic contracts must have all these elements to be valid. A valid offer must be made by one party to another; the offer must be accepted by the other party or parties; there must be an intention to be bound by the contract or to create legal relations; the promises made in the contract by the ‘promisor’ to the ‘promisee’ must be supported by a valuable consideration and the terms of the contract must be certain.18 In order to ascertain whether the parties have concluded negotiations and reached an agreement there must have been an offer and an acceptance. If there is an offer and an acceptance, then it indicates the intention of the parties to be bound by the contract. Such a contract will be legally enforceable.19

4.3.1 Offer and Invitation to Treat

An offer in a contract is an indication of one person’s willingness to enter into a contract with another person or persons on certain terms. It must express willingness to be bound without further negotiations regarding the terms of the contract.20 There is no general rule or restriction on the type or number of persons to whom an offer may be made by an offeror. An offeror is free to make an offer to one person or to a particular group of persons or even to the world at large.21 In an online environment, an offer can be made through various means such as a website or email.22 Like other means of communications, emails and electronic data interchange (EDI) transactions

17 Squires, above n 15.
18 Carter and Harland, above n 3, 3; S Christensen, above n 4, 22–4.
20 Australian Woollen Mills Pty Ltd v Commonwealth (1954) 92 CLR 424.
21 Seddon and Ellinghaus, above n 2, 103.
can express willingness to be bound without further negotiations regarding the terms of the contract to constitute an offer.

All contracts are agreements that usually consist of an identifiable offer and an identifiable acceptance. However, there may be instances where a separate offer and a separate acceptance may not be obvious. In such instances, it is not possible to identify with certainty as to which party made an offer and which party accepted the offer, yet this may result in a contract provided the parties did reach a final agreement. Hence, where an offer is not readily and separately identifiable, the intention of the parties must be clear and the terms must be defined properly. 23 In Smith v Hughes24 Blackburn J explained:

If, whatever a man’s real intention may be, he so conducts himself that a reasonable man would believe that he was asserting to the terms proposed by the other party and the other party on that belief enters into a contract with him, the man thus conducting himself would be equally bound as if he had intended to agree to the other party’s terms.

An offer that can be converted into a contract upon acceptance can be distinguished from invitation to treat.26 An invitation to treat invites an offeror to make an offer and opens the process of negotiation.27 It invites a bargaining response from the parties and covers negotiations that are not offers.28 Thus, a very fine line distinguishes an offer from an invitation to treat. An invitation to treat is only an advertisement for something, in contrast to an offer to enter into a contract.29

The seller often makes an ‘invitation to treat’, which is a request to buyers to make an offer and is a part of the negotiation process. When a seller makes an ‘invitation to treat’.

---

23 Clarke v Dunraven (1897) AC 59.
24 Smith v Hughes (1871) LR 6 QB 597.
25 Smith v Hughes (1871) LR 6 QB 597.
28 Seddon and Ellinghaus, above n 2, 90.
treat’ then a reply to such an ‘invitation to treat’ will be an offer, which provides the seller with an option to accept the offer.  

Advertisements and price lists of products that provide details of goods and products do not generally amount to an offer. In *Spencer v Harding*, it was held that a circular stating ‘we are instructed to offer to the trade for sale’ was not an offer that was capable of acceptance and it was only an invitation to treat. The same result is achieved where goods are advertised for sale and where goods are displayed for sale in a shop. In *Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd* Somervell LJ stated:

I can see no reason for implying from this self-service arrangement any implications other than it is a convenient method of enabling customers to see what there is and choose and possibly put back and substitute articles which they wish to have and then go up to the cashier and offer to buy what they have so far chosen.

While, in *Partridge v Crittenden* considering the advertisements as an invitation to treat Lord Parker said:

I think when one is dealing with advertisements and circulars, unless they indeed come from the manufacturers, there is business sense in their being construed as invitation to treat and not offers for sale.

Similarly, in *Grainger & Sons v Gough*, Lord Herschell commented that merchants must not be put in a position where they have contractual obligations that they cannot clearly meet when referring to a trade circular as follows: The transmission of such a price list does not amount to an offer to supply an unlimited quantity of the wine described at the price named, so that as soon as an order is given there is a binding contract to supply that quantity. If it were so.

---

31 Ibid; *Spencer v Harding* (1870) LR 5 CP 561; *Grainger & Sons v Gough* (1896) AC 325; *Spencer v Harding* (1870) LR 5 CP 561.
32 *Spencer v Harding* (1870) LR 5 CP 561.
33 Carter, Peden and Tolhurst, above n 19, 42–3.
34 *Partridge v Crittenden* (1968) 2 All ER 421.
35 *Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd* (1953) 1 QB 401.
36 Ibid 401, 405.
37 *Partridge v Crittenden* (1968) 2 All ER 421, 424.
38 *Grainger & Sons v Gough* (1896) AC 325, 334.
the merchant might find himself involved in any number of contractual obligations to supply wine of a particular description which he would be quite unable to carry out, his stock of wine of that description being necessarily limited.

In *Fisher v Bell* Lord Parker differentiated between offer and invitation to treat as follows:39

It is clear that, according to the ordinary law of contract, the display of an article with a price on it in a shop window is merely an invitation to treat. It is in no sense an offer for sale the acceptance of which constitutes a contract.

The same view applies to the electronic contracts today. Thus, the seller’s, online presence, may be considered an invitation to treat that is similar to the display of goods in a shop in a traditional manner.40

Business organisations usually operate a website with a home page containing information about the site and as well as provide links to further information deeper within the site.41 The increased circulation offered by the internet and the nature of electronic advertisements result in complex situations as seen in an advertisement issued by Argos Distributors. Argos Distributors displayed a television on their website priced at £2.99 incorrectly instead of £299. Hundreds of customers in Europe and the UK placed an order for the television but the retailer refused to fill the orders stating that the television was incorrectly priced by mistake and the correct price was £299.42 The increased exposure of the internet advertisement had attracted a large number of customers. If the same advertisement had appeared in a paper-based medium such as a newspaper or catalogue and merely provided information about the goods for sale43 with an incorrect price, then the advertisement will be considered an invitation to treat.44 Since the advertisement that belonged to Argos Distributors

40 Squires, above n 15, 102–3; Graw, above n 2, 459–60.
42 Christensen, above n 4.
43 Ibid.
44 *Partridge v Crittenden* (1968) 2 All ER 421.
was only an invitation to treat, it was within their rights to refuse to fulfil the orders.\textsuperscript{45}

However, the display of goods or services by an online merchant on its website may also amount to an offer if the website is formulated in a manner to facilitate formation of a contract.\textsuperscript{46} In such a situation, the intention of the seller is very important to understand if the seller is making an invitation to treat or an offer.\textsuperscript{47} Whether a vendor’s advertisement is an offer or an invitation to treat is determined by examining the objective intention of the business’s conduct. A vendor will be considered to have made an offer if a reasonable person believes that an offer was being made. Such offers will be binding on the vendor. Thus vendors activity on the internet through websites or by email will be regarded as an offer if those activities appear to a reasonable person as signifying intention to be bound if a response is made by the customer.\textsuperscript{48} For example, based on \emph{Carlill v Carbolic Smoke Ball Co}\textsuperscript{49} statements like this made by the websites can be regarded as offer:\textsuperscript{50}

\begin{quotation}
Purchase a participating LG 3D TV or any model LG TV product on the same day and same stores, the first 4,000 will receive $150 CASH BACK!
\end{quotation}

If a customer responds to a promise made by a seller to do something in return if a condition is fulfilled then such statements can also be regarded as offers for example:\textsuperscript{51}

\begin{quotation}
Get a Bonus Vegas Movie HD Platinum movie editing software when you purchase a SONY handy cam
\end{quotation}

In addition to the language used on the website the type of website is also relevant in deciding whether the seller is making an offer or an invitation to treat. Websites may be of two kinds: non-interactive sites and interactive sites.\textsuperscript{52} A non-interactive site

\textsuperscript{45} Christensen, above n 4.
\textsuperscript{47} Squires, above n 15; Christensen, above n 4.
\textsuperscript{49} \textit{Carlill v Carbolic Smoke Ball Co}. (1893) 1 QB 256.
\textsuperscript{51} \textit{Carlill v Carbolic Smoke Ball Co}. (1893) 1 QB 256.
\textsuperscript{52} Squires, above n 15; Christensen, above n 4.
only provides information and any contact with the online merchant or seller is through other means such as confirmation of an order by phone or by offline delivery of goods. Hence, there will be very little difference between an advertisement that is paper-based, conventional or traditional and an online advertisement on the web page. The website conveys the implied intention of the seller through its nature of being non-interactive that the seller will negotiate the terms of the contract. Such an implied intention is arguably conveyed as a non-interactive website which only provides information about the product that is being sold, like an advertisement. It merely directs customers to contact the seller to carry out the transaction through other means of communication such as phone, fax or mailing address.\textsuperscript{53}

Comparatively more complicated transactions take place through interactive sites as they not only advertise or display products but also facilitate negotiation.\textsuperscript{54} In an interactive site, a person will be able to log into the website, choose an item for sale, make payment by entering details and conclude the agreement, thereby the display of items on the website goes beyond a mere invitation to treat and may in some cases be considered an offer. However, if the website is considered the same as a display of goods in a window of a store or on a shelf, then the courts will be reluctant to hold the display as an offer. While deciding whether there is an invitation to treat or an offer in the process of formation of contract, it is necessary to consider whether the online vendor intended to be bound by the response received or retained a discretion to be bound or not. If a non-interactive website merely displayed or advertised products and did not provide for an automated response from the buyer then the display or advertisement must be considered an ‘invitation to treat’ unless the vendor or seller intended otherwise.\textsuperscript{55}

Interactive websites display terms and conditions on the website and buyers accept these terms while placing an order. This fact combined along with the design aspect of the web site strengthens the argument that the display of goods through interactive websites could be regarded as offers and not as invitations to treat. These terms

\textsuperscript{53} Squires, above n 15; Christensen, above n 4; Techno and Gadget Zone at Bryo Zone, Setting up a Non–Interactive Web Page <http://www.bryozone.com> 4 March 2011.
\textsuperscript{54} Squires, above n 15, 99–100, 104; Glatt, above n 7, 50.
sometimes limit the liability of the seller and also specify the conditions on which
they will be bound immediately. By means of an interactive website the entire
transaction can be carried out online while the delivery of the product takes place
offline in a normal manner. Such websites will most likely be interpreted as offers
and not invitation to treat. In Australia websites of major retailers appear to fall
under this category. Transactions carried out through interactive websites differ
from face to face transactions which are carried out in person. Hence differentiation
between offer and invitation to treat becomes more problematic in an online scenario.

Some interactive sites may be automated websites that are completely operated by a
computer. In such sites, the buyer adds their credit card details and request certain
information or software, and this information is then transmitted automatically over
the internet to the online merchant. In such a situation, there may be a strong analogy
to be drawn with the offering of goods or a ticket in a vending machine as seen in
Thornton v Shoe Lane Parking Ltd. In this case the English Court of Appeal
considered that in vending machines, the offer is made when the proprietor of the
machine holds it out as being ready to receive the money. Transactions carried out
through vending machines are regarded as unilateral offers as seen in Thornton v
Shoe Lane Parking Ltd. Here the automatic vending machine was installed to enter
into contract with customers for using a car park. It indicated the proprietor’s
intention to be bound by the contracts entered by the automatic machine. By analogy,
the actions of an automatic web site set up in a similar manner could be attributed to
the vendor. Setting up of such automatic websites could be regarded as unilateral
offers.

Lord Gordon Wheeler stressed on the fact that the transaction carried out by
a vending machine are irrevocable.

In the case of ticket which is proffered by an automatic machine there is
something quite irrevocable about the process. There can be no locus
poenitentiae

56 Christensen, above n 4; David Jones <http://www/davidjones.com.au> 4 March 2012; Coles Myers
57 Thornton v Shoe Lane Parking Ltd (1971) 2 QB 163.
58 Ibid.
59 Squires, above n 15, 103–106.
Similarly automatic websites which allow customers to download music and books appear to be irrevocable in the similar manner.\(^6^1\) Comparatively more complicated transactions take place through automatic websites as they not only advertise or display products but also facilitate formation of contract completely.\(^6^2\) In addition, websites which control the actions of a customer significantly by making the transaction time bound do not provide much scope for a customer to negotiate the contract similar to a vending machine. However, vending machines slightly differ from automatic websites in both content and functionality. Vending machines are usually used only for cheap disposal items such as chocolates, soft drinks unlike websites which are used for expensive products like laptops and sometimes even cars. Vending machines carry out the transaction by merely making the selected product available to the customer. While, automatic websites carry out more advanced functions by making decisions such as issuing discount coupons, issuing special product vouchers. They also use Web based cookies to identify, follow and target users in a personal and timely manner. Mobile phone marketing also enables bar codes scanning, integrated viewing of products, product demonstration and price comparison. In addition retail specific and store specific applications are also made available to the users. Furthermore, a new technology called senseng allows users to feel the texture of products. This can be done while carrying out activities such as organizing desktops, surfing the web and selecting text.\(^6^3\) Further, through vending machines direct physical selection of products is made unlike web based transactions which are carried out remotely. Due to these difference web based transactions provide scope for more errors. This issue is more clearly demonstrated by kodak.com.

Price of a digital camera was wrongly stated by Kodak.com. Many buyers placed orders to buy the digital camera but the company refused to fulfil the orders placed by them. Around 2,000 orders were placed for wrongly offered price on the website which was £ 100 instead of £329. An acknowledgement was sent to the customers for the orders placed. However, the company denied that the contact was in fact

\(^{62}\) Squires, above n 15, 99–102, 104; Glatt, above n 7, 44–50.
formed and apologised to the customers but refused to honour the orders. Following this a legal action was threatened but did not materialise. The company later decided to fulfil the orders due to the risk of fighting a losing court battle and negative publicity. Thus, legal intervention may be required in the light of the error made by kodak.com. This case slightly differed from the Argo’s case discussed above. In the Argoes’s case customer’s order was not confirmed although the site was an interactive website. While, in Kodak’s case customer’s order was confirmed. Such a confirmation can be deemed to be acceptance in the legal sense.  

Similarly, Mark & Spencer online line website wanted to reduce £ 599 on a 50 inch Panasonic TV but ended up reducing £ 199. Hundreds of shoppers placed orders through the website before Mark & Spencer corrected the error. They initially refused to honour the orders and offered £ 25 goodwill voucher. Several customers placed complained on the hot UK deal website subsequent to this Mark & Spencer agreed to go ahead with the deal of £ 199 by sending confirmation email to the customers.

On similar lines, Zappos.com suffered a loss of $1.6 Million due to a billing error caused by its software programme. While, in 2009 an LCD screen was offered by Dell computers from its Taiwan website for $ 15 instead of $ 148. Within a short span of time 26 thousand customers placed orders for more than 140 thousand screen. Dell refused to honour the orders. The consumer Protection Agency of Taiwan intervened and a fine of $ 30,000 was inflicted on Dell. These cases indicate the intensity of the issue.

---


67 Ibid.

Likewise a merchandising team of a website called 6pm.com set the price at $49.99 instead of $1000. As soon as the error was detected the website was shutdown. However, the company lost $1.6 million by honouring the orders which took place as a result of price error.\(^{68}\)

In a similar manner Dell advertised a cannon camera worth $1600 for a price of $196. The company gave the customers a choice to cancel the order and accept a $230 lens. Later Dell cancelled the order and gave replacement lens to its customers. It relied on the terms and conditions which said that it will not be responsible for pricing errors. However, such terms may not be enforced always and such a clause may be challenged on the basis of being unreasonable. Further, terms may not be enforced always due to jurisdictional issues discussed in section 2.32.3 of the chapter below.\(^{69}\)

While, buy.com had to agree for a $575,000 settlement when 7,000 customers sued the company when it refused to honour their orders for a Hitachi monitor worth $164 which was displayed on the website for $588.\(^{70}\)

### 4.3.1.1 Electronic Mistakes

When a mistake is committed at the time of formation of a contract, then the parties may set aside the contract under common law and also equity. This principle applies to all contracts including paper based or traditional or conventional and also electronic contracts. Even in Australia, no distinction is made between a paper based contract and an electronic contract when mistake is present in a contract while setting aside such a contract. However, the fact that electronic contracts may be made quickly and can be automated, increases the risk of mistakes that cannot be readily

---


corrected before a recipient of an electronic communication has relied on the mistake.\textsuperscript{71}

From the above, it may be concluded that where a mistake has been made during the formation of a contract, the same legal principles will apply to the contract irrespective of whether the contract has been formed traditionally or electronically. Where the parties intend to use electronic transactions to form a contract then the parties may implement communication protocols to minimise the occurrence of inadvertent mistakes in the contract.\textsuperscript{72} Despite these precautions if mistakes do occur in an electronic contract then the parties may avoid such contracts by the application of the general law of contract. Unilateral mistakes can make the contract void. This will happen if the non mistaken party knew about the error. Internet retailers often offer genuine deals which appear to be too good to be true. For example web sites such as half.com focuses on such cheap deals. Websites such as Amazon.com also offers deals which are not normally offered at offline stores. It makes it difficult to assess whether the customer knew that it was an error unless it is as obvious as it was in Argos were the TV was offered for 2.99.\textsuperscript{73} Unlike traditional offline stores most online sales take place automatically through websites hence the likelihood of mistakes is intensified in the online world. An online vendor will usually detect the mistake only at the time of shipping the order after the formation of contract. In case of offline vendor mistakes will be usually detected at the checkouts before the formation of contract.\textsuperscript{74}

As a protective measure, to avoid liabilities associated with pricing errors, some online vendors are deferring the formation of contract till the time of delivery as follows:\textsuperscript{75}

\begin{quote}
Your order represents an offer to us to purchase a product which is accepted by us when we send e-mail confirmation to you that we've dispatched that product to you
\end{quote}

\textsuperscript{71} Christensen et al, above n 9, 16.
\textsuperscript{72} Ibid 16–17.
\textsuperscript{73} Taylor v Johnson (1983) 151 CLR 422; Groebner, above n 70.
\textsuperscript{74} Groebner, above n 70.
\textsuperscript{75} Amazon.co.uk <http://www.amazon.co.uk/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=1040616> 17 July 2012.
While, some websites are specifying more detailed requirements along with deferring the time of contract formation as follows:  

When entering into a sale contract via the website, you will be taken to have communicated your offer to purchase the products(s) only when:
(i) any requirement set out in these terms have been met;
(ii) the electronic instruction containing the offer from you enters and is recorded in our database;
(iii) a record is created and stored in our database; and
(iv) Harvey Norman online receives in its account full payment from you.

However, the above approach is ill-suited. It provides more scope for a customer to cancel the order till the time of delivery or till the payment is made. Further, a contract will never form if the customer provides wrong email address by mistake, if the address gets clipped by the data base, if the data stored on the server is lost or gets corrupt.

Overall, the traditional principles in relation to invitation to treat are displaced in the online medium. It appears that the automatic online websites are giving an impression that the online vendor is making an offer to a reasonable customer. The principles of unilateral mistake will also not be of much help to the vendors. Traditional contract law does not provide clear-cut principles in relation to electronic contracts.

Similar concerns regarding inadequacy of traditional contract law are reflected in the discussion paper exploring the scope for reforming Australian contract law as follows:

The internet is now used for an increasing number of transactions- affecting commercial and consumer contracts. Arguably, Australian contract law has

---

been slow to adapt to new methods of business-to-business communication and the widespread use of the Internet for business and leisure purposes. Important issues remain unanswered. Traditional rules may be unsuitable in this new context or their applicability may be unclear.

Attorney General Nicola Roxon has highlighted the need of contract law reform from the perspective of electronic contracts as follows:

Ensuring that Australian contract law is innovative and adaptive will help to build business confidence in the digital economy, and help business to embrace new opportunities.

While, the need for a predictable and certain legal environment to boost the confidence of business and consumers was highlighted in the following manner:

Contract law is an essential base for economic activity, providing businesses and individuals the certainty and predictability needed to trade and invest with confidence.

Analysis of traditional principles in relation to invitation to treat indicated lack of predictable and certain environment for electronic contracts. Concerns expressed by the discussion paper regarding lack of appropriate framework for electronic contracts seems correct.

4.3.1.2 Electronic Transaction Legislation of Australia: Invitation to Treat and Australia’s Response to International Norms

In recognition of difficulties dealing with invitation to treat the *Electronic Transactions (Victoria) Amendment Act 2011* made amendments to the *Electronic Transactions (Victoria) Act 2000* to include a new criteria dealing with invitation to treat. It also aims to bring the current legislation into line with the United Nations Convention on the Use of Electronic Communications in International Contracts.

---

Similar amendments have also been made by the other states and territories of Australia.  

Under article 11 of the convention, the binding nature of advertisements made on websites is discussed. It also deals with invitation to treat. Accordingly, Recommendation 5 made by the Attorney-General’s Department for accession of the convention states:  

5) The ETAs should incorporate a provision that proposals to enter a contract made by electronic means to the world at large are to be treated as an invitation to make offers, unless there is a clear indication by the trader of an intention to be bound.  

Article 11 addresses the difference between an invitation to offer or treat and offer. The distinction turns on a vendor’s intent, when the vendor fails to indicate willingness or intention of being bound under an offer.  

Under Article 11, the intention of the vendor to be bound by an offer must be evaluated based on the circumstances, such as automatic systems used for placing order and click wrap icons provided for the formation of contract. This criterion is not completely convincing by itself as different technologies used for expressing intent will represent different degrees of intent. This criterion can also confuse consumers regarding vendors’ actual intentions. This approach is too weak to be effectively workable for electronic commerce, as it leaves many questions unanswered, such as how the intention of trader must be determined, and which technology must be considered satisfactory  

80 Electronic Transactions Amendment Act (NSW) 2010; Electronic Transactions Amendment Act (TAS) 2010 Electronic Transactions Amendment Act (Cth) 2011; Electronic Transactions Amendment Act (NT) 2011; Electronic Transactions Amendment Act (WA) 2011; Electronic Transactions Amendment Act (SA) 2011; Electronic Transactions Amendment Act (ACT) 2012.  
82 Ibid 19.  
84 Ibid 65–9.
Section 14 B of the Electronic Transactions (Victoria) Amendment Act 2011 deems all the websites as invitations. Proposals to form a contract are regarded as invitation to treat unless they are specifically addressed to one or more parties. The distinction depends upon the intention of the vendor. In the absence of clear intention to be bound, the vendor will not be bound until the price offered by the buyer is accepted by the seller. Article 14 makes an attempt to reflect the distinction made between offer an invitation to treat seen in Spencer v Harding, Partridge v Crittenden, Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd, Grainger & Sons v Gough and Fisher v Bell.

Under the electronic transactions legislation proposal to form a contract will be regarded as an invitation to treat if two requirements are met: (1) proposal must not be specifically addressed to a person. (2) Vendor’s intention to be bound by the contract must not be expressed. The first criteria does not take into account the fact that the registration required by all most all the online shopping websites can be regarded as communications specifically addressed to the buyer. Communications can also be regarded as specifically addressed to a person when promotional advertisements are sent to the email address of a person. In addition, pop up advertisements, advertisements made available through hyperlinks can also be regarded as proposals made specifically to a person as they target specific people. Therefore, the criteria appear to be unworkable. Further, under Section 14 B the proposal must be ‘generally accessible’ to the parties using the information system.

---

87 Spencer v Harding (1870) LR 5 CP 561.
88 Partridge v Crittenden (1968) 2 All ER 421.
89 Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd (1953) 1 QB 401.
90 Grainger & Sons v Gough (1896) AC 325, 334.
92 Electronic Transactions (Victoria) Amendment Act 2011.
93 Ibid.
95 Electronic Transactions (Victoria) Amendment Act 2011.
96 Ibid.
The term ‘general accessible’ can amount to global world wide access it does not provide precise criteria in relation to accessibility from the prospective of invitation to treat. 97

The second criteria is also equally flawed.98 Under the second criteria intention of the vendor is the decisive factor. In the online environment intention to be bound can be expressed in various modes such as click through icons, product description.99 Sending acknowledgement of order and confirmatory email.100 These factors can help in determining intention to be bound. In addition, website which incorporates shopping carts prescribes sequence of steps that the buyer should follow to form a contract. These factors provide strong evidence that the vendor wishes to be bound by the contract immediately.101 Moreover, automatic websites facilitate formation of contract instantly. Making goods and products available through automatic websites itself provide strong proof that the vendor intends to be bound by the transaction immediately.102

The electronic transactions legislation intends to transform the traditional principles relating to invitation to treat in the online environment. Unlike traditional law electronic transaction legislation, presumes websites as invitation to treat although websites sometimes make offers. It does not distinguish offers and invitations to treat based on the technology involved. Inability to negotiate the contract is not considered as the basis as in the case of vending machines as seen in Thornton v Shoe Lane Parking Ltd.103 it merely focuses on the language used by the website vendors.104

4.3.1.3 Electronic Transaction Legislation of Australia: Errors and Australia’s Response to International Norms

97 Ibid.
98 Ibid.
99 Electronic Transactions (Victoria) Amendment Act 2011; Polaski, above n 94.
100 Electronic Transactions (Victoria) Amendment Act 2011.
101 Ibid; above n 94.
102 Electronic Transactions (Victoria) Amendment Act 2011.
103 Thornton v Shoe Lane Parking Ltd (1971) 2 QB 163.
104 Electronic Transactions (Victoria) Amendment Act 2011.
In recognition of difficulties associated with online errors, electronic transactions legislation of Australia prescribes rules which deal with errors. The *Electronic Transactions (Victoria) Amendment Act 2011* made amendments to the *Electronic Transactions* (Victoria) Act 2000 to include a new criteria dealing with errors. It also aims to bring the current legislation into line with the United Nations Convention on the Use of Electronic Communications in International Contracts 2005.

The Article 14 of the convention enables a party to withdraw the portion of the communication consisting of input errors. The convention however does not deal with electronic mistakes specifically. Therefore is not completely adequate. Like the convention, the underlying intention of the *Electronic Transactions (Victoria) Amendment Act 2011* is barely to provide a specific remedy in relation to input errors and not to interfere with the common law principles dealing with mistake seen in *Taylor v Johnson* discussed above. If the specific criteria dealing with errors under section 14 of the *Electronic Transactions (Victoria) Amendment Act 2011* are not met then the consequences of the mistake will be as provided by the common law.

Section 14 D of the electronic transaction legislation of Australia merely says that the transaction which contains errors can be set aside. It does not deal with the issues of pricing errors from the perspective of, online vendors. Furthermore, Section 14 D is not broad enough to cover data base errors in general this aspect has been sidestepped. It merely deals with input errors made by a natural person when dealing with automated systems and allows a party to withdraw the contract if an error is

105 Ibid.
106 Ibid.
108 *Taylor v Johnson* (1983) 151 CLR 422B.
110 Ibid.
111 Ibid.
made. It deals with input error such as entering wrong quantity of goods in an order form. The safeguard provides an opportunity to withdraw the contract. Arguably, s 14 D covers input errors such as multiplication errors, price calculation errors and currency conversion errors which are generally made by automatic websites. It provides a remedy only in relation to such errors. However, such errors are obvious to the buyers therefore vendors can set aside the contract on the basis of common law principles related to mistakes. Therefore, s 14 D has barely duplicated the effect.

Section 14D (2) (a) deals with situations when input errors are made by natural persons in their transactions with automated message systems. Section 14 D (2) (b) limits the scope of the section by stating that it only applies when the automated message system does not provide an opportunity to correct errors. While, s 14 D (2) (C) and (D) allow a party to withdrawn the portion of the contract consisting of error if material benefits are not obtained.

Section 14 D (3) states that the safeguard is not intended to give parties an opportunity to repudiate disadvantageous contracts or to avoid legal commitments. It should be noted that Section 14 D (3) does not go far enough and prevents parties from cancelling their orders on the basis of errors. Under s 14 D (2) (C) and (D) withdrawal can only be made after notifying the other party about the error. This approach provides scope for significant delays in the contract formation process and displaces the benefits of speedy worldwide transactions facilitated by the internet. Under 14 D (2) (C) and (D) a customer can withdraw the portion of contract

112 Electronic Transactions (Victoria) Amendment Act 2011, Explanatory Memorandum, 18; Electronic Transactions Act 2011 (Victoria), Section14 D (2) (b); Electronic Transactions (Victoria) Amendment Act 2011.
113 Electronic Transactions Bill 2011 (Vic) Explanatory Memorandum, 18.
116 Ibid.
117 Centrovincial Estate v Merchant Investors [1983] Com LR 158; Hartog v Colin and Shields (1939) 3 All ER 566; Taylor v Johnson (1983) 151 CLR 422B.
consisting of error till goods are received. It provides significant scope for withdrawing the order on the basis of errors and open door for manipulation.\footnote{Electronic Transactions (Victoria) Amendment Act 2011.}

4.4 Position in the UK and Invitation to Treat

The \textit{Electronic Communications Act 2000} (UK)\footnote{Electronic Communications Act 2000 (UK).} provides vague provisions relating to electronic contracts and does not deal with the issue of invitation to treat specifically. The Act defines the term ‘electronic communication’ as communication transmitted by means of electronic communication networks. Electronic Commerce (EC Directive) Regulations 2002 defines the term ‘commercial communication’ as communication intended to promote goods and services of a person pursuing a commercial activity. These definitions are broad enough to cover electronic contracts formed by emails, electronic data interchange (EDI) and web based transactions.\footnote{Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No 2013.}

Regulation 7 of the Electronic Commerce (EC Directive) Regulations 2002 requires service providers to ‘clearly identify’ any promotional offers and to make them available in an ‘unambiguous’ manner. Additionally, the person on whose behalf such a commercial communication is made must also be identified clearly. Notably, it does not state how the commercial communication must be made available in a ‘clearly identifiable’ manner and leaves scope for uncertainties. It raises unanswered questions as to what amounts to ‘clearly identifiable’ manner and is therefore inappropriate. Although the regulation deals with ‘promotional offers’ it does not define what amounts to promotional offers.\footnote{Ibid.} The regulation only deals with promotional offers, it does not specifically deals with invitation to treat by taking account the technical features of automatic websites.

Regulation 9 talks about the different technical steps which the service provider must prescribe for concluding a contract. Unfortunately, it does not go far enough and deal with invitation to treat which have broader implications.\footnote{Ibid.} The question of determine whether an order under Regulation 9 is a contractual offer is left to the

\footnotesize{\begin{itemize}
  \item\footnote{Electronic Transactions (Victoria) Amendment Act 2011.} \item\footnote{Electronic Communications Act 2000 (UK).} \item\footnote{Electronic Commerce (EC Directive) Regulations 2002, SI 2002 No 2013.} \item\footnote{Ibid.} \item\footnote{Ibid.}
\end{itemize}}
courts by the application of common law principles seen in *Spencer v Harding*,\(^ {124}\) *Partridge v Crittenden*,\(^ {125}\) *Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd*,\(^ {126}\) *Grainger & Sons v Gough*,\(^ {127}\) *Thornton v Shoe Lane Parking Ltd*.\(^ {128}\) Consequently, it only provides a provisional and partial solution by merely specifying technical steps which the service provider must adopt.

Unlike the electronic transaction laws of UK, the Australian legislation prescribes more specific provisions. Hence, this requirement can help in minimising the issues in a better manner although it is not completely satisfactory.

Under the regulation the parties who are not consumers are free to decide not to apply regulation 9 (1) and (2) to their contract. Therefore, it suffers from limitation. Regulation 9 (3) requires the service providers to provide the terms and condition applicable to the contact in a form which can be stored and reproduced. It should be noted that, it does not explain how the terms must be provided in a form which can be stored and reproduced and leaves scope for ambiguity. As a result, this requirement can add another layer of uncertainty in terms of advertisements made available through automatic websites which can be updated easily.\(^ {129}\)

The criteria prescribed under the electronic transaction laws of UK differ from the Australian electronic transaction legislation.\(^ {130}\) Unlike in the UK, the Australian legislation provides guidance regarding invitation to treat although it has some shortcomings as identified in the previous section.

4.4.1 Position in the UK and Errors

The *Electronic communication Act* 2000 (UK) has side stepped the issues of input errors although it intends to facilitate the formation of electronic contracts.\(^ {131}\) On the

---

\(^{124}\) *Spencer v Harding* (1870) LR 5 CP 561.  
\(^{125}\) *Partridge v Crittenden* (1968) 2 All ER 421.  
\(^{126}\) *Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd* (1953) 1 QB 401.  
\(^{127}\) *Grainger & Sons v Gough* (1896) AC 325, 334.  
\(^{128}\) *Thornton v Shoe Lane Parking Ltd* (1971) 2 QB 163, 174.  
\(^{130}\) *Electronic Transaction Act 2000* (Vic) s 13.  
\(^{131}\) *Electronic Communications Act 2000* (UK).
other hand, the Electronic Commerce (EC Directive) Regulations 2002 has vaguely addressed the issue of input errors. The regulation does not provide specific contract formation provisions. However, Regulation 12 talks about contractual offers by specifying that under Regulation 9 (1) (c) and Regulation 11 (1) (b) the ‘order’ will be a contractual offer. Under the Regulation, the order is deemed to be a contractual offer therefore the regulation provides opportunity for correcting errors before an offer is made. Consequently, under the regulation the service providers must make available to the recipients ‘appropriate, effective and accessible technical means’ for correcting input errors which could allow the recipient to correct input error before the order is placed. However, the regulation does not explain what amounts to ‘appropriate, effective and accessible technical means.’ This can lead to concerns in relation to electronic contracts especially because the underlying technology of online transaction itself is prone to make errors. As a practical matter, different types of errors can arise such as bulk purchases may exceed the tax calculation limit of the software. Further, tax calculation errors, shipping cost calculation errors of the product can also occur. Neither the Electronic Communications Act 2000 nor the Electronic Commerce (EC Directive) Regulations 2002 attempt to resolve these novel issues raised by electronic contracts.

Although the regulation acknowledges input errors it only provides means for correcting input errors before the order is placed. It disregards the fact that the computer system may not always provide an opportunity to correct input errors before placement of order. For instance, errors associated with incorrect quantity fields of a shopping cart may not provide an opportunity to the buyer to correct the error rendering the data entry final. The regulation is primarily concerned with input errors made by human beings. Various technical errors such loss of data stores on the server, clipping of addresses stored on the data base fall beyond the scope of the regulation. In addition, the scope of Regulation 11 is limited as it does not apply to contracts concluded solely by email or other equivalent technologies.

---

134 Ibid.
135 Ibid.
136 Ibid.
if the service provider fails to provide means for correcting input errors a customer can rescind the contact.\textsuperscript{137} This places an unreasonable burden upon the vendors.

\section*{4.5 Position in the US and Invitation to Treat}

Like the model law, UETA focuses primarily on removing traditional barriers to enable formation of electronic contracts.\textsuperscript{138} However, the terms used under the Act and the model law differ slightly. The model law makes references to ‘data messages’, while UETA refers to ‘electronic records’ under s 3(a) of the Act.\textsuperscript{139} UETA is broad and it creates stability for electronic transactions. Like the Australian Legislation, UETA does not change the traditional legal principles, instead it establishes equivalence between traditional and electronic transactions.\textsuperscript{140} Section 3 of UETA states that the Act applies to electronic records as well as electronic signatures in their relation to a transaction.\textsuperscript{141} The term ‘transaction’ is defined as:\textsuperscript{142}

\begin{quote}
\textbf{an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.}
\end{quote}

Section 7(b) of the of the Act deals with formation of contracts and states:\textsuperscript{143}

\begin{quote}
A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
\end{quote}

The legislation not only recognises contracts formed through electronic means but also acknowledges the differences between electronic and paper-based media by specifically referring to electronic records.\textsuperscript{144} Although s 7(b) takes into account electronic media-based differences of electronic contracts and deals with contract formation, it was not intended to deal with all the aspects of contract formation such

\begin{thebibliography}{9}
\bibitem{137} Ibid.
\bibitem{139} Boss, above n 138, 304.
\bibitem{141} Uniform Electronic Transactions Act 1999, § 3.
\bibitem{142} Ibid, § 2(16).
\bibitem{143} Ibid, § 7.
\bibitem{144} Ibid, § 7.
\end{thebibliography}
as offer, acceptance and invitation to treat and leave scope for the application of traditional principles.  

4.5.1 Position in the US and Errors

The UETA has also made an attempt to resolve the issue of mistake in an online context. Under the legislation, a consumer will not be regarded as bound if the mistake was caused due to electronic error in relation to automatic transactions. An electronic error is defined as ‘ an error in an electronic message created by a consumer using an information processing system if a reasonable method to detect and correct or avoid the error was not provided’. It allows the consumer to avoid the effect of mistake by notifying the other party promptly after knowing about the error. It also allows the consumer to take reasonable steps to avoid the error. In relation to errors caused due to security procedures UETA states:

If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the non conforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

This provision allows the transacting parties to correct the error if the error is caused due to security procedure. It deals with any transmission where the parties have agreed to use some security procedure for the purpose of detecting errors. This provisions works against the non conforming party. It requires the party in the best position to avoid the change or error regardless of whether that person is the sender or the recipient. It is broad enough to cover both the errors made by the machines as well as man made errors. Under the Act the traditional common law rules will be applied if the error cannot be detected with the help of a security procedure.  

The UETA acknowledges the technological developments more precisely unlike the Australian legislation. For instance, the term security procedure is defined as follows:\textsuperscript{147}

“security procedure” means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The includes procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgement procedures.

However, although it acknowledge technical features of security procedures more precisely, it can create ambiguity regarding reasonableness of the security procedure used and is therefore, inadequate.

4.6 Conclusion

The chapter determined the extent to which traditional contract principles are applicable to electronic contracts in an effective manner. The discussion provided valuable insights regarding the applicability of traditional contract principles to electronic contracts. The overall discussion of the chapter leads to the consideration of deficiencies in relation to invitation to treat and electronic mistakes. The common key deficiency that emerged from the analysis is that the traditional contract principles cannot always be adequately applied to electronic contracts. Analysis also indicated that the traditional law is displaced when applied to electronic contracts.

In this regard, traditional contract principles when applied to electronic contracts can cause difficulties due to the unique features of electronic contracts. Automatic websites which allow customers to download music and books appear to be irrevocable as seen in \textit{Thornton v Shoe Lane Parking Ltd}.\textsuperscript{148} In addition, websites which control the actions of a customer significantly by making the transaction time bound do not provide much scope for a customer to negotiate the contract like a vending machine. Automatic websites resemble vending machines strongly but also

\textsuperscript{147} Uniform Electronic Transactions Act 1999.
\textsuperscript{148} Thornton v Shoe Lane Parking Ltd (1971) 2 QB 163, 174.
slightly differ from automatic websites in both content and functionality. Vending machines are usually used only for cheap disposal items unlike websites which are used for expensive products like laptops. Vending machines carry out the transaction by merely making the selected product available to the customer. While, automatic websites carry out more advanced functions by making decisions such as issuing discount coupons, issuing special product vouchers. Further, through vending machines direct physical selection of products is made unlike web based transactions which are carried out remotely. Due to these difference web based transactions provide scope for more errors.

The principles of unilateral mistake will also not be of much help to the vendors for terminating the contract. Traditional contract law does not provide clear-cut principles in relation to electronic contracts. If online websites are always regarded as offers instead of invitation to treat, then the online vendor may be exposed to the risk of an unanticipated number of acceptances. This risk is increased due to the global nature of the internet. Therefore, the traditional principles in relation to invitation to treat may need reconsideration in the online context.

The chapter then examined the impact of the Electronic Transaction Legislation of Australia. The analysis indicated that the legislation has not resolved the issues left unresolved under the traditional laws. Over all, Electronic Transaction Legislation of Australia which mirrors the international principles is also inadequate. The chapter examined the legal effect of electronic contracts by also doing a comparative analysis of the laws of Australia, the UK and the US. This chapter submits that the influence of technology and international and national developments has led to the development of different approaches. Comparative analysis of the laws of Australia, the UK and the US indicate that the laws of the UK and the US have fallen behind. The laws of the UK and the US lack precise criteria dealing with invitation to treat and electronic mistakes. Although they acknowledge technical features of electronic contracts they contain ambiguous technical terms that provides limited relief and creates confusion.
This chapter identifies the gaps that arise when traditional contract principles are applied to electronic contracts. The next chapter will analyse the issues that arise under other traditional laws, difficulties posed by traditional contract law are also further emphasised in the next chapter.
CHAPTER 5
ENFORCEABILITY OF ELECTRONIC CONTRACTS: ISSUE OF TIME AND PLACE OF CONTRACT FORMATION

5.1 Introduction
5.2 Acceptance
5.2.1 Postal Rule and Electronic Contracts
5.3.2.1 Instantaneous Communication
5.3.2.2 Time of Contract Formation and Jurisdiction
5.3.2.2.1 Time and Place of contract formation
5.4 Electronic Transaction Legislation of Australia: Time of Contract formation and Australia’s response to international norms
5.4.1 Technical aspects and the Electronic Transactions Legislation
5.4.1.2 Time of Receipt: Australia
5.5 Time and place of Contract Formation: Position in the UK
5.6 Time and place of Contract Formation: Position in the US
5.7 Conclusion

5.1 Introduction

Chapter four assessed the issues dealing with invitation to treat and mistakes under both the common law principles and the Electronic Transaction Legislation of Australia. This chapter advances the argument by evaluating the issues associated with time and place of contract formation. The aim of this Chapter is to identify the main factors that may be creating uncertainty in relation to time and place of contract formation. The chapter does not attempt to find solutions to the issues. It discusses the application of general principles of contract law to electronic contracts. The basic elements of a contract such as acceptance and postal acceptance rule are examined. The discussion will then proceed to evaluate the effect of regulatory measures on the contact formation process. The Chapter also assess the manner in which Australia has responded to the international developments examined in chapter two and
three. This thesis focuses specifically on Australian law. The Laws of the US and the UK is carried out only to gain addition insights.

5.2 Acceptance

Under the general principles of the law of contract, a contract is formed at the time and place where an acceptance is communicated to the offeror.\(^1\) In order to displace the normal rule of acceptance, the offer must clearly state the intention of the offeror.\(^2\) The terms of the offer may provide details of the form and mode of acceptance such as an offer must be accepted by sending a return facsimile by a certain date. An acceptance will be valid only if it complies with the terms of the offer and the stipulated mode of acceptance is adopted. However, if a non-stipulated mode of acceptance is adopted and if it turns out to be more advantageous to the offeror, the acceptance may still be valid.\(^3\) If an offeror makes an offer by a fax then, it is an implied indication that the offeror expects a prompt reply and an acceptance by a regular mail will not be sufficient.\(^4\)

Further, an acceptance of an offer must be communicated unless the offeror waives the right to be notified of an acceptance as seen in *Carlill v Carabolic Smoke Ball Co.*\(^5\) Such waivers are found in unilateral contracts, which are mostly seen in reward case. In these cases, the offeror is interested in performance of the contract rather than its formal acceptance. The performance then constitutes acceptance of an offer whether the offeror is aware of the acceptance or not.\(^6\)

It is noteworthy that determination of the precise time of contract formation is necessary both from the perspective of the revocation of offer as well as the determination of place of contract formation.\(^7\) Once an offer has been accepted it

\(^1\) Tallerman and Co Pty Ltd v Nathan’s Merchandise (Vic) Pty Ltd (1957) 98 CLR 93.
\(^2\) Latec Finance Pty Ltd v Knight (1969) 2 NSWR 79.
\(^4\) Quenerduaine v Cole (1883) 32 WR 185; Carter, Peden and Tolhurst, above n 3, 59.
\(^5\) *Carlill v Carabolic Smoke Ball Co.* [1893] 1QB 256.
\(^6\) Graw, above n 3, 460–461.
becomes irrevocable.\(^8\) Accordingly, up until the point of time that the offer has been accepted and a contract is formed, the offeror is free to withdraw the offer. Time of contract formation also indicates the moment of transfer of ownership and risks between the parties. Moreover, determination of time will be necessary in situations when there are competing acceptances.\(^9\) It can also have an impact on the terms of the contract. The terms and conditions which are included in a contract after the formation of a contract will not be regarded as enforceable.\(^10\) Online web sites can be updated easily. Therefore, if the time of contract formation is not determined, then it can provide scope for a vendor to claim that the users are bound by terms added to the site after the formation of the contract. For example, *eBay International AG v Creative Festival Entertainment Pty Ltd,*\(^11\) which involved the online sale of tickets highlights this issue. In *eBay International AG v Creative Festival Entertainment Pty Ltd*\(^12\) Rares J considered the conditions that applied to the resale of tickets for the *Big Day Out* music festival held in different locations in Australia between January and February 2007. The issue was whether Creative Festival had contravened s 52 of the *Trade Practices Act 1974* (Cth) by including among the conditions of sale printed on the back of the tickets for the events of 2007, Condition 6. Condition 6 stated that all *Big Day Out* Tickets that were resold for profit would be cancelled and the holders of such resold tickets would be refused entry. In order to ascertain whether the representations made in Condition 6 printed on the ticket were misleading or deceptive and/or likely to mislead or deceive in trade or commerce, the court was required to determine first of all, the conditions on which the tickets were being sold. The tickets were not only sold over the counter but also sold direct online from the *Big Day Out* website and the Ticketmaster website. Rares J described website user’s experience as follows:\(^13\)

A purchaser would enter the *Big Day Out* website. A webpage appeared which offered the facility of buying tickets online by clicking on a link. The same page of the website also had a link for opening up the terms and conditions of buying tickets online. If one clicked on the button to buy tickets, the purchaser was then

---

\(^{8}\) *Great Northern Railway Co v Witham* (1873) LR 9 CP 16.


\(^{10}\) *Olley v Marlborough Court* (1949) 1 KB 532.

\(^{11}\) *eBay International AG v Creative Festival Entertainment Pty Ltd*, FCA 1768, 28 (2006).

\(^{12}\) *eBay International AG v Creative Festival Entertainment Pty Ltd* (2006) FCA 1768.

\(^{13}\) Ibid 11, 231.
redirected seamlessly and unnoticeably to [Creative’s agent] Online Fulfilment’s website. And, it is on the latter website that the transaction which resulted in the dispatch of a ticket was completed...

...The webpage indicated that the order had been confirmed for the relevant ticket(s), the price had been successfully charged to the nominated credit card account and the ticket(s) would be mailed to the address given by the purchaser. An email was sent immediately following this which confirmed that the order had been successfully charged to the credit card and would now be processed and tickets mailed to the purchaser.

Rares J also held that\(^\text{14}\) a contract for the purchase of Big Day Out tickets was made on the terms displayed on the Big Day Out website. The contract was formed only after the customer clicked on the buttons agreeing to the terms and conditions and provided details of credit card and also other details and clicked on the ‘Send this Order’ button. The ticket was sold on the basis of the terms and conditions that appeared on five successive web pages on the Big Day Out website that had to be accessed by the customer to buy a ticket online. After a detailed review of the steps involved in the process of purchase of ticket on the Ticketmaster website, Rares J held\(^\text{15}\) that the online transaction was a contract for purchase of the tickets, in writing and signed by the parties. Accordingly, the contract was formed when the purchaser clicked on the ‘Purchase Tickets’ button on the website of Ticketmaster, subject to credit card approval and verification of billing address. During the entire process, the purchaser was unable to access any information that set out any of the conditions on the ticket or on the Big Day Out website. An online purchaser of the ticket was unable to see new Condition 6 until the tickets were received and the process took over six weeks after completion of the transaction online.

Finally, Rares J concluded that Condition 6, as it appeared on the tickets that were sent to the purchasers did not apply to any tickets purchased through Ticketmaster website or to purchases made through the Big Day Out website prior to 8 November 2006 (when the website was updated to include the new version of Condition 6)\(^\text{16}\)

\(^{14}\) Ibid 27.
\(^{15}\) Ibid 44.
\(^{16}\) Ibid 28, 52.
Rares J also held that Condition 6 on the tickets did not have contractual force and it was not relevant to the contracts under which the tickets were purchased. Thus, by sending tickets including Condition 6, Creative had made false representation in trade or commerce, which indicated that it formed a part of the contract under which tickets were purchased and was effective as a condition of sale. Therefore, the representations as to future matters contained in Condition 6 of the Big Day Out tickets contravened s 52 of the Trade Practices Act 1974 (Cth).

In order to establish consensus ad idem [meeting of minds] and an agreement, it is not enough if one of the parties agree to the offer but fails to communicate acceptance to the other party. For a binding contract to exist, it is essential to demonstrate that an acceptance of an offer was actually communicated to the other party or the offeror. Once actual communication takes place, then it is easier to establish that both the parties have consented and there is mutual assent regarding the contents of the contract and the two minds have come together and understood the terms of the contract in the same way as the other party. Under the traditional contract law it is not clear when acceptance in an electronic contract takes place. The issue is when it can be said that the acceptance was communicated. For example if an offer is sent by an email, is the acceptance made when the seller presses the sent button or when the email leaves the seller’s server or when it enters the buyer’s mail server or when the buyer actually reads the email. Similarly, with regards to automatic shopping websites there a number of issues such as how should acceptance be communicated? Is an online merchant expected to email formal acceptance to the customer? If so, when does communication of acceptance occur?

Acceptance can be communicated by an unequivocal act which evidences an intention to accept the offer such as debiting the customer’s credit card or account with the price or dispatching the goods. However, such acts pose problems because

---

17 Ibid 28.
an offer may be withdrawn any time before an acceptance is notified. If acceptance occurs by debiting the customer’s account or credit card then, such acceptance will not be notified to the customer until the customer becomes aware or until the next monthly credit card or account statement is provided to the customer. Similarly, when goods are dispatched communication of acceptance will not occur until the goods arrive and if the customer decides to revoke the offer, then the customer may refuse to accept the goods or services when they are delivered to the customer. Hence, some form of electronic notification may avoid such a situation and the online merchant will construct the website in such a way that it will generate and provide the customer with a formal notification that the customer’s offer has been accepted. In order to avoid any controversies the website must generate and provide the customer with a booking or reference number to allow the transaction to be traced in case of any dispute. Email confirmation can also act as a back up notification. However, automatic email confirmation and automatic web based notifications will bind the vendors even if there are pricing errors thereby creating problems as discussed in chapter four.

In most case, the acceptance may occurs when the online merchant sends the email. However, this aspect creates evidentiary problems when a dispute arises because it is difficult for an online merchant to prove that the customer opened and read the emailed acceptance. The email “Return receipt” function may assist to some extent, but it only acknowledges that the message has been received by the recipient and it does not prove that the intended recipient has read the message. Therefore, this approach provides significant scope for a customer to revoke the offer.

Partly, problem is caused due to the nature of electronic communication itself. Electronic communication differs significantly from traditional form of communication. Devices such as phone, telex or fax only have one machine at each side of the communication channel. In relation to these devices communication is made from phone to phone or fax to fax. Most electronic communications are based on the client-server mechanism. With regards to email there are at least two originating devices that is the sender’s mail client and the outgoing mail-server and

---

20 Graw, above n 3, 460–462.
21 Ibid 460–461.
two terminating devices the receiver’s incoming mail-server and the mail-client. Mail servers transfer messages along the transmission path, while the mail clients are the final destination devices of the email. Messages are pulled from the mail server by mail clients. This function is usually performed manually. Messages are pulled periodically in this manner. Immediate session does not take place between the mail client and the mail server. Transmission between the mail servers takes place almost immediately. However immediate transmission does not take place between the mail client. The issue therefore arises as to what should be taken into account for determining the acceptance. Should it be the mail-client or the mail-server? The decision will have vital impact on determination of time of contract formation as there can be substantial delays between the time a message arrives at the server and the time it is transferred to the client.

The issue is further complicated as the electronic communication involves multiple intermediaries. The position of internet service providers (ISPs) which underlie the communication channel and provide the infrastructure used by the contracting parties may be difficult to evaluate. In relation to determination of time of contract formation issue can arise as to whether the message should enter the receivers network or barely leave the senders network. Further, an email may reach an electronic address or certain computer network but may be rejected due to security measure adopted and could never become retrievable. This could happen due to spam filters, firewalls and antivirus software’s operating at various points in the network. Further mail server can also crash due to which email may not reach its destination.

Thus, there can be substantial differences in the time of formation of contract depending on whether a message reaches the receiver, enters a network or becomes accessible. Acceptance must be actually communicated to the offeror. However, the postal rule is an exception to this general rule. The following section analyses different case laws to determine how the general rule of acceptance and postal

---


23 Ibid.

24 Ibid.

25 Christensen et al, above n 7.
acceptance rule is applied to more traditional forms of communications such as telex, fax and telegram.

5.2.1 Postal Rule and Electronic Contracts

The postal acceptance rule was created to overcome the difficulties associated with postal negotiations and to overcome the separation of parties by time and distance. It is an accepted fact that there is a delay between the posting of a letter and the arrival of the letter at the intended address of the recipient. Parties who dealt with postal acceptance did not consider themselves bound by the contract until they had received confirmation of receipt of their correspondence by the other, thus leading to uncertainty.  

According to the postal rule, where acceptance by mail is contemplated by those involved in a transaction, acceptance will be deemed to be complete as soon as the letter is posted appropriately. The postal rule is excluded if a more instantaneous form of communication is used during the negotiations of a contract. Therefore, the time and place of acceptance and formation of contract occurs at the time and place of posting of the letter.

The postal acceptance rule has also been extended to other delayed forms of communications such as telegram. Traditional case law distinguishes between delayed forms of communications such as the telegram from instantaneous communications such as telephone. The term ‘instantaneous communication covers means of communication, such as telephone, where a person will know instantly, whether the communication was unsuccessful. An analysis of case law has been carried out in the following section to determine whether postal acceptance rule can be applied to electronic contracts.

5.2.1.1 Instantaneous Communication

26 Adam v Lindsell (1818) 106 ER 250, 251.
27 Ibid 250.
28 Ibid 251.
The modern rule regarding instantaneous communications has its roots in the English case *Entores Ltd v Miles Far East Corporation*. If an instantaneous means of communication is used like telephone or fax contract is formed when the acceptance is received by the offeror. Lord Dening in this case stated:

.... my conclusion is that the rule about instantaneous communications between parties is different from the rule about post. The contract is only complete when the acceptance is received by the offeror and the contract is made at the place where the acceptance is received.

The principle laid down in *Entores Ltd v Miles Far East Corporation*, about using new technology has been widely accepted and applied in a number of cases related to acceptance. It has been accepted as Australian law it has been applied where an acceptance was made by telephone such as in *Aviet v Smith & Searls Pty Ltd.* and by telex in *Leach Nominees Pty Ltd v Walter Wright Pty Ltd*.

Telex has also been recognised as an instantaneous mode of communication in *Express Airways v Port Augusta Air Services*, *Mendelson Zeller Co Inc v T & C Providores*, and in *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH*. Despite the fact that a telex may not be completely instantaneous, the court has recognised that both the offeror and the offeree must be regarded for all the intents and the purposes as being in each other’s presence.

However, in *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH*, the rule was slightly modified. According to Lord Wilberforce, the situation may be different where the message is sent or received by a third party and where it is sent...
outside the office hours if it is not intended to be read immediately. 40 Lord Wilberforce stated that the rule can be modified as follows:41

The message may not reach, or be intended to reach, the designated recipient immediately. Messages may be sent out of office hours or at night, with the intention, or upon the assumption that they will be read at a later time. There may be some error or default at the recipients end which may prevent receipt at the time contemplated and believed by the sender. The message might have been sent and/or received through machines operated by third person. And any other variations may occur. No universal rule can cover all such cases; they must be resolved by reference to the intentions of the parties, by sound business practice and in some case by a judgment where the risks should lie.

Lord Wilberforce noted that, no universal rule could cover all the cases. Those cases need to be resolved by taking into consideration the intention of the parties, business practice etc. 97 Thus, this case left scope for different variants. It seems from this that the communication must be regarded as received at the time when the acceptor could have reasonably been expected to have read it. It turns on what appears to be reasonable in all the circumstances. However, this approach is clearly advantageous to the person making the acceptance as it enables acceptance to take place even if the person who makes the offer remains unaware of it due to his failure to check incoming messages within a reasonable time. This problem does not seem to fit comfortably within the traditional approach of identifying agreement. It appears that the courts are not concerned with the mechanism of offer and acceptance instead they are concerned about the point at which acceptance is made within a reasonable time.42

41 Per Lord Wilberforce, Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH (1983] 2 AC 34, 41–42.

164
It is now established that the postal rule will not apply to the communications sent by telephone, telex and facsimile. However, in relation to other means of communication, such as instant chat message, interactive websites and automatic websites that are received by the parties immediately, postal rule may not apply. Postal rule may apply to non interactive websites which only provide product details and acceptance takes place by postal delivery. However, some interactive websites and automatic websites use email as a mode of communication to send confirmation email regarding the transaction to the customer or an email saying dispatch has been made is sent to the customer. It is not clear whether the postal rule applies to electronic communications such as emails. This is because the transmission speed of email communications is relatively slower than traditional instantaneous communications such as the telephone. The acts of contracting parties can also cause delays such as entering incorrect address or delay in accessing emails. Emails allow for the confirmation that the email has been sent, which exceeds the knowledge available when messages are sent through post.

Even if it is accepted that the postal rule is not applicable to email, interactive websites and automatic websites and that the acceptance occurs when the message is received, there is an ongoing debate regarding, when communication to the other party actually occurs. Thus, a bigger problem arises in case of electronic communications such as emails.


46 Ibid.

communication. Although email can be argued to be quick like fax and telex it does not signal its receipt like fax, telex and telephone. Cases such as *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH*\(^48\) appear to have adopted the position that if the offeree uses a permissible method of indicating acceptance and does everything to ensure that the acceptance is communicated then the risk that it is not communicated lies with the offeror. This rule is called the deemed receipt rule. It is analysed in the following section to assess its application to emails and websites.\(^49\)

5.2.1.2 Deemed Receipt Rule

The common law has adopted certain rules in relation to instantaneous communication. In an instantaneous communication mode, the actual communication rule applies, where the offeror must actually receive and read or hear the acceptance for a contract to be formed. It is the receipt and not just the arrival of acceptance at the offeror’s machine that is relevant time or moment for the formation of a contract. Hence, it would be unreasonable for a recipient to avoid or delay contractual obligations merely because the recipient deliberately avoided actual receipt of an acceptance or its communication or actual communication was not possible because the recipient’s machine was not maintained properly and was not in a position to receive the message. The common law has considered these options with respect to the more traditional forms of communication and adopted a deemed receipt rule. Thus, a recipient who does not receive a message on time or does not receive the message at all because of poor business practices regarding checking correspondence, deliberate evasion, faulty machine or any other reason for which the recipient is responsible, will not be able to avoid or delay the moment of acceptance as seen in *Entores Ltd v. Miles Far East Corporation*\(^50\) and *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH*.\(^51\) In *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH* Lord Fraser explained this as follows:\(^52\)

\(^{48}\) *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH* (1983) 2 AC 34.

\(^{49}\) Christensen et al, above n 7, 11–3; Clark, above n 43.

\(^{50}\) *Entores Ltd v. Miles Far East Corporation* (1955) 2 All ER 493.

\(^{51}\) *Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34.

\(^{52}\) Ibid per Lord Fraser, 43.
once a message has been received on the offer’s telex machine, it is not unreasonable to treat it as delivered to the principle offeror, because it is his responsibility to arrange for prompt handling of messages within his own office.

In a communication, if the sender such as offeree or acceptor sends a message and assumes that, it has been sent or transmitted successfully but the message has not been received or its receipt has been delayed due to the fault of the receiver or offeror, then at law the receiver or offeror is stopped from denying that they have not received the message as seen in *Entores Ltd v. Miles Far East Corporation.*\(^{54}\) This principle will apply only if it is reasonable to expect receipt it will not apply if it is unreasonable.

Under the deemed receipt rule, the relevant moment for receipt is the time acceptance would come to the knowledge or attention of the recipient on its arrival during the normal course of business as seen in *Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)*\(^{55}\) Thus, the moment is not necessarily the moment when the machine receives the acceptance of the message but the moment the recipient becomes aware of the acceptance or the message during the normal course of business. In *Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)* Megaw LJ explained it as follows:\(^{56}\)

> If a notice arrives at the address of the person to be notified, at such time and by such means of communication of that person on it arrival, that person cannot rely on some failure of himself or his servants to act in a normal businesslike manner in respect of taking cognisance of the communication, so as to postpone the effective time of the notice until some later time when in fact it came to his attention

Thus the deemed receipt rule does not displace the need for actual communication in the manner in which the postal acceptance rule does. Hence the actual receipt at the designated location of correspondence of the offeror or recipient is still considered as

---

53 Hill, above n 47, 151; Hill, above n 18.
54 *Entores Ltd v. Miles Far East Corporation* (1955) 2 All ER 493.
55 *Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)* [1974] 3 All ER 88, per Edmund Davies LJ at 96 and per Megaw LJ at 113.
the relevant moment.\textsuperscript{57} In \textit{Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)}\textsuperscript{58} telex was considered as reasonably received when it was reproduced in the office during office hours. Edmun Davies LJ was of the view that:\textsuperscript{59}

A telex is received when the message is physically reproduced in the recipient’s office during office hours.

Similarly in NSW Supreme Court case \textit{NM Superannuation Pty Ltd v Baker} fax was considered as reasonably received when the fax machine was left on in the office and there were people in the office.\textsuperscript{60}

In any case there is no reason why I should assume that the trustee through its employees or agents was not in its office at 5.22 pm on 30 June 1989 or on any other business day in the ordinary course of its business. I cannot take judicial notice that people are not normally at work between 5 pm and 5.30 pm and there is no evidence which would suggest that the trustee through its representatives was not present at that time. It may well be in appropriate circumstances that evidence could be given that notwithstanding that a facsimile machine is left in operation there was nobody in the office to receive the message until the following day but that is not the case here.

For electronic contract, formed through email and website what should be regarded as office hours? Due to lack of territorial boundaries office hours can be claimed to be twenty four hours a day. If email acceptance is regarded as received when it reaches the server acceptance will be effective on a twenty four hour basis. Such a situation will create a commercial nightmare. Why would offeror subject themselves to acceptance outside the normal offline business working hours? If this approach is adopted the rights and obligations of the parties may begin even when they are away from the office.\textsuperscript{61} Lord Denning further highlighted the point that if the offeror is at fault “offeror must be estopped from denying the receipt of acceptance where it

\begin{footnotes}
\item[57] Hill, above n 47, 151; Hill, above n 18.
\item[58] \textit{Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)} [1974] 3 All ER 88, per Edmund Davies LJ at 96 and per Megaw LJ at 113.
\item[59] \textit{Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes)} [1975] QB 928, per Edmun Davies LJ (para 4).
\item[60] \textit{NM Superannuation Pty Ltd v Baker} [1927] ACSR 105 at 114–115.
\end{footnotes}
should be reasonable to expect him to ensure that the message is received.”

Then, based on the reasoning of Lord Denning, offerors communicating through email will be responsible for prompt handling of messages even outside the offline business hours. It will therefore be the responsibility of the recipient to avoid the risk of delay by maintaining the machine and checking the messages. If the correspondence by email is delayed or did not reach the offeror because the offeror did not maintain their server or because they failed to log in or check emails, they will be estopped from denying the receipt of acceptance.

Similarly, if office hours of an automatic website is regarded as twenty four hours a day acceptance will be effective as soon as it arrives on the vendor’s website. Then, vendor will be bound by the contract even if there are inventory errors. In such a situation there will be delay in shipping the order or the order will never be delivered.

However, if products made available through interactive websites are regarded as invitation to treat vendors of a website will send acceptance to the customers. In such a scenario what should be regarded as customer’s office and office hours? Traditional means of communications such as telex, fax and telephone are confined to office or home of a person unlike websites and emails which can be accessed from anywhere. Additionally, traditional devices have single accessible devices unlike websites and emails which have multiple accessible devices. A person will be more in control of traditional means of communication and can promptly handle communication with less difficulty. In traditional means of communication receipt of a message is usually delayed due to the act of transacting parties unlike email and web based communication where a message can get delayed due to the acts of third parties such as virus attacks.

---

64 Hill, above n 47, 151; Hill, above n 18.
Thus, traditional principles dealing with time of contract are displaced. The summary of the discussion paper has also expressed the need to keep up with technology as follows:\(^{66}\)

…Contract law also may need to adapt to new technologies and ways of doing business, such as electronic contracting.

In addition, the discussion paper has highlighted the impact of outdated legal framework as follows:\(^{67}\)

Rules which are out of step with current commercial practice and expectations undermine predictability because they can later emerge to surprise parties who have acted on the basis of common sense assumptions.

When electronic contracts are formed in an international scenario, determination of the specific time of contract formation can be important, both in relation to international trade or simple purchases made through the internet. Due to the geographical nature of internet determination of the time of contract formation will become necessary. Issues can arise about the time of receipt when such terms are provided by the website:\(^{68}\)

If Harvey Norman online gives you notice that it will be unable to deliver your order within 10 business days of receipt of your order, due to lack of stock, you may cancel your order without charge and Harvey Norman online will arrange for a full refund of any payment made by you to be processed.

Websites function on a twenty four hours basis if such terms are provided determination of ‘10 business days’ can be problematic due to the global nature of internet in international transactions. Similarly, issue of time of receipt can also arise when such terms are provided by the websites.\(^{69}\)

---


\(^{69}\) Slatterymedia <http://www.slatterymedia.com/termsofuse/>.
Due to the global nature of internet issue can arise regarding what amounts to ‘24 hours of ordering’ in international transactions? Determination of time will have a direct impact upon the price paid and rights and obligations of transacting parties.\(^{70}\) Determination of time of contract formation will also likely create problems especially in situations where a contract is open for a specific time\(^{71}\) as seen in *Bressan v Squires*.\(^{72}\) In this case Squires gave an option to Bressan to purchase a land by sending notice in writing at any time on or before 20\(^{th}\) December 1972. Notice was received on 21\(^{st}\) December. Bowen C.J concluded:\(^{73}\)

I think that what was required for due exercise was actual notice to the defendant on or before 20th December, 1972. Since actual notice was not received by the defendant until 21st December, 1972, the plaintiff must fail.

Similarly, determination of time was an important aspect in *Carrapetta v Rado*.\(^{74}\) In this case Barrett JA noted that:\(^{75}\)

...the responded had on 1 December 2011, served on the appellants a valid and effective notice to complete; that the service of the notice caused time to become of the essence of the contract so as to require completion on or before 16 December 2011; that the appellants defaulted in their to complete by that deadline; and that the respondent was thereby entitled to terminate the contract....

Overall, traditional contract principles dealing with time of contract formation are inadequate. There is a lack of one single rule applicable in different circumstances.

\(^{70}\) Hill, above n 47, 151; Hill, above n 18.
\(^{71}\) *Bressan v Squires* [1974] 2 NSWLR 460; *Smilie Pty Ltd v Bruce* (‘Smilie’) [1998] 8 BPR (Bryson J); [1998] 9 BPR 16723 (Court of Appeal), *Imperial Brothers Pty Ltd v Ronim Pty Ltd* [1999] 2Qd R 172.
\(^{72}\) *Bressan v Squires* [1974] 2 NSWLR 460.
\(^{73}\) Ibid.
\(^{74}\) *Carrapetta v Rado* [2012] NSWCA 202.
\(^{75}\) Ibid per Barrett JA, para 4.

…Some centuries-old common law rules of contract survive largely intact, attracting the criticism that the elements of Australian contract law are tried and inadequate to contemporary circumstances. It is worth considering whether the law could be better suited to the needs of today.


Australia’s contract law should support businesses in creating a culture of innovation, embracing technology and looking for new trading opportunities ….

There is lack of rule dealing with time of electronic contracts. Concerns expressed by the discussion paper seems correct. There is no rule that can automatically indicate the time of contract formation for electronic contracts.

5.3 Time and Place of Contract Formation

Internet websites offer goods and services that can be accessed by anyone from all over the world.\footnote{J Quek, ‘Jurisdiction and the Internet—Where Can Your Clients be Sued?’ (2006) 8(9) \textit{Internet Law Bulletin} 121.}{78} With regards to traditional forms of communications such as fax and post it can be easily determined where the sender and receiver are located. If a person provides fax numbers it can clearly be ascertained where the receipt will occur and where it is located. Conversely, when an email address is given it can be accessed from anywhere in the world. It is not confined to the work place of a
173

It is important, therefore, to be able to determine where the electronic contract was formed and hence, which country’s laws should govern the contract. Notably, the time of formation of the contract will also impact upon an analysis of where the contract has been formed. The relationship between time (when) and place (where) of contract formation was explained by Lord Denning LJ in *Entores Ltd v Miles Far East Corporations* as follows:

The contract is only complete when the acceptance is received by the offeror and the contract is made at the place where the acceptance is received.

Time and place of the formation of contract may be identified by considering when and where the contract is formed electronically. The time of formation of the contract or when the contract was formed is relevant in identifying the moment from which the parties have legal obligations to one another. It is the time that indicates from when the contract has come into existence and has become enforceable. The place or where an electronic contact is formed is relevant in establishing the jurisdiction where a dispute may be resolved in case of any disagreement or controversy between the transacting sides. For a court to have jurisdiction in relation to a contract dispute, the contract must be either 1) formed within its jurisdiction, 2) governed by the law of the forum or 3) broken within its jurisdiction. The first criteria is most relevant to the discussion being carried out in this chapter while the other criteria falls beyond the scope of this thesis.

When parties belonging to different jurisdictions enter into contract laws of several countries may be relevant to the issues arising under the contract. An Australian company dealing with a Japanese distributor may not like to file a case in a Japanese court due to the difference in legal systems.

---

79 Hill, above n 47, 151; Hill, above n 18.
80 Christensen et al, above n 7, 14–5.
81 *Byrne & Co v Leon Van Teinhoven & Co* (1880) 5 CPD 344.
82 *Entores Ltd v Miles Far East Corporation* [1955] EWCA Civ 3; [1955] 2 QB 327 per Lord Denning at 334.
84 Jew, above n 83.
In the light of the uniqueness of the internet, approach of using place of formation of contract as a basis to determine jurisdiction in a contract dispute can be argued to be inappropriate. Although a contract is formed where the last act essential to make the contract binding occurs (where the offeror receives the acceptance), this approach can be questioned. Based on this approach, in a situation where two parties arrive at an agreement after several counter offers the place of contract formation is determined only by coincidence.85

The issue of jurisdiction is established by the courts after considering if a contract has been formed in a particular place or country, so that the place has jurisdiction to resolve the dispute.86 There is no rule which can specifically indicate the place of contract formation for electronic contracts. Lack of specific rule regarding place of contract formation may result in uncertainty. The online merchant has an option to overcome the problems related to jurisdiction by inserting a specific provision regarding the governing law of the contract stating that the parties agree that in case of dispute, the laws of Victoria in Australia applies. Further, the website must also state the terms on which the contract is based and stipulate that in case of any disputes, the disputes must be determined by the courts and or tribunals of that jurisdiction. Websites are introduction jurisdictional provisions in the following manner:87

Both parties to this agreement specifically agree to submit to the exclusive jurisdiction of and venue in the courts of New South Wales Australia in any dispute arising out of or in relation to this agreement

However, contractual provisions which are included to remove uncertainty with regards to jurisdiction may not be always effective. Although the courts of most countries give effect to such clauses specifying the choice of law it does not amount to an agreement to submit to the jurisdiction of that country. It does not mean that the claims must be brought in that forum only. Although a contractual parties agreement, to submit to Australian jurisdiction, will be a relevant factor when deciding, whether

85 Svantesson, above n 83.
86 Hill, above n 47, 151; Hill, above n 18; Hill, above n 83.
Australia is the appropriate jurisdiction, it will not be the only decisive factor. Even if contractual parties agree to submit to the jurisdiction of a particular country, it may still be possible for one of the parties to obtain stay of proceedings or to bring action in another country. This can happen if it is established that the other country say England is the most appropriate jurisdiction for determining the dispute.\(^{88}\)

Despite the provisions regarding governing laws, there may be residual enforcement problems that may arise when an online merchant sues and obtains a judgment in Australia. Such an Australian judgment cannot be enforced in an overseas jurisdiction. The enforcement jurisdiction of courts is even more limited. Judgments of foreign countries are not always enforced by the courts of a particular country. This indicates the extreme of limited power of the courts with regards to enforcing judgments made against people residing in foreign jurisdiction. This generally happens in circumstances where the judgment is made in default of appearance of parties or if the defendant does not have asserts in a jurisdiction where the judgment was passed. Further, this can also happen if the person against whom the judgment is passed does not have any connection with the foreign state. In addition, states will not enforce matters involving taxation, criminal or other public laws.\(^{89}\) This issue was clearly illustrated by a French case.\(^{90}\) The French organisation sent a letter to Yhaoo's Headquarters located in United Sates of America (USA) which claimed that its auction services breached the French Laws. The French organisation also threatened to take action in France if its demands were not fulfilled. French Organisation claimed that since the contents of the website were also accessible in France it violated French laws. French Court held that it was possible to block the contents of the website through technological means. Since the contents of the website were viewed in France it came under the jurisdiction of French court. Yahoo was ordered to comply with the orders in the event of non compliance the Court

\(^{88}\) Jew, above n 83, 24, 24–29.


\(^{90}\) UEJF and LICRA v Yahoo Inc and Yahoo France <http://www.juriscom.net/\texttt{txt/jurisfr/cti/yauctions20000522.htm}\>; Yahoo!, Inc v La Ligue Contre Le Racisme et l’Antisémitisme et al., 169 F Supp 2d 1181.
sought to impose penalties. Yahoo obtained a declaratory judgment which held the court’s orders were not enforceable under the laws of USA.91

Hence, online merchants must consider these problems regarding electronic contracts while setting up their websites. In addition, it should be noted that any jurisdiction clause incorporated by means of click wrap agreements that limits or excludes the liability of the merchant must be unambiguous and brought to the notice of the customer. Unless the limiting and exclusion clauses are brought to the notice of the customer before the formation of an electronic contract, they do not become enforceable.92 Similar concerns regarding inadequacy of traditional contract law are reflected in the discussion paper exploring the scope for reforming Australian contract law as follows:93

In the case of cross-border Internet transactions, it will often be unclear what legal system is the governing law. Even if Australian law applies, there may be difficulties. Internet users are often presented with an on-screen list of terms and conditions and asked to click a box stating ‘I agree’. Alternatively, the terms and conditions for use of a website may be available somewhere on that site (often under a hyperlink) but the user is not expressly required to assent to them. In many such cases, it may be unclear whether a contract was even formed.

It appears that the fear of jurisdictional issues is forcing websites to limit their transactions within a particular territory. Some of the websites are limiting their ambit of transaction in the following manner:94

We can only deliver to addresses within United Kingdom


92 Graw, above n 3, 461–6. Insight, above n 87.


94 Voodoobikes <http://www.voodoobikes.co.uk/terms>.
A leading case dealing with the issue of jurisdiction in Australia is *Dow Jones & Co Inc v Gutnick*[^95] where a defamation action was brought against the online publishers. The High Court of Australia held that the material published online is deemed to have been published in the place it is viewed and not in the country of origin. Thus, in *Dow Jones and Company v. Gutnick*[^96] the High Court held that in relation to jurisdiction it is, where the publication of the defamatory statement was made available on the internet. Based on this case it can be argued that electronic contracts will normally be governed by the law of the place where the acceptance is received and the courts of the place of receipt will have jurisdiction to resolve any such dispute.[^97] However, this approach does not provide a decisive solution for determining the place of formation of electronic contracts. This approach is unsatisfactory in the light of the nature of websites. Websites are computer programmes residing on servers. Websites do not have a fixed location. Websites can be located on a server in Brasilia on one day and some other country the subsequent day. The same website can also be mirrored on different servers of the world. Further, a website can have its text content located on a server in one county and pictures stored on the server of another country. It is impossible for an average person to determine the location of a website. A vendor can also easily change service provides. Such a dispersal creates juridisdictional and enforcement issues. This portable feature of internet makes it significantly different from other communication channels. Internet does have geographical identifiers. The only information available will be the Internet Protocol address and a domain name. The domain name of a country cannot be regarded as a reliable geographical identified as any country can use the country code of other country. Internet protocol addresses also are not reliable geographical identifications.[^98] In case of interactive websites, automatic websites and emails contract formation takes place either on the webpage of the vendor or when acceptance is received at the server. In the light of the nature of internet and websites there can be multiple locations involved when acceptance takes place. Therefore determination of place of contract formation is problematic.

[^96]: Ibid.
[^98]: Squires, above n 45, 99–102.
Approach adopted in *Dow Jones and Company v. Gutnick*\(^9^9\) is unsatisfactory for electronic contracts. Precise place of formation of contract cannot be determined. There is lack of rule which can indicate specific place of formation of electronic contracts. The flaws of the decision in *Dow Jones and Company v. Gutnick*\(^1^0^0\) was highlighted by Justice Kirby in the following manner:\(^1^0^1\)

Internet publishing would be exposed to law suits anywhere in the world and it would be a concern particularly in cases where the plaintiff has a substantial reputation in more than one legal jurisdiction and seeks to recover for damages in all such jurisdictions in a single proceeding.

Based on the reasoning of Justice Kirby if the approach laid down in *Dow Jones and Company v. Gutnick*\(^1^0^2\) is adopted for determining place of contract formation, plaintiff can sue for same cause of action from different jurisdictions multiple times.

The infolet of the discussion paper further explains the impact of uncertain law on electronic commerce as follows:\(^1^0^3\)

Statistics suggest that there is a lower take-up of e-commerce in Australia than in other countries. In 2009-10, around 63 per cent of small businesses did not promote their products online, while around 76 per cent did not take orders over the Internet.

Part of the reason may be that small businesses and consumers are worried about their legal rights and their ability to enforce them if they make contracts online. If this is identified as a problem, contract law reform may offer one way to address it by making sure that our law adapts to new technologies and supports e-commerce.

The discussion paper has also stressed the need of certain law as a means of reducing business costs as follows:\(^1^0^4\)

---


\(^1^0^0\) Ibid.

\(^1^0^1\) Ibid para 152.

\(^1^0^2\) Ibid.


\(^1^0^4\) Attorney General’s Department, *Summary: Australian Contract Law Reform* <http://www.ag.gov.au/Consultationsreformsandreviews/Pages/Contract-Law-Discussion-
Improving certainty in those areas of contract law which are unsettled or unclear would have a number of benefits. When the legal consequences of actions or omissions are clear and predictable, individuals and businesses have the information they need to make informed choices and to develop long-term plans. Legal certainty also has important economic benefits such as allowing contracting parties to allocate risk more efficiently. Greater certainty in the law lessens the likelihood of disputes arising or being escalated, reducing costs both for parties and for governments.

It appears that legal certainty is essential for the continued development of electronic commerce. Traditional principles dealing with the place of contract formation are uncertain. Therefore, for the effective formation of electronic contracts legal intervention may be required.

5.4 Electronic Transaction Legislation of Australia: Time of Contract Formation and Australia’s Response to International Norms

The Electronic Transactions (Victoria) Amendment Act 2011 has made amendments to the time and place criteria of the Electronic Transactions (Victoria) Act 2000. The amendment was made to bring the time and place criteria into line with the United Nations Convention on the Use of Electronic Communications in International Contracts 2005. Under Article 3, the convention preserves autonomy of party in respect of matters relating to the time and place of dispatch.

---

The timing of the despatch of goods and its receipt is important regarding acceptance of a contract.

Under contract law, an agreement comes into existence as soon as communication of acceptance is made to the offeror.\(^{108}\) With respect to the application of the rule of acceptance, the position regarding communications by email has not yet been settled. Hence, the general rule applies, unless rebutted under particular circumstances by the parties.\(^{109}\)

The Convention fails to provide a rule regarding the exact timing of contract formation where electronic communications is used. Both the above common law rules can be applied if it is clarified as to when dispatch and receipt of communication has taken place. Thus, the Convention intends to facilitate communication in electronic contract without making any changes to traditional or domestic contract law.\(^{110}\) Accordingly, the consultation paper suggested:\(^{111}\)

(9) The default rules in the ETAs for timing or dispatch should be amended so that:
   (i) the ETAs’ formula for determining time of dispatch (‘when it enters an information system outside the control of the originator’) reflect instead the Convention’s formula (‘when it leaves an information system under the control of the originator’) and
   (ii) if the electronic communication has not left an information system under the control of the originator (e.g. where the parties exchange communications through the same information system or network) the time when the electronic communication is received.

(b) The default rules in the ETAs for timing of receipt should be amended so that:
   (i) 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 at an electronic address (an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee’s electronic address), and

---

\(^{108}\) Ibid para 5.2.
\(^{109}\) Ibid para 5.3.
\(^{110}\) Ibid para 5.4.
\(^{111}\) Ibid para 33.
(ii) 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.

(c) The rules in the ETAs for time and place of dispatch and receipt make it clear that the fact that an information system of an addressee is located in a jurisdiction other than that in which the addressee itself is located does not alter the application of the rules in articles 10.2(time) and 10.3(place) of the Convention.

The proposed amendments used clearer terms to indicate the exact timing of receipt and dispatch of communication that is made electronically. However, the provision does not significantly go beyond the *Electronic Transactions (Victoria) Act 2000*, as it only uses refined terms.\(^{112}\) Regarding electronic communication, it states:\(^{113}\)

> 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.

Although the criteria appear to be appropriate, under the criteria, ‘awareness’ can amount to both actual receipt by the receiver and just receipt of the message in the inbox.\(^{114}\) Hence, does not state whether the receiver must actually read the message or whether just the availability of the message in the inbox is sufficient. Therefore, issues seen *SZAEG & ORS v Minister For immigration*,\(^{115}\) *Piha Pty Ltd v Spiral Tube Makers Pty Ltd*,\(^{116}\) *Aristocrat Technologies Inc v IGT*,\(^{117}\) *American Express Australia Ltd  v Michaels*,\(^{118}\) *Sainju v Minister for Immigration and Citizenship and Another*,\(^{119}\) *Reed Constructions Pty Ltd v Eire Constructions Pty Ltd*\(^{120}\) still persist.

---

112 Ibid para 5.4.
113 Ibid para 30.
114 Ibid.
115 *SZAEG & ORS v Minister For immigration* [2003] FMCA 258.
118 *American Express Australia Ltd v Michaels* BC201000873.
120 *Reed Constructions Pty Ltd v Eire Constructions Pty Ltd* BC200906296.
Further, the recommendation stated that, the default rules under the *Electronic Transactions* (Victoria) Act 2000 should undergo an amendment, where it could be presumed that dispatch has occurred as soon as the communication has left the system of information that has been in the originator’s control.\textsuperscript{121} Although the amendments use refined criteria, there is lack of indicative factors to determine whether a particular system of information has been controlled by sender or receiver. Hence, significant uncertainty can arise as to what amounts to ‘control’ in relation to dispatch of the communication.\textsuperscript{122} The time of dispatch can only be ascertained if threshold requirement of ‘control’ is determined.\textsuperscript{123}

The *Electronic Transactions* (Victoria) Act 2000 and the *Electronic Transactions (Victoria) Amendment Act* 2011 will be jointly referred as Electronic Transaction Legislation of Australia for the discussion carried out below. The Electronic Transaction Legislation aims to modernize the law hence it is necessary to understand some technical aspects of commonly used recent technologies.

5.4.1 Technical Aspects and the Electronic Transactions Legislation

Cloud technology allows hosting of applications and documents into a cloud consisting of thousands of computers and servers which are linked together and accessible through the internet. Everything done on the computer through cloud technology is web based instead of being desktop based. Thus, desktop based documents and applications are moving into the cloud. People will no longer be tied up to a single computer located in the office as the data can be stored on the web and can be accessed from anywhere in the world.\textsuperscript{124}

\begin{footnotesize}
\begin{enumerate}
\item Ibid 27–8.
\end{enumerate}
\end{footnotesize}
Cloud computing encompasses multiple computers, multiple servers and multiple networks. In a layman’s language cloud is a collection of computers and servers which are accessible through the internet. A web based application or service offered via the internet is called cloud computing. It can include cloud based word processor, email and power point presentation.\textsuperscript{125}

Cloud computing can be seen as a collection of services. It can be described as a layered cloud computing architecture. Services offered through the internet usually consist of information technology services and is called SaaS (Software as a service). It allows software to be run remotely via a cloud. Infrastructure as service (IaaS) guarantees processing power, storage and internet access.\textsuperscript{126} Platform as a service (PaaS) provides platform to the developers to host web applications.\textsuperscript{127}

The Electronic Transactions Legislation merely provides default rules for determining the time of receipt and dispatch of messages. It enables the application of common law principles. It does not provide precise criteria for ascertaining time of contract formation.\textsuperscript{128}

Under the Electronic Transaction Legislation of Australia addressee is a person with whom originator intends to communicate. People who happen to just receive, copy or forward the message in the course of the communication are excluded from the definition of the addressee.\textsuperscript{129} Originator is the person who sends the communication. It differs from the definition of the addressee which focuses on the intent of the action. However, the definition of both addressee and originator cover natural persons, corporate bodies and legal entities.\textsuperscript{130}

Section 13 of the electronic transactions legislation deals with time of dispatch of an electronic message. Under section 13(1) (a) dispatch takes place when an electronic

\begin{itemize}
\item \textsuperscript{125} Ibid.
\item \textsuperscript{126} B Furht, \textit{Handbook of Cloud Computing} (2010) 5.
\item \textsuperscript{128} \textit{Electronic Transactions Bill 2011} (Vic) Explanatory Memorandum, 11; \textit{Electronic Transactions (Victoria) Amendment Act 2011}.
\item \textsuperscript{129} \textit{Electronic Transactions Bill 2011} (Vic) Explanatory Memorandum, 6.
\item \textsuperscript{130} Ibid; \textit{Electronic Transactions Act 2000} (Vic).
\end{itemize}
communication leaves the information system of the originator. The term ‘information system’ is defined as a system used for ‘generating, sending, receiving, storing or otherwise processing electronic communication’. The term electronic communication is defined as ‘a communication of information in the form of data text or image by means of guided or unguided electromagnetic energy’. The electronic transaction legislation does not explain what amounts to the ‘information system of the originator’. It is broad enough to encompass the server, web browser and the full communication network itself. The definition of the information system is broad enough to encompass IaaS, PaaS and DaaS of cloud technology.

There is lack of specific criteria describing what factors should be considered for determining dispatch. The criteria poses even more bigger problems in relation to mobile devices such as PDA (Personal Digital Assistant), laptops and mobile phones. Data is transferred to and forth between the mobile devices and cloud infrastructure in the following manner: 1) First data from a mobile hand held device is sent to cloud infrastructure. 2) Then the data is sent to the transmission tower. Section 13(1) (a) is broad enough to cover the entire transaction network consisting of cloud infrastructure and wireless transmitters. There is lack of a single specific criteria. Further, Cloud infrastructure does not adequately supports data transfer between portable devices as they require more memory space than devices such as PDAs. Further, they do not recognize many communication protocols. Therefore, due to these novel features communication can suffer significantly when transactions are conducted through mobile devices.

Under Section 13(1) (b) if the communication does not leave the information system of the originator then dispatch occurs when the communication is received by the addressee. According to the explanatory memorandum of the bill this criteria anticipates exchange of electronic communications within the same information

131 Electronic Transactions Act 2000 (Vic).
system. It does not tell whether the addressee must actually view the message or whether receipt of message at the inbox or server will amount to receipt. In parallel, Section 13 (1) (b) appears to be problematic as there can be firewalls, antivirus software’s which can prevent the message from reaching the addressee. Moreover, cloud computing infrastructure suffers from the issue of interoperable standards due to which receipt may never occur. Further, receipt may not occur if the system has access control list filters. There are traffic control filters used on routers which identify specific type of data and prevent it from passing through the network.

The issue is also complicated in relation to mobile phones. Mobile phone internet browsers have infinitely variable degree of support with regards to web pages and graphics. Therefore, criteria for receipt can create problems in relation to these devices especially if actual reading or viewing of the message is required under Section 13 (1) (b).

5.4.2 Time of Receipt: Australia

In relation to receipt the legislation provides different criteria for a designated information system (when a specific email address is provided for sending communication) and a non-designated information system (when a specific email address is not provided for sending communication). Hence, the time of receipt will vary depending upon whether there is a designated or non-designated information system.

Under Section 13A (1) time of receipt is the time when the electronic communication becomes capable of being retrieved by the addressee at a designated electronic

---

137 Electronic Transactions Bill 2011 (Vic) Explanatory Memorandum, 11–12.
142 Electronic Transactions (Victoria) Amendment Act 2011.
address. The legislation replaces the term ‘information system’ used while defining the criteria of dispatch with the term ‘electronic address’. Electronic address indicates the specific part of the information system which can be the email address or the Internet Protocol (IP) Address of cloud infrastructure. It is uncertain whether terminology is pointing towards the email address or the IP address of cloud infrastructure. In William Close Pty Ltd v City of Salisbury & Anor (No 2) the term designated information system was liberally interpreted and the receipt of email in the dead folder of the email account due to a mistake in the email header was regarded as entry into the designated information system. Similar, view was also expressed in Re David Scott Ellis; Ex Parte Triple M Mechanical Services Pty Ltd. However, given the broad definition of information system, with regards to cloud computing technology issue will arise as to which part of the infrastructure should be consider for determining receipt. For instance, in SZSKX v Minister for Immigration and Anor it was held that the facsimile was never capable of being retrieved as there was no log of actual receipt of the facsimile transmission on the information system which was designated. Similar view was also expressed in Liu and Ors v Minister for Immigration and Anor. While, in Thorn Airfield Lighting Pty Ltd v W it was held that the electronic transactions Act applies only if the parties have agreed to receive electronic communication.

Like Section 13 (1) (b) receipt will not occur under Section 13A (1) if firewalls, antivirus software’s and filters prevent the message from reaching the addressee. Difficulties may also arise if the message is received but in an unreadable form. Moreover, cloud computing infrastructure suffers from the issue of interoperable standards due to which receipt many never occur. In particular, Section 13A (1) will create problems in relation to online shopping transactions.

143 Ibid.
144 William Close Pty Ltd v City of Salisbury & Anor (No 2) [2012] SAERDC 26 (3 May 2012).
145 Re David Scott Ellis; Ex Parte Triple M Mechanical Services Pty Ltd [ No 2] [ 2013] WASC 161 (2 May 2013).
147 Liu and Ors v Minister for Immigration and Anor [2013] FCCA 2208 (9 December 2013).
150 Electronic Transactions (Victoria) Amendment Act 2011; Karoline, above n 132.
151 Electronic Transactions (Victoria) Amendment Act 2011.
If the message is sent to some other electronic address then it will be regarded as received when it becomes both ‘capable of being retrieved and the addressee becomes aware’ that the message was sent to that particular electronic address. These criteria’s can create problems if a message is sent to a non designated system which the user has ceased to use. In such circumstances receipt will never occur. Similarly, if the message is sent when the employee of a company is laid off or is away from the office for a long period of time then the receipt of message on the server will bind the company even without the knowledge of the message. In addition, under this approach receipt will not occur until the user actually becomes ‘aware’ that the message was sent. The requirement of awareness provides scope for manipulation. An addressee can claim that the message was not received to delay the time of formation of contract or to revoke the contract.\(^{152}\)

Websites function on a twenty four hours basis. Some websites prescribe specific time for cancelling order. Determination of time can arise issues when such time limits are provided.\(^{153}\) Determination of time of contract formation will also, likely, create problems especially in situations where a contract is open for a specific period.\(^{154}\) Under the cloud computing technology data will be stored on several data centers of cloud service provides. Thereby raising jurisdictional issues. (where in the world is my data?). Under Section 13(6) an electronic communication will be deemed to be dispatched at the originator’s place of business. It will be deemed as received at the addressee’s place of business. The term ‘Place of business’ has been defined as a place where the party has a non transitory establishment to carry out an economic activity. Cloud computing infrastructure and websites are transitory in nature therefore are not accommodated comfortably by the definition. Under section 2 (b) if the party is a natural person then that persons habitual residence must be regarded as place of business. A person can have multiple residences therefore this section does not provide a definitive answer. Further for the purpose of section 2 the

\(^{152}\) Electronic Transactions Bill 2011 (Vic) Explanatory Memorandum, 12.


place indicated by a party is presumed to his place of business unless it is disproved by the other party. This places an unreasonable burden of disproving it on the other party and is therefore unworkable. Under section 3 (b) if the location is not indicated by the party then the place which has the closest connection to the transaction must be regarded as the place of business. The infrastructure of cloud computing technology is such that there will always be more than one closest connection to the transaction. Therefore this section is equally flawed. Section 3 (c) (i) of the Act states that a location is not a place of business merely because the equipment and technology supporting the transaction is located at that place. This section disregards the fact that a distinction between location of equipment and place of business cannot be made with regards to the virtual online companies who carry out the entire transaction online. Section 3 (d) states domain names and email addresses must not be taken into account for determining place of business.

5.5 Time and Place of Contract Formation: Position in the UK

The Electronic Communications Act 2000 empowers the government to modernize outdated legislation in such a way that an option to use electronic communication is offered as an alternative to paper-based transactions. These provisions are general and lack specific criteria in relation to time of contract formation. Like the European Directive, the Electronic Commerce (EC Directive) Regulations 2002 does not provide time of receipt provisions and deals with acknowledgement of receipt instead\(^{155}\). The regulation is primarily concerned with imposing duties on the service provider when contracts are formed by electronic means.

Although regulation 11 talks about acknowledgement of receipt it does not specifically state the time of contract formation and is therefore inadequate.\(^{156}\) This aspect has been left to the common law.\(^{157}\) Under the Regulation it is up to the courts to determine whether an acknowledgement is a contractual offer under the principles

\(^{155}\) Electronic Communications Act 2000 (UK).
of common law seen in *Entores Ltd v Miles Far East Corporation* ¹⁵⁸ and *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH*,¹⁵⁹.

Regulation 11 of the Electronic Commerce (EC Directive) Regulations 2002 specifies the duties of a service provider. It requires service providers to acknowledge the receipt of the order to the recipient without ‘undue delay’ by electronic means. However, it does not state what amounts to ‘undue delay’.¹⁶⁰ Consequently, lack of specific criteria can give rise to various issues as it disregards the novel features of web based transactions.¹⁶¹ For instance, communication may not get processed altogether if the transaction gets lost. In some instances, message may not get processed due to browser incompatibility or if there is no enough memory on the server where the data base resides. In addition, customer data can also get erased or deleted from the database.¹⁶² These novel issues can have a significant impact on business reputation, damage the business significantly and cause loss of revenue.¹⁶³

The Electronic Commerce (EC Directive) Regulations 2002 further states that the order and the acknowledgement of order will be deemed to be received when the contractual parties are in a position to access it. It disregards various technical factors which can create issues. For instance, incorrect data configuration and input in a wrong format may not allow a party to access information.¹⁶⁴ Unfortunately, the issue is also complicated in relation to mobile phones. Mobile phone internet browsers have infinitely variable degree of support with regards to web pages and graphics. Therefore, criteria for receipt can create problems in relation to these devices. Thus, it is clear from the foregoing that electronic contracts expose transacting parties to significant risks in an online scenario.

¹⁵⁸ *Entores Ltd v Miles Far East Corporation* (1955) 2 QB 327.
¹⁶¹ Ibid.
¹⁶² Vijayraghavan, above n 65.
¹⁶⁴ Vijayraghavan, above n 65.
Although the *Electronic Communication Act* 2000 intends to remove barriers to electronic communication it does not go far enough and deal with the issues of place of contract formation.\(^{165}\) The question of determining place of contract formation has been left to the courts by applying common law principles seen in *Entores Ltd v Miles Far East Corporation*.\(^{166}\) Instead of dealing specifically with place of contract formation Regulation 6 of the Electronic Commerce Regulation Directive 2002 prescribes the conditions which the service provider must follow with regards to location of the service providers. It requires the service provider to provide information regarding the geographical address at which the service provider is established and also their electronic mail address. However, geographical indicators and email address cannot be regarded as exclusive indicators of location.\(^{167}\) In effect, websites are meant to operate on an international basis and conduct transactions globally. Therefore they cannot be regarded as having close connection with any territory in particular. Indicators such as domain names and internet protocol addresses can be manipulated. Fundamentally, a transaction may have multiple connecting factors such as the place where the goods were manufactured, place where the order was placed, place where the goods dispatched, and multiple servers where the website is located. Which aspect of the transaction should be regarded as having the closest connection? Place where the website was accessed may be regarded as the closest connecting factor but this will give rise to a phenomena of worldwide jurisdiction. In the responded had multiple address including an email address. In *Blackwell v Clark, Johnson (Tenancy)*\(^{168}\) the issue was which address should be considered for the purposes of establishing jurisdiction of the court. The responded had indicated for all practical purposes to the applicant that the Sydney address remains a business address at least until 30 April 2013. Therefore, their Sydney address was considered as the concerned address only because the responded had indicated it to be their business address. This can only happen if such an indication has been made. Uncertainties will arise if such an indication has not been made.

---

\(^{165}\) *Electronic Communications Act* 2000 (UK).

\(^{166}\) *Entores Ltd v Miles Far East Corporation* [1955] EWCA Civ 3; [1955] 2 QB 327 per Lord Denning at 334.


Under the regulation if the service provider is registered trading body then the registration number must be provided. However, this factors cannot help much in determination of place of contract formation. Registration number will not be of much help because traders may outsource the products to various other countries. They may have warehouses at several locations and different products can be shipped to fulfill the order. Due to the world wide reach of electronic commerce an order can be made from the house or work place of transacting parties. It can be received by a vendor at the office situated at a different location. Payment made by credit card will likely be received at yet another location. Therefore, these indicators appear to be unworkable.

Further, the regulation requires service provides to provide information in a form and manner which is “easily, directly and permanently accessible”. However, it does not state how the information must be made “easily, directly and permanently accessible”. The regulation limits the application of these requirements requiring it to permanently accessible. Making information permanently accessible can be problematic due to the non transitory nature of the web sites. Usually, websites of an online business can be located on several servers in various jurisdictions. Location of the websites can be easily changed they lack permanency like traditional offline shops. Therefore, websites may not comfortably fit within the requirements provided by the regulation. As a result, these requirements appear to be unworkable.

5.6 Time and Place of Contract Formation: Position in the US

Drafters of both Model Law on Electronic Commerce 1996 (Model Law) and UETA regarded it necessary to state when and where a message is sent and received. Section 15 of UETA is similar to Model Law however, it provides slightly different

---

172 Electronic Transactions (Victoria) Amendment Act 2011.
criteria for receipt and dispatch of electronic communication. Section 15 (a) of the Act deals with dispatch of electronic communication. Under s 15 (a)(1) of the Act, an electronic communication will be considered as sent if it is addressed properly and sent to an information processing system which the recipient has designated or makes use for the purpose of receiving messages of similar type. The term information system is defined as ‘an electronic system used for creating, generating, sending, receiving, storing, displaying or processing information’. Section 15(a) (1) is broad enough to encompass IaaS, PaaS and DaaS of cloud technology.

Under s 15 (a)(2) an electronic communication will be considered as sent if it is capable of being processed or retrieved. Section 15(a) (2) will apply only if the message becomes capable of being processed or retrieved. SaaS allows delivery of web-based content through a browser. The software resides within the cloud. While, PaaS, provides hardware, operation systems, data base systems and network support. Therefore section 15 (a) (2) appear to be pointing specifically towards both PaaS and SaaS infrastructures. ¹⁷⁴

Under s 15(a)(3) of the Act, a message will be considered sent if it ‘enters an information system that is under the control of the recipient’. This section disregards the fact that the cloud consumers will not have control over the underlying computer resources. This provision slightly improves the requirement provided under the Model Law on Electronic Commerce. Under the model law, a message will be regarded as sent when it enters an information system outside the control of the sender. UETA recognised that in certain situations both the sender and recipient of the message might be the part of the same information processing system. Such a situation arises when both the sender and the receiver are the part of the same intranet or same public network. ¹⁷⁵ However, s 15(a) leaves scope for uncertainty by not specifically stating what factors must be considered to determine whether a message

entered an information system under the control of the recipient. Clarification regarding this aspect can promote legal certainty.\textsuperscript{176}

Unlike Model Law on Electronic Commerce, the criteria provided under UETA also take account of some technical aspects of electronic communication. It requires the electronic communication to be addressed properly. Further, it requires the communication to be sent to a system from which it can be processed appropriately. In addition, it also requires it to be sent to a system from which it can be viewed appropriately.\textsuperscript{177} However, this provision has limited scope, as it will only apply if the message is ‘addressed properly or otherwise directed properly to an information processing system that the recipient has designated’.\textsuperscript{178} Under the cloud infrastructure an organisation may outsource a number of functions to cloud services offered by different vendors. A company may use Gmail for email services and salesForce.com for HR services. What amounts to designated information system can raise many issues and questions.\textsuperscript{179}

Under s 15 (b) (1) electronic communication will be regarded as received when it enters an information system which the recipient has designated or uses for the purposes of receiving electronic records of the kind sent. The section emphasizes on entry of the message into the information system but does not specifically state which part of the information system must be considered. Section 15 (b) (2) the message must be capable of being processed by that system. The criteria provided for receipt of electronic communication requires the message to be in a form capable of being processed. However, this criteria disregards the interoperability issues involved with a cloud computing technology.

Other aspects that differ from the model law are the analysis of designated and non-designated information system. The model law provides two different criteria to deal with situations when an information system is designated and non-designated by the addressee. Further, the Model Law on Electronic Commerce has a special rule when

\begin{itemize}
  \item\textsuperscript{176} Uniform Electronic Transactions Act 1999, § 15(a).
  \item\textsuperscript{177} Uniform Electronic Transactions Act 1999.
  \item\textsuperscript{178} Ibid § 15(a)(1).
  \item\textsuperscript{179} T Dillon et al, Cloud Computing: Issues and Challenges (Paper Presented at the 4th IEEE Conference on Advanced information Networking and Challenges, 2010)
\end{itemize}
the message is sent to a non-designated information system. For example, under model law, if it is sent to a non-designated information system then the message will be deemed received only when the addressee retrieves the message.\textsuperscript{180}

UETA does not have any specific rule dealing with non-designated information system like model law. Instead, \textsection 15(b)(1) differentiates it as ‘information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent’.\textsuperscript{181} Under UETA, if the message is sent to a system that was not designated, but is the one used by the receiver for the electronic messages of type, then general provision will apply and the message will be deemed received.\textsuperscript{182} However, this provision has limited application as it will only apply if the message is sent to an information system that is either designated by the recipient or used by the recipient for receiving such message.\textsuperscript{183}

The criteria for receipt fell short of this intended purpose as the provision is not broad enough to cover situations when the message is sent to some other email address that is neither designated by the receiver nor used by the recipient for receiving such message. In such circumstances, a recipient can still leave messages on a server or other services and avoid receipt.\textsuperscript{184} Julie C. White, \textit{ET VIR v Lucas Strange}\textsuperscript{185} involved a suit on contract with regards to buy and sell real estate property. The buyer made an attempt to terminate the contract to buy the property. However, the seller did not receive a timely notice to terminate the contract. Judgment was rendered in favour of the seller. In this case it was noted that the Uniform Electronic Transactions Act only applied if there was an agreement to conduct transactions by electronic means. Context and surrounding circumstances of the cases did not indicate that there was any such agreement between the parties therefore the Act was not applied.

\textsuperscript{181} Uniform Electronic Transactions Act 1999, \textsection 15(b)(1).
\textsuperscript{183} Uniform Electronic Transactions Act 1999, \textsection 15(b)(1).
\textsuperscript{184} Ibid.
\textsuperscript{185} Julie C. White, \textit{ET VIR v Lucas Strange ET UX 80 So. 3d 1189, 2011 La. App. LEXIS 1657}.
Under UETA place of business is the place having closest relationship to the transaction. ⁸⁶ If the recipient does not have place of business then recipient’s residence. Cloud infrastructure is transient in nature therefore the criteria provided will give rise to unworkable results.

5.7 Conclusion

This chapter examined the legal effect of electronic contracts under both the traditional contract principles and the Electronic Transaction Legislation of Australia. A comparative analysis of the laws of Australia, the US and the UK was carried out to gain additional insights. This chapter submits that the influence of technology and international and national developments has led to the development of different approaches. The overall discussion of the chapter leads to the consideration of deficiencies in relation to time and place of contract formation. The laws of the US and the UK lack precise criteria. Although they acknowledge technical features of electronic contracts they contain ambiguous technical terms that provides limited relief and creates confusion. In comparison, Australian legislation provides more modernised criteria as noted in the chapter.

The traditional contract law principles cannot be applied effective to acceptance made by electronic means. The regulatory responses are equally flawed. In relation to determination of time of contract formation the law of the UK is very vague while, the law of US appears to be pointing towards the entire cloud computing infrastructure is therefore inadequate. Although the approach adopted by the Australian legislation has its own uncertainties it provides more precise criteria and appears to be pointing towards IP address of the cloud infrastructure or the email address in relation to time of contract formation.

Likewise, in the light of the nature of internet and websites there can be multiple locations involved when acceptance takes place. Therefore, determination of place of contract formation is problematic under traditional contract principles. Precise place of formation of contract cannot be determined. There is also lack of rule which can

indicate specific place of formation of electronic contracts under the law of Australia, the US and the UK. This chapter examined the issues associated with time and place of contract formation the next Chapter will evaluate other aspects of contract formation.
CHAPTER 6
ENFORCEABILITY OF ELECTRONIC CONTRACTS AND MISTAKEN IDENTITY

6.1 Introduction
6.2 Online Transactions and Mistaken Identity
6.3 Traditional Common Law Principles and Mistaken Identity
6.3.1 Face To Face Dealings and Transactions Carried Out by Correspondence
6.4 Authentications and Carelessness of Parties
6.5 Electronic Authentication and Australia
6.6 Electronic Authentication and Position in the UK
6.7 Electronic Authentication and Position in the US
6.8 Conclusion

6.1 Introduction

Chapter five examined the issues associated with time and place of contract formation. This chapter will advance the argument and evaluate the issues associated with mistaken identity under both the common law principles and the Electronic Transaction Legislation of Australia. A comparative analysis of the laws of Australian, the UK and the US has been carried out to gain additional insights.

6.2 Online Transactions and Mistaken Identity

In order to conduct online business transactions in an effective manner participating entities must be in a position to determine the identity of each other. When transactions are conducted through electronically parties rely on technical means to determine the identity of another party and authenticate the transaction.\(^1\) In an offline environment choice of entering into a contract with a person is often based on special skills of a person or characteristics of a person. While, in an online

environment identities take the form of digital information. People merely rely on this information for forming contracts.²

Advancements in mobile infrastructure also shed new light on the issue of mistaken identity. For instance, technical advancement illustrate the intensity of the issue. In practice, although mobile hand held devices are becoming ubiquitous, they are compact in size. Traditional means of protecting data can strain the resources of these devices. They do not have powerful processors found in traditional desktop based computers. In addition, in the case of mobile devices downloading data can be a time consuming process which will also place load on the battery. In order to overcome these shortcomings the data of a mobile device is now being moved into the cloud. Mobile cloud computing can be defined as an architecture where storage and processing of data takes place outside the mobile device. Mobile cloud application store the data away from the mobile device in a remote collection of computer serves which is known as the cloud by means of wireless networks.³ In a cloud computing infrastructure data will be placed on remote servers therefore it becomes more vulnerable to internet based security threats. As a result, mobile cloud computing can also easily give rise to the issue of identity theft and mistaken identity.⁴

6.3 Traditional Common Law Principles and Mistaken Identity

Under the general principles of the law of contract the offer can only be accepted by the person to whom it is made.⁵ Therefore, issues arise if the identity of a person is impersonated. In mistaken identity cases a fraudster often impersonates the identity of a person and obtains goods on credit or on the basis of a worth less cheque. Later

³ D Nagamalai, Advances in Parallel, Distributed Computing (2011) 514.
the fraudster sells the same goods to an innocent third party and then disappears. Contractual remedies based on misrepresentation will be of little help in such cases as the fraudster will disappear after deceiving the parties. Therefore, the person first deceived will often bring an action against the innocent third party to recover the goods. The action is based on the claim that the ownership of goods cannot pass to the third party as the contract between the person deceived first and the fraudster is void. Therefore, in most cases the innocent third party will be made to bear the loss. However, traditional cases indicate that it is difficult to reconcile one decision in these cases.

6.3.1 Face To Face Dealings and Transactions Carried Out by Correspondence

In relation to mistaken identity the law distinguishes between face to face transactions and transactions carried out by written correspondence. The leading English cases dealing with mistaken identity such as *Cundy v Lindsay*[^8] and *Shogum Finance Ltd v Hudson*[^9] were in writing. In these cases it was held that there was no mutual agreement and meeting of two minds therefore a contract was not formed. However, if the parties carry out face to face transactions it will be generally presumed that the parties intended to deal with the person who is physically present as seen in *Lake v Simmons*[^10], *Ingram v Little*[^11], *Phillips v Brooks*[^12] and *Lewis v Averay*.[^13] Similar view was also expressed in Australian cases such as *Porter v Lactec Finance (Qld) Pty Ltd*[^14], *Vassallo v Haddad Import and Export Pty Ltd*[^15] and *Southdown Publication Pty Ltd v ACP Magazine PTY Ltd*.[^16]

[^6]: *Cundy v Lindsay* (1878) 3 App Cas 459; *Shogum Finance Ltd v Hudson* [2003] UKHL 62; *Lake v Simmons* [1927] AC 487; *Ingram v Little* [1961] 1 QB 31; *Phillips v Brooks* [1919] 2 KB 243; *Lewis v Averay* [1972] 1 QB 198.
[^8]: *Cundy v Lindsay* (1878) 3 App Cas 459.
[^9]: *Shogum Finance Ltd v Hudson* [2003] UKHL 62.
[^10]: *Lake v Simmons* [1927] AC 487.
[^12]: *Phillips v Brooks* [1919] 2 KB 243.
[^14]: *Porter v Lactec Finance (Qld) Pty Ltd* (1964) 111 CLR 177.
[^16]: *Southdown Publication Pty Ltd v ACP Magazine PTY Ltd* (2003) 60 IPR 367.
Such a distinction between face to face transactions and transactions carried out through correspondence cannot be made adequately in relation to electronic contracts. The difficulties associated with electronic communications were also acknowledged in *Shogum Finance Ltd v Hudson* Transactions carried out through electronically can range from email communication to video calls. Transactions can also take place by means of video call, text messages, email messages, video conferencing, voice messages, short text messages and multimedia messages. In addition, it can take the form of social networking communication, Facebook posts, communication carried out though face deal software, photos, picture messages, animations and even video clips. Furthermore, advance machine to machine communication which are carried out with the help of chips, micro sensors, wireless networks, automated processing systems without human intervention further blurs the distinction.

Text base mobile communications sent through different smart phone applications such as viber, WeChat, WhatsApp, tango facility real time communication. Therefore, traditional principles seen in *Cundy v Lindsay* cannot be applied effectively. In this case a fraudster order goods from Lindsay. He signed his name and made it look like ‘Blenkiron’ which was a reputable firm. When goods were received he sold it to a third party buyer Cunday. Payment was made by Cunday to the fraudster but the fraudster did not pay Lindsay. So Lindsay sued Cunday for conversion. Lord Crains explained “Their minds never met even for an instant of time rested upon him, and between him and them there was no consensus of mind which could lead to any agreement or contract whatsoever”.

---

17 *Cundy v Lindsay* (1878) 3 App Cas 459; *Shogum Finance Ltd v Hudson* [2003] UKHL 62; *Lake v Simmons* [1927] AC 487; *Ingam v Little* [1961] 1 QB 31; *Phillips v Brooks* [1919] 2 KB 243; *Lewis v Averay* [1972] 1 QB 198.

18 *Shogum Finance Ltd v Hudson* [2004] 1 AC 919, 70.


20 *Cundy v Lindsay* (1878) 3 App Cas 459.

21 Ibid.

22 Ibid 465
Traditional principles appear to be too simple when examined in the light of technological advancements. Technically, communication will take place between two mobile identities when mobile applications such as viber, WeChat, WhatsApp, tango are used. Similarly, communication will take the form of mere identities when carried out by means of email or instant chat messages. As a result, lack of consensus ad idem as seen in Cundy v Lindsay cannot be established easily. Further, the real time communication element of these applications will add another layer of complexities. The transaction cannot be regarded as taking place in the absence of the parties completely like text based offline transactions. Therefore, direct application of traditional law can easily prejudice the innocent parties involved in the transaction.

It should be noted that the communication method used affects the quality and quantity of authentication information which becomes available to the parties. In Phillips v Brooks it was held that the face to face scenario enables the parties to identify a person by sight and hearing. When dealing with mobile phones and internet based communication only information available to the parties will take the form of email address, internet protocol address, phone number. It will also take the form of the international Mobile station equipment identity (IMEI) for the Hand set itself. The SIM card (Subscriber Identity Module) or the international mobile subscriber identity (IMSI). Therefore, direct application of traditional principles appear to be displaced in the online context.

When transactions are conducted by means of video conferencing or video call they are more likely to be interpreted as face to face dealings as seen in Lake v Simmons, Ingam v Little, Phillips v Brooks and Lewis v Averay. Further, in

---

23 Ibid.
24 Ibid.
25 Mik, above n 2.
28 Lake v Simmons [1927] AC 487.
it was felt that the presumption of face to face dealings should be retained. It was also highlighted in this case that if there is “an alleged contract reached by correspondence, offer and acceptance must be found if there are to be found at all, in the terms of the document”.

In face to face dealings as seen in Lake v Simmons, Ingam v Little, Phillips v Brooks and Lewis v Averay it will be generally presumed that the parties intended to deal with the person who is physically present. Generally, the deceived party will have very little means to rebut the presumption even in the offline environment. Technically, in an online scenario the person deceived will be placed in a greater disadvantaged position. On one hand, the deceived party will have very few means to rebute the presumption, on the other hand the law will presume the person so deceived to be intending to deal with the fraudster. Passing on the risks to an innocent third party will equally prejudice their position.

6.4 Authentications and Carelessness of Parties

In an online scenario transactions are usually conducted remotely. Authentication or the process of determining the identity of the party takes place by means of passwords, smart cards or biometric data. Regardless of whether email correspondence is carried out or an internet based video call is made through a smart phone issue of mistaken identity can arise due to the inherent insecure nature of the internet. Mistaken identity issues generally arise due to the carelessness of the transacting parties. Underlying carelessness of the parties plays a major role in mistaken identity scenarios. Therefore effectiveness of technologies used to determine the authenticity of the transaction plays a very important role in an online context.

33 Shogum Finance Ltd v Hudson [2004] 1 AC 919, para 51.
34 Lake v Simmons [1927] AC 487.
38 Mik, above n 2.
Steps taken by the parties to determine the identity of each other was assessed in some traditional cases such as *Ingram v Little*[^39] *Shogum Finance Ltd v Hudson*[^40] and *Lewis v Averay*.[^41] The person first deceived was held to be careless for briefly checking the street address in *Ingram v Little*.[^42] Similarly, mere reliance on identity card presented was regarded as carelessness in *Shogum Finance Ltd v Hudson*.[^43] While, in *Lewis v Averay*[^44] fraudster was asked to provide some identity proof without taking effective steps to determine the identity. However, when transactions are carried out remotely in an online environment parties will have very few means to determine the identity. Consequently, there is a need for greater certainty in relation to electronic contracts.

In *Ingram v Little*[^45] a fraudster purchased a car from an owner. The possession of the car was obtained by means of a cheque. The owner checked the identity in the telephone directory and handed over the car. While, in *Shogum Finance Ltd v Hudson*[^46] a fraudster purchased a car by claiming to be Durlabh Pate. He provided identification which indicated his name as Durlabh Patel and also forged the signature. Later the car was delivered to him. Similarly, in *Kings Norton Metal Co Ltd v Edridge, Merrett and Co Ltd*[^47] a fraudster ordered goods by using a printed letter head of a company called Hallum and Co. Later the goods were delivered to him on credit. On similar lines, in *Lewis v Averay*[^48] a fraudster entered into a contract by claiming himself to be a famous personality. He showed a special pass which had the name of the famous personality on it. The owner was convinced with the identification information provided and parted with the car. In all these cases the plaintiff was misrepresented about the credit worthiness of the party. The person first deceived in these cases had taken a considerable risk by entering into the contract and was duped. In these cases possession of goods was handed over to the fraudster party without taking adequate precautions.

[^40]: *Shogum Finance Ltd v Hudson* [2003] UKHL 62.
[^41]: *Lewis v Averay* [1972] 1 QB 198.
[^43]: *Shogum Finance Ltd v Hudson* [2003] UKHL 62.
[^44]: *Lewis v Averay* [1972] 1 QB 198.
[^46]: *Shogum Finance Ltd v Hudson* [2003] UKHL 62.
[^47]: *Kings Norton Metal Co Ltd v Edridge, Merrett and Co Ltd* (1897) 14 TLR 98.
In *Lewis v Averay* Lord Dennings claimed ‘Man’s very name is one of his attributes. It is a key to his identity’. In contrast, name written in an electronic medium cannot be said to be a key to a person’s identity due to the high risk of data loss. For instance, every organisation collects, uses and stores personally identifiable information. Most organisations store the details of their employees. Depending upon the area of business they may even store and use the details of their patients, customers, students and residents. Use of technology has given rise to much greater flexibility and speed when it comes to making purchases, processing, payment and data management. Data loss puts PII (personally identifiable information) of people at a significant risk. PII can take various form such as address information, mother’s maiden name, taxpayer identification number, address information, personal characteristics, photographic images, fingerprints, hand writing, voice signature, geographical indicators, employment information, medical information, educational information, financial information and place of birth. However, online personal identification information (PII) about a person stored can be regarded as a mere label. Regardless of how vast the information is additional technical evidence will be required to authenticate the online data. Further, loss of PII can easily occur at different stages of transaction. It can occur when data is being used on endpoints by employees to do their job. It can also occur when data is at rest in information repositories such as exchange servers, share point servers and web servers. In addition it can also take place when data is in motion over the internet. Therefore, identity management policies and procedures should be strictly scrutinized when deciding mistaken identity cases. Security breaches can easily lead to misuse of data. A message may appear to have originated from a particular source which could actually might be a case of security breach. As a result, distinction between attribute and actual identity in question becomes much more difficult in the online

---

49 Ibid.  
51 *Shogum Finance Ltd v Hudson* [2003] UKHL 62.  
53 Mik, above n 2.
context. In the online scenario greater proofs of attributes should be sought from the contracting parties with regards to mistaken identity cases.  

In *Ingram v Little*  it was stressed that the ‘plaintiff’s unguarded transaction had caused loss to another’. By implication, electronic communications will always take the form unguarded transactions. For instance, text based passwords can be said to be at the base of online authentication used to prevent identity theft. Instead of making users type complex passwords on small mobile devices business are now looking at new authentication techniques which can make use of graphical and touch screen technologies. Pattern based and image based authentication techniques allow users to authenticate in a more natural way. Instead of remembering passwords users can touch a series of pictures to identify which ones actually match their secret authentication categories. Such image based authentication techniques allow users to execute and complete their transaction quickly. In the offline medium when a person forms contract by means of face to face dealings the transaction can be easily attributed to the actual human being involved. Such an attribution cannot be made in an online medium.

It was further noted in *Ingram v Little* that ‘For doing of justice, the relevant question in this sort of case is not whether the contract was void or voidable, but which of the two innocent parties shall suffer for the fraud of a third’. By analogy electronic contracts raises even bigger concerns as electronic means of authentications only generally indicate that the transaction was originated from a particular source. Authentication methods such as email passwords are created by taking some general information such as name, date of birth, address which itself can be manipulated. Even when genuine information is provided the electronic identity so created will take the form of a general electronic attribute which will not uniquely identity the person. Most digital identities such as passwords, will only link the transaction to the electronic information provided by the person while creating the identity. They will not form any association with the specific human being. Just like passwords brain wave authentication can be used to authenticate mobile devices.

---

54 Mulcahy, above n 7, 118–125.
56 Ibid.
Users can gain access by thinking certain thoughts or picturing specific images. However, using brain waves will not necessarily make the device more secure. Regardless of the authentication method used, digital data will be sent over the internet which itself is an insecure medium.

In *Shogum Finance Ltd v Hudson*\(^{57}\) it was highlighted that “given the equivocal nature of a person’s identity, there is something to be said for selecting those aspects of the offeror’s identity which are material in causing the other party to accept the offer”. However, electronic identities do not effectively provide any material basis. Even unique identifiers like biometric identifiers will only insubstantially link the person with the identity as they are prone to misuse and tampering.\(^{58}\) For instance, sensors embedded on smartphones enable its owner’s biometrics and behaviour to act as an authentication technique. Microphones can be used for voice recognition. Cameras can be used for facial recognition. A person’s rhythm of walking can also act as authentication. Biometric data will be verified against the information stored on the database not with the genuine human being as in case of offline transactions. Any person who manages to tamper the biometric data or impersonate the biometric data will be verified by the database as a genuine person.\(^{59}\)

In *Kings Norton Metal Co Ltd v Edridge, Merrett and Co Ltd*\(^{60}\) it was explained “There was only one entity, trading it might be under an alias, and there was a contract by which the property passed to him” In contracts, electronic contracts provide more easy means for creating decrepitly similar identities. The companies which develop social networking sites perceive them as a means to solve the identity issue. Attempts made by both Google and Facebook to turn their websites into concrete means of determining online identity of people have not been successful. Google strongly demanded its users to use real names but the problem was impossibility of determining the true identity of people. Facebook made an attempt to

---

\(^{57}\) *Shogum Finance Ltd v Hudson* [2003] UKHL 62, 75.  
\(^{58}\) *Brain Waves Could Make Passwords Old School* (2013) Technews.com  
\(^{60}\) *Kings Norton Metal Co Ltd v Edridge, Merrett and Co Ltd* (1897) 14 TLR 98.
resolve the identity issue by requesting its users to scan their government documents such as passport and send them to Facebook over the internet. Like google, Facebook attempt to resolve the issue of identity has not been successful so far. Identity automatically accompanies and implies attribute in the physical world but same cannot not be said with regards to the online world.

Different authentication measures used by the party can range from simple passwords to more complex authentication measures offering different levels of security. As noted in Shogum Finance Ltd v Hudson\textsuperscript{62} innocent parties rights should not depend upon the misrepresentation made by the fraudster. There is need for a more concrete criteria for determining the rights of the third party. In Lord Walker’s view\textsuperscript{63} “there is sometimes an inclination to regard the eventual buyer from the rogue as the more deserving of sympathy”. However, in an online context both the person first deceived and the third innocent party will be in an equally disadvantage position.

In an offline medium attributes of a person such as special skills of a person, characteristics of a person can be used as a basis to recognise the person.\textsuperscript{64} However, the electronic attributes created in an online medium such as biometric data can be easily separated from the actual person and manipulated. Overall, the general information available in the online medium will take the form of mobile number, email address and online identity being used. Therefore, liberal interpretation of traditional legal principles will cause greater damage to the deceived parties in an online scenario. In an online medium both transactions carried out by correspondence and transactions carried out face to face by video call always take place remotely. The insecure nature of internet and easy means of tampering identity of another party warrants judicial intervention. It is submitted that there is need for law reform in the area. There is a wide disagreement of principles in traditional cases. The advance technological developments are adding further uncertainty.

\textsuperscript{62} Shogum Finance Ltd v Hudson [2003] UKHL 62.
\textsuperscript{63} Shogum Finance Ltd v Hudson [2004] 1 AC 919, 181.
\textsuperscript{64} Mik, above n 2.
There is a need to re-evaluate the traditional mistaken identity principles in the light of insecure nature of the internet. Appropriate legislative measures must be taken to prescribe specific security standards which can protect the innocent parties to a considerable extent. In the light of easy means of tampering the identity of a person in an online scenario adequate measures must be taken to protect the rights of the parties. A standard based on a technical neutral approach must be adopted to protect both the person first deceived and the innocent third party. There is a need for a specific standard on the basis of which losses between the person first deceived and the innocent their party can be allocated.

In *Lickbarrow v Mason* it was held that ‘whenever one of two innocent persons must suffer by the acts of a third, he who has enabled such third person to occasion the loss must sustain it’. In mistaken identity cases the person first deceived will be in a better position to cancel the transaction if he is not satisfied with the identity of the party. Innocent third party cannot protect himself in a similar manner. Arguably, internet is an inherently insecure medium and if the party first deceived takes the risk of entering into a contract over the internet then the party first deceived should be made to bear greater part of the loss in mistaken identity scenarios as seen in *Lickbarrow v Mason*. Innocent third party should be made to bear lesser part of the loss. The person first deceived relies on the information provided by the fraudster and facilitates the misrepresentation. Therefore, in online transactions innocent third part deserves more protection.

Traditional principles are inadequate. A comparative analysis of the electronic transaction legislation of Australia and the *Electronic Communications Act 2000* (UK) will be carried out in the next section. The analysis is carried out to see to what extent they addressed the issues related to mistaken identity.

### 6.5 Electronic Authentication and Australia’s Response to International Norms

---

65 *Lickbarrow v Mason* (1787) 2 Temp.rep.63 at 70.
66 Ibid.
In Australia, amendments were made to the signature criteria of the *Electronic Transactions Act 2000* (Vic). The amendment was made to modernise the framework of electronic commerce as noted in Chapter 3. Like the United Nations Convention on the Use of Electronic Communications in International Contracts 2005, the *Electronic Transactions (Victoria) Amendment Act 2011* does not specifically deal with mistaken identity. However, it deals with electronic signatures. Electronic signatures are generally used to authenticate online transactions. Therefore, it is necessary to assess the criteria dealing with electronic signatures from the perspective of mistaken identity.

The *Electronic Transactions (Victoria) Amendment Act 2011* requires the signature method to be reliable and appropriate but does not state what amounts to a reliable method. Section 8 of the Act states that the reliability of the signature method must be assessed in the light of all the circumstances associated with the signature. By being minimalist in nature it does not specifically deal with authenticity and integrity. It does not require the signature method to identify a person uniquely. Therefore, even if a contract has an electronic signature it can still give rise to the issue of mistaken identity.

However, it appears to have slightly reduced the risk of non-repudiation. The amendment states that a contract should not be repudiated if identity is not disputed. This test can only apply if the identity of the party is not really in dispute. It is not...
concerned with situations when a signature is impersonated. Therefore, it is not adequate and its usefulness can be questioned.\textsuperscript{78} For instance, Echo Sign is a newly invented electronic signature. It allows contracting parties to sign documents online and return documents without the use of printers, fax machines or mail delivery methods. It automates the entire process such as requesting signature, distributing it and executing documents. Archival copies of signed documents are also automatically stored in Echo sign account. The issue of mistaken identity is substantially raised in this method due to the insecure nature of the internet.\textsuperscript{79} On the other hand, Apple made an even bigger attempt. It requires its customers to associate their finger prints with their iPhone. After doing this the iPhone becomes the means for identifying the identity. The identity is created by swiping a finger on the iPhone and then securing it with a four digit passcode lock. The passcode can be turned off when not in use.\textsuperscript{80} However, it can be compromised if stolen. As a result, contracting parties have limited means for determine the identities of the parties.

Attribution and the intention to enter into a contract with a specific individual requires the ability to identify the person in question.\textsuperscript{81} A person can impersonate the signature and pretend to be the genuine person to the owner of the goods. The imposter can then make the owner of the goods to part with the goods on the basis of such impersonation. Online means of authentications merely confirm that a message was originated by using a particular authentication method. They cannot uniquely tie a person with the online authentication method. The legislation has side stepped this issue.

The legislation provides insubstantial criteria for determining the identities of the parties. Like the traditional cases of mistaken identity the signature criteria provided under the Act does not provide any guidance regarding the roles and responsibly of parties in relation to authentication. Although internet is an insecure medium parties

\textsuperscript{78} Ibid.
\textsuperscript{80} Elgan, above n 61.
\textsuperscript{81} Mik, above n 2.
are not obligated to safeguard the information which can lead to identity theft. Therefore, the risk of identity theft is enhanced in an online context.  

6.6 Electronic Authentication and Position in the UK

The Electronic Communications Act 2000 deals with the legal status of electronic signatures and empowers the government to modernise outdate legislation in such a way that an option to use electronic communication and to provide storage is offered as an alternative to paper-based transactions. The Electronic Communications Act 2000 also recognises self-regulatory schemes that ensure the quality of electronic signatures and cryptography support services. The Electronic Signatures Regulations 2002 were introduced to implement the European Directive on electronic signatures that was enforced on 8 March 2002. The EU Electronic Signatures Directive facilitates the use of electronic signatures and contributes towards the legal recognition of electronic signatures.

The Electronic Signatures Regulations 2002 incorporates the EU Directive provisions related to the supervision of certification and data protection requirements, whereas the provisions on the admissibility of electronic signatures under legal proceedings are implemented in the Electronic Communications Act 2000. Under s 7(2) of the Electronic Communications Act 2000 and s 2 of the Electronic Signatures Regulations 2002, electronic signature can be represented in multiple forms and serves as a method of authentication. However, the Electronic Communications Act 2000 does not describe the legal effects of electronic signatures. The Act appears to validates different signatures methods ranging from email to highly secure digital signatures. It does not provide specific criteria for attributing the

---

82 Electronic Transactions (Victoria) Amendment Act 2011.
86 Wang, above n 83, 32, 35–8.
87 Electronic Signatures Regulations 2002.
signature to a specific person. The Act only states that electronic signatures, the certification and the process under which such signatures and certificates are created, issued and used shall be admissible in evidence in terms of the authenticity of the communication or data or the integrity of the communication or data. These provisions, appear to go a step beyond the Australian legislation and specifically state what type of authentication measures can be used as an evidence for justifying the use of a particular signature method. In comparison, Australian legislation merely state that the reliability of the signature method must be assessed in the light of all the circumstances associated with the signature. However, none of the approaches provide a comprehensive criteria as they do not provide unique means of linking a signature to a particular person. Therefore, they do not offer solution from the perspective of mistaken identity.

Further, unlike the Australian law the law of the UK appears to me more inclined towards digital signatures. As a result it is not as technology neutral as the Australian law. Digital certificates are used to establish the authenticity of Digital signatures. Digital signatures, are a sub-set of electronic signatures based on Public Key Infrastructure (PKI). If the private key is lost then the digital signatures will wrongly attribute the signature to some other person and give rise to the issue of identity theft and mistaken identity.

The criteria provided under the law of the UK is broad enough to accommodate digital signatures created by mobile devices. For instance, communication can also take the form of Short Message Service (SMS) which facilitates sending of short messages. Users can also authenticate their messages by using encryption technology. However, this mechanism has many disadvantages as SMS service itself has small bandwidth and can only send short messages. Further, under this

88 Ibid.
89 Electronic Communications Act 2000 (UK) c 7.
90 Electronic Transactions Amendment Act 2011(Vic).
91 Electronic Transactions (Victoria) Amendment Act 2011.
mechanism SIM card manufacturer create general encryption and stamp of the signature. Therefore, encryption technology will not be under the sole control of end users. From the perspective of mistaken identity means of identification takes the form of generally coded digital data and cannot be regarded as an unique identifier. Although, the encryption methods used by SIM card manufactures have low security threshold they will be admissible as evidence in terms of the authenticity of the communication under the law of UK. In comparison, under the electronic transaction legislation of Australia an electronic signature can only protect a person from fraud on the basis of surrounding facts and circumstance of a case. Therefore, encryption methods used by SIM card manufactures will be more readily considered as authentic. The electronic transaction legislation of Australia was not intended to deal with the evidential aspects of an electronic signature. Therefore, the approach adopted by the electronic transaction legislation of Australia slightly differs from the law of the UK and arguably offers less security.

Under the law of the UK the evidential value of an electronic signature is decided by the court based upon the facts of a particular case and the Act does not define any requirements for acceptance of electronic signature. Hence, the legislation in the UK in this respect is different from the European Directive on electronic signatures, because the EU Directive gives qualified electronic signatures the same legal effect as that of a handwritten signature. The UK does not implement this Directive because it holds that handwritten signatures have no special evidential status under the UK legislation. The Act disregards the fact that the handwritten signatures can be attributed to a specific person based on the analysis of handwriting such an attribution cannot be made in case of electronic signatures. However,

---

95 Electronic Communications Act 2000 (UK) c 7.
96 Electronic Transactions (Victoria) Amendment Act 2011.
97 Ibid.
100 Ibid.
101 Ibid.
103 Electronic Signatures Regulations 2002.
under s 7 of the *Electronic Communications Act 2000*, the parties may decide about the legal status of electronic signatures between them. Like the Australian legislation the *Electronic Communications Act 2000* does not specifically mention the potential liabilities of the parties in relation to identity theft.

6.7 Electronic Authentication and Position in the US

In the US, many states have now passed legislation in order to implement a *Uniform Electronic Transactions Act 1999* (UETA). Since 1995, a number of states have enacted their own legislation on electronic commerce and electronic signatures. However, these states have taken divergent approaches resulting in inconsistencies in the regulations in different states. Like the international developments, conflicting approaches or movements are found within states of a particular country. Different patterns of laws emerged in the US. Utah was the first state that adopted a technology-specific approach.

Utah, along with states such as Minnesota, Mississippi, Missouri and New Mexico, Illinois developed digital signatures arrangement that was based on PKI and adopted a technology-specific approach. Whereas states such as California, Alabama, Arizona, Colorado, Connecticut, Delaware and Georgia followed a completely different approach that was technology-neutral approach that gave multiple forms of electronic signatures the same legal effect as that of handwritten signatures, provided the electronic signatures met certain requirements.

---

Some of the US states took a lead in regulating online authentication by passing digital signature laws.\(^{108}\) Most other states had a combination of the two approaches that created a hybrid law,\(^{109}\) while Massachusetts adopted a minimalist approach.\(^{110}\) In contracts, electronic transaction legislation of Australia broadly accommodates different authentication measures. It expressly provides equal validity to both highly secure and highly insecure signatures. It merely requires a signature method to be reliable and appropriate and offers a less threshold.\(^{111}\)

In order to promote uniformity in the legislation governing electronic contracts and electronic signatures, two initiatives have been introduced: UETA and the *Electronic Signatures in Global and National Commerce Act* (E-SIGN). UETA is considered a model law that may be modified by the states when adopted. Most states have adopted UETA with some modifications though they continue to show inconsistencies.\(^{112}\)

The purpose of UETA is to build a strong foundation for the use of electronic transactions and electronic signatures.\(^{113}\) UETA originally developed in 1999 as a Model Act by the National Conference of Commissioners on Uniform State Laws.\(^{114}\)


\(^{109}\) Freedman, above n 107, 807, 810.


\(^{111}\) *Electronic Transactions (Victoria) Amendment Act 2011*.


The UETA project, which had its source in the Model Law on Electronic Commerce, began in 1997 and it was completed in 1999. Before the introduction of UETA, the fundamental question posed by the courts and the legislators was: ‘Under what circumstances electronic records and signatures were as trustworthy as traditional writings and signatures?’ The main purpose of UETA is to align state laws of different states regarding a number of electronic commerce matters including the validity of electronic signatures in order to support valid electronic contracts and retain paper records. However, the scope of UETA is strictly limited to commercial transactions and issues. The aim of UETA is to create legal certainty and predictability in electronic commerce by affording electronic signatures and electronic records the same legal status that exists with the written signatures and records or traditional contracts. UETA defines signature as an electronic sound, symbol or process associated with the record if it has been used with an intention to sign the record. Under this criteria mobile numbers, email addresses and any online identity used by a party can be regarded as a signature as long as it has been used with an intention to sign. In contrast, the electronic transaction legislation of Australia does not require specific adoption of the signature method and appears to have a broader scope. Therefore, provides more scope for impersonation and mistaken identity.

Despite UETA being adopted by many states in some form or the other, there is no uniformity in the states regarding the enactment of laws related to electronic transactions. Since the state version of UETA in different states contained a number of exceptions and modifications, the state legislation became diverse and changed quickly that the federal government stopped tracking laws related to electronic transactions since 2003. Both the objectives of E-SIGN and UETA are similar and facilitate electronic commerce by providing a system to enforce and validate

116 Scoville, above n 110, 345, 347.
118 Electronic Transactions (Victoria) Amendment Act 2011.
electronic signatures. Hence, it is criticised as to why these practically co-extensive laws co-exist. In this context, Carl, C, Ciocchetti, C, Barton, W and Christensen, N have stated as follows:

Without a uniform standard, many jurisdictions ruled inconsistently, while other jurisdictions did not consider the issue. This disparate treatment threatened the legitimacy of on-line agreements and deprived both consumers and businesses of the certainty and predictability expected from well developed markets. The law’s formalities evolved outside of the digital world, and the process of adapting them to it has proven to be more difficult than expected. Congress reacted to this trend by enacting broad legislation to give nationwide validity to electronic records and signatures.

Due to the inconsistencies and the time that the states may take in adopting UETA, in the year 2000, the Congress passed E-SIGN. UETA is a federal legislation applicable to all states in the US. Both UETA and E-SIGN have the same objective of facilitating the use of electronic records and signatures in order to establish a uniform legal framework for the creation and use of electronic signatures and records. Both E-SIGN and UETA have provisions that specify that electronic contracts and electronic signatures shall not be denied legal effect or enforceability simply because they are electronic. These two legislations are not identical but they do overlap significantly. In both these Acts, the definition of ‘electronic signature’ is similar. E-SIGN is technology-neutral in its approach and it promotes uniformity regarding

---

119 By 2007, the only four states that had not adopted UETA were Illinois, Georgia, New York and Washington. The laws governing electronic signatures in these four states are similar and are considered model state legislation for contracts governed by the state law. Balloon, above n 112, 908–10; S Mason, Electronic Signatures in Law (2nd ed, 2007) 232–6. The National Conference of Commissioners on Uniform State Laws is a non-profit unincorporated association that is comprised of state commissions on uniform laws from each state in US, the District of Columbia, the Commonwealth of Puerto Rico and the US Virgin Islands. It was formed in 1892 in order to promote the uniformity of state laws in the US.


electronic signatures and electronic records among states. Both Acts are procedural and subject to the substantive law. The laws merely require logical association of the electronic record with the signature. These laws are broad enough to accommodate different authentication measures such as video call, text messages, email messages, video conferencing, voice messages, short text messages, multimedia messages, social networking communication, Facebook posts, communication carried out through face deal software, photos, picture messages, animations and even video clips. Further, it is also broad to accommodate text base mobile communications sent through different smart phone applications such as viber, WeChat, WhatsApp, tango facility real time communication. Under these Acts electronic signatures cannot specifically protect transacting parties from impersonation. The electronic attributes created in an online medium such as biometric data can be easily separated from the actual person and manipulated. The laws appear to have side stepped this aspect of electronic data. In comparison, the Australian legislation does not require specific logical association as seen under the laws of USA and is arguable more liberal. It merely requires the signature method to be reliable and appropriate and is therefore more ambiguous.

E-SIGN is considered an overlay law because it does not amend any laws and only provides that any transactions in or affecting interstate or foreign commerce that involves a signature or contract or record must not be denied legal effect, validity or enforceability solely because it is in electronic form. In spite of the application of E-SIGN in the US, it does not affect any other federal or state legislation or common law that applies to electronic contracts and transactions.

126 Electronic Transactions (Victoria) Amendment Act 2011.
Section 9(a) of the UETA describes attribution procedures used to verify that an electronic signature, message or record is that of the person purporting to provide it. If it is assumed that the requisite intention and association with the record exists, then the following signatures qualify as electronic signatures such as: 129

a. Biometrics;
b. Digital signatures;
c. A manual signature transmitted through a facsimile;
d. Typed name;
e. Digitised picture or image of a manual signature;
f. Clicking on ‘I agree’ or ‘purchase now’ button; 130
g. Including the name of a person as part of an electronic mail or including the name of the form on a facsimile; and
h. Voice on an answering machine.

In contrast, the electronic transaction legislation of Australia does not expressly talks about association and attribution of record as seen under the s 9(a) of UETA. 131

Section 5(b) of UETA states that it applies to a transaction only if parties have agreed to use electronic media. 132 The main purpose of UETA is to align state laws of different states regarding a number of electronic commerce matters including the validity of electronic signatures in order to support valid electronic contracts and retain paper records. However, the scope of UETA is strictly limited to commercial transactions and issues. UETA is one of a large number of Uniform Acts that are proposed by the National Conference of Commissioners on Uniform State Laws (NCCUSL). Prior to the enactment of UETA, banks in every state of the US were required to keep physical record of all cheques that were processed. UETA is considered a model act and its aim is to align states legislation on a national basis in

129 Christensen, Duncan and Low, above n 122.
order to allow for a uniform method for retention of paper records in electronic form, thereby making the electronic copy as valid as an ink copy for the purpose of interstate trade and commerce. Over 38 states in the US enacted UETA by the year 2001 and in 2002 California and Hawaii introduced legislation, amending their existing UETA law. The legislation in California is similar to E-SIGN but the Hawaiian legislation has added provisions regarding the security of electronic commerce. Similarly, Virginia has revised the electronic signature legislation in order to prohibit a signature from being denied the legal effect or enforceability solely because the signature is in an electronic form. By March 2007, 47 states had enacted some form of UETA protecting electronic records.

The criteria goes beyond the approaches adopted in Australia as it specifically list authentication measures. The legislation provides insubstantial criteria for determining the identities of the parties. Like the traditional cases of mistaken identity the signature criteria provided under the Act does not provide any guidance regarding the roles and responsibly of parties in relation to authentication. Although internet is an insecure medium parties are not obligated to safeguard the information which can lead to identity theft. Although the legislation talks about more technical aspects and some authentication measures it is not comprehensive and is therefore unworkable.

6.8 Conclusion

The chapter examined the legal effect of mistaken identity from the prospective of smart phones. A comparative analysis of the laws of Australia, the UK and the US was carried out to gain additional insights. The overall discussion of the Chapter leads to the consideration of deficiencies in relation to mistaken identity. Traditional common law principles cannot accommodate mistaken identity issues in relation to mobile commerce. Unlike offline transactions identities cannot be adequately identified and attributed to a specific person in the online scenario. Digital identities

---

133 Mason, above n 119.
are growing rapidly and are distinct from our physical offline existence. These digital identities are blending into the digital enterprise. Users create personal credentials for baking, consumer products, electronic commerce retailing, government services, home insurance policies and even for remote internet access. Organizations are realizing the power of digital identities. However, a logical single and trustworthy universal secure digital identity which can be used with confidence across different sectors is still lacking.

Traditional common law principles appear to be displaced with regards to mobile commerce. Liberal interpretation of traditional contract principles can easily prejudice the innocent parties involved in the transaction. The insecure nature of internet and easy means of tampering identity of another party warrants judicial intervention. Appropriate legislative measures must be taken to prescribe specific security standards which could protect the innocent parties to a considerable extent. In the light of easy means of tampering the identity of a person in an online scenario adequate measures must be taken to protect the rights of the innocent third party. A standard based on a technical neutral and media neutral approach must be adopted to protect both the person first deceived and the innocent third party.

Due to the inherent insecure nature of internet a person cannot be made specifically accountable for an act in the online medium. As a result, there is a need for specific guidelines which can be used to assess the adequacy of the authentication measure used by the parties in relation to mistaken identity cases. There is a need for law reform in these three areas. Firstly, the distinction between face to face dealings and paper based transactions should be removed. Secondly, there is need for specifying what measures contracting parties should take to secure their transactions. In this regard, there is also a need to prescribe guidelines regarding who should bear the loss if the authentication method is compromised. Arguably, the internet is an inherently insecure medium and if the party first deceived takes the risk of entering into a contract over the internet then the party first deceived should be made to bear

---


221
greater part of the loss in mistaken identity scenarios. Innocent third party should be made to bear lesser part of the loss. Thirdly, it is necessary to provide guidelines regarding how the importance of identity should be proved and against whom the contract should be enforced. Equally important is the need to state what should be the basis to assess whether a person is who he claims to be. In particular, legislative response should specify what minimum measures should a party take to determine the authenticity of the transaction and who should be made accountable.

Comparative analysis of the laws the UK, the US and Australia indicate that the laws are deficient from the prospective of mistaken identity. Different approaches have been adopted by these two jurisdictions. Influence of technology and international developments has led to the adoption of different approaches. However, the Australian law appears to be more technology neutral in approach and appears to be a better model. In addition, reform of Australian contract law appears to be the first step in the right direction.
7.1 Introduction

Previous chapter evaluated the issues related to mistaken identity. This chapter advances the argument and evaluates the issues related to writing and signature requirements. The purpose of this chapter is to analyse the Australian Electronic Transaction legislation in relation to writing and signature requirements. The analysis is carried out to see to what extent it has addressed the issues related to writing and signatures requirement. Comparative analysis of the law of the UK and the US is carried out to see whether the approaches differs from the approach adopted in Australia.

The Electronic Transaction Legislation does not provide contract formation principles. Instead, the legislation mainly establishes technology-neutral criteria in relation to validity of electronic transaction, writing and signature. The adequacy of these criteria is analysed in this chapter.
This chapter seeks to explore the effect of Electronic Transaction Legislation in providing an appropriate legislative framework. The relevance and importance of the Electronic Transaction Legislation is discussed and the enforceability of electronic contract and electronic signature is examined. Although this chapter refers to the Electronic Transaction Legislation of other jurisdictions of Australia throughout the discussion, it specifically examines the Electronic Transaction Legislation of Victoria.

7.2 The Validity of Electronic Contracts, Writing Requirements and Response to International Norms

The *Electronic Transactions (Victoria) Amendment Act* 2011 has made amendments to the writing criteria of the principal Act. It brings it in line with the United Nations Convention on the Use of Electronic Communications in International Contracts 2005. After the amendment a provision is added stating that the requirement for a contract to be in writing can be met in an electronic form. The new criteria merely fine tunes the criteria provided under the old Act.

A contract is generally not required to be in writing and may be legally effective even in the absence of a signature. The absence of ‘writing’ and ‘signature’ does not affect the enforceability of a contract. However, it provides additional assurance to the other party regarding the acceptance of the terms of the contract and is therefore important.


2 Ibid, para 2.9.

The Electronic Transaction Legislation states that a transaction is not invalid for being conducted electronically. Accordingly, in *eBay International AG v Creative Festival Entertainment Pty Limited* contents of a web site were liberally interpreted and regarded as writing. The electronic transaction legislation attempts to achieve functional equivalence without transposing all the functions of paper based documents into the online environment. In effect, the information contained within a paper based document does not change or get altered after it is created. Traditional paper based documents are tangible, stable and confined to a specific paper. A person will have control over how a document is created and stored. In contrast, when a document is created by means of cloud computing a person will not have any control over the manner in which it is created, stored and processed. Traditional paper based documents or even the documents saved on the desktop of a personal computer are confined to a specific place they are not scattered and stored over various servers as in the case of cloud computing technology. Cloud computing based documents are stored on the internet therefore the insecure nature of internet also raises security concerns.

Moreover, cloud computing which is the most commonly used technology encompasses multiple computers, multiple servers and multiple networks. In a layman’s language cloud is a collection of computers and servers which are accessible through the internet. A web based application or service offered via the internet is called cloud computing. It can include cloud based word processor, email and power point presentation. Therefore, under a cloud computing infrastructure a user will not know who is accessing their document and the data cannot be monitored in any way.

The user cannot be sure that a confidential file which they delete has in fact been deleted from the system. As the cloud computing technology can always store a backup file. Cloud computing fully depends upon the internet for access and is

---

5 *eBay International AG v Creative Festival Entertainment Pty Limited* [2006] FCA 1768 at 48, 49.
6 E K Mik, ‘From Clay Tablets to AJAX Replicating Writing and Documents in Internet Transactions’ 15(8) *Journal of Internet Law* 2, 2–4.
7 Ibid.
therefore phone to security risks twenty four hours a day.\textsuperscript{8} Documents and data are processed outside the company therefore inherent risks are always involved. In cloud computing technology outsourced services bypass the physical, logical and personal controls.\textsuperscript{9} In desktop based documents data can be recovered from the hard drive of the laptop or desktop computer. In contrast, in case of cloud computing data is stored online hard drive cannot be removed to recover data.\textsuperscript{10}

Under traditional desktop based models administrative access to servers and is controlled though on premises. While in cloud computing administrative access is through internet exposing the organisation to risks. Many times user credentials are stored outside the organisation in cloud infrastructure. Therefore companies must ensure that the accounts of employees are removed from the cloud infrastructure once they leave the company. Virtualization is one of the key components of cloud computing. Virtualised machines can be paused, restarted and reverted to earlier instances. Due to this dynamic structure of cloud computing security cannot be maintained constantly.\textsuperscript{11}

Under the electronic transaction legislation the requirement to give information in writing is satisfied if the information provided is accessible and usable for subsequent reference. It merely focuses on ‘accessibility’ and ‘usability’. It does not specifically deal with retaining contents in a stable manner.\textsuperscript{12} Electronic documents differ from paper based documents they are not only created but also processed through the cloud infrastructure. Online writing becomes accessible via various levels of cloud infrastructure unlike paper based writing. The criteria is wide enough to cover any storage device cable of retaining the information. These broad requirements leave more scope for disagreement regarding what terms and conditions were agreed between the parties. Arguably, in an online environment

\begin{itemize}
  \item \textsuperscript{8} Stanford School of Medicine, Cloud Computing: An Overview <http://med.stanford.edu/irt/security/cloud.html> 23 January 2013.
  \item \textsuperscript{12} Mik, above n 6.
\end{itemize}
additional factors such as technological variations and easy alterable ability of electronic documents make traditional paper-based safeguards even more crucial. The guidance provided under the legislation will be of little help from the perspective of agreed terms of a contract.

Australia, electronic transactions legislation gives legitimacy to all transactions that are performed entirely through electronic communications. It thereby grants the same legal status to electronic contracts as that of traditional paper-based contracts. Instead of amending every traditional law that makes either implied or express references to paper-based or traditional signatures, the legislation provides a general umbrella provision that covers all the traditional laws.\textsuperscript{13} The Act does not override any existing laws.\textsuperscript{14} It broadly removes legal impediments and allows transactions to be conducted through electronic mediums.\textsuperscript{15} The electronic transaction legislation has adopted a minimalist approach for the regulation of electronic transactions, which clarifies the legal status of contracts formed through electronic means.\textsuperscript{16} The \textit{Electronic Transactions Act 2000} (Victoria) intends to protect electronic transactions. Section 7(1) of the Act \textit{Electronic Transactions Act 2000} (Victoria) states that a transaction is not invalid for being conducted through electronic means.\textsuperscript{17} The Explanatory Memorandum\textsuperscript{18} states that the section does not by itself

\begin{itemize}
\item \textsuperscript{17} \textit{Electronic Transactions Act 2000} (Vic) s 7(1); E T Laryea, ‘Dematerialisation of Insurance Documents in International Trade Transactions: Need for Legislative Reform’ (2000) 23(1) \textit{University of New South Wales Law Journal} 78, 80; J Lambrick, ‘Managing Legal Risks in Web Contracting’ (2002) 52(1) \textit{Telecommunications Journal of Australia} 45, 47.
\item \textsuperscript{18} \textit{Electronic Transactions Bill 2000} (Vic) Explanatory Memorandum, 6.
\end{itemize}
establish the validity of a transaction. Thus, the electronic transaction legislation does not provide comprehensive or fully-fledged criteria for the formation of electronic contracts. Instead, it only provides minimum rules or criteria that facilitate the formation of contracts in an electronic medium. The legislation only reinforces that a transaction can take place in an electronic medium. It merely establishes equivalence between traditional transactions and electronic transactions; hence, the approach is disappointing. It is based on a functional equivalence and technology-neutral principle under which both paper-based transactions and electronic transactions are provided equal status. Discrimination is not made between different technologies. The Electronic Transactions Act 2000 (Victoria) deals with electronic communications and broadly defines electronic communication to include ‘a communication if the form of sound, where the sound is processed at this destination by an automated voice recognition system’. According to the Explanatory Memorandum, the electronic communication is intended to ‘capture information which is provided by voice in such a way that it enables it to be recorded in written form’. However, instead of the term ‘electronic communications’ as used in the Electronic Transactions Act 2000 (Victoria), the model law uses a much narrower term called ‘data massage’. Data Message means ‘information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram or telecopy’.

For a valid electronic contract to be formed, it is necessary to satisfy all the elements of traditional contract formation. The legislation only neutralises the position of electronic contracts by stating that if contracts are formed using electronic means then such contracts are valid.

---

19 Ibid.
24 Model Law on Electronic Commerce [art 2].
25 Fitzerald et al, above n 20, 513.
26 Electronic Transactions Act 2000 (Vic) s 7(1).
Section 7 (1) of the Act provides general validity to electronic transactions by stating:  

For the purposes of a law of this jurisdiction, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.

Section 3 (1) of *Electronic Transactions Act 2000* (Victoria) defines a transaction as follows:

Transaction includes any transaction in the nature of a contract, agreement or other arrangement, and also includes any transaction of a non-commercial nature.

Under s 3 (1) of the Act, a transaction includes contracts and agreements. Hence, both s 7 (1) of the Act and s 3 (1) facilitate formation of electronic contracts. The explanatory memorandum states that the term ‘transaction’ includes transactions of both commercial as well as non-commercial nature. However, the criteria is concerned primarily with providing general validity to electronic transactions. The Expert Group report outlined this as follows:

A provision covering the general statement of principle in article 11 of the Model Law is important to remove any uncertainty concerning the use and validity of data messages in contract formation.

The legislation is concerned primarily with providing general recognition to electronic transactions. It is important to note that it does not deal with contract formation principles such as acceptance and offer.

---

27 Ibid.
28 Ibid s 3(1).
Unlike the *Model Law on Electronic Commerce 1996*, the electronic transaction legislations contains an addition requirement of consent for satisfying the requirement of electronic writing and signatures. Under this provision the person to whom information in required to given must consent for the requirement to be satisfied electronically. The term consent is defined under the *Electronic Transactions Act 2000* (Victoria) as follows:

Consent includes consent that can reasonably be inferred from the conduct of the person concerned, but does not include consent given subject to conditions unless the conditions are complied with;

Under the *Electronic Transactions Act 2000* (Victoria) consent is defined to include: What can be reasonably inferred from the conduct of the concerned person but consent does not include the consent given subject to conditions unless those conditions are complied with. Sections 8, 9 and 10 of the *Electronic Transactions Act 2000* (Victoria) requires ‘consent’ in an electronic transaction. However, difficulties may arise in determining whether the conduct of a person amounts to a consent. Though express consent is not required, it is difficult to determine consent in an electronic transaction. The Explanatory Memorandum is also inconsistent in determining consent because, it suggests that, ‘consent can be inferred from a history of transactions or previous dealings’. Accordingly, prior correspondence through electronic communications may infer consent. However, the Explanatory Memorandum also suggests that,

“If a person should not, by the operation of this definition, be deemed to have consented to the receipt of information in the form of an electronic communication merely because they have sent or previously used electronic communications.”

---

34 *Electronic Transactions Act 2000* (Vic) s 3.
36 Ibid.
37 Explanatory Memorandum to the *Electronic Transactions Bill 2000* (Vic), 2.
Once again the Explanatory Memorandum states\(^{38}\) that if a person has used electronic mail to make an offer to a business, then that should be sufficient to allow the business to assume that the person has consented to receive an acceptance through electronic communication. Analysis of cases discussed below dealing with the requirement of ‘consent’ highlight the issue clearly.

The issue of obtaining consent before communicating through electronic means again arose in IIich & Anor and Baystar Corporation Pty Ltd.\(^{39}\) The relevance of electronic transaction legislation was discussed in this case. Jason Domenic Musca and Suzanne IIich were the proprietors of lot 8.\(^{40}\) In this case the validity of a by law was at issue.\(^{41}\) On 23 December 2003 McMohan under the signature of Melissa Bray of Mcmahon as Stata office Manager forwarded to the applicant an addendum to notice meeting.\(^{42}\) McMohan sent by laws by mail and asked the applicant to return a proxy by mail if they could not attend the meeting.\(^{43}\) Within 28 days the applicant sent a letter to McMahan by facsimile they referred to lot 8 as follows:\(^{44}\)

> “we are writing regarding the Resolution Without Dissent which required to adopt the by-law under Section 48(8) of the Strata Titles Act 1985 that would permit the retention of the ‘installation’ made to and in the common property comprising the Strata plan in connection with the Sushi Bar. We, Jason Domenic Musca and Julia Suzanne IIich, the co-operators of Lot 8 Unit 6 131 Royal Street, EAST PERTH Strata Plan 42040 hereby vote No to adopting the by-Law...”

The purported dissent consisted of the letter from the applicant sent by fax dated 22 January and a mail sent by email from Stephen.fraser@powerco.co.nz to the address beverly@mcmohanrealestate.com.au dated. The purported dissent was regarded as electronic communication under s 8 of Electronic communications Act 2003 (WA).

\(^{38}\) Ibid.
\(^{39}\) IIich & Anor and Baystar Corporation Pty Ltd [2004] WASTR 25.
\(^{40}\) Ibid para 2.
\(^{41}\) Ibid para1.
\(^{42}\) Ibid para 31.
\(^{43}\) Ibid para 32.
\(^{44}\) Ibid para 35.
In relation to s 8 of the Act it was found that consent could include implied consent as follows:45

‘Consent’ includes consent that can be reasonably inferred from the conduct of the person concerned. Section 8(1) ETA is not definitive in relation to when consent must exist. Paragraph 8(1) (a) ETA specifically refers to ‘at the time the information was given’ in relation to the expectation the communication was reasonably accessible but this would appear not to qualify paragraph 8(1) (b) ETA. However, both the ‘giving’ of the information and the ‘consent’ are expressed in the present tense, which may well indicate a legislative intention that, at the time the information was given, consent must exist. In other words, subsequent words or conduct are, strictly, irrelevant.

It was held that there was no valid consent to receive electronic communication as required under s 8 by McMahon as follows:46

If the applicants assert that the consent of the strata company was given by the conduct of McMahon’s, Baystar submits that there is no substantial evidence of that, certainly not consent to the receipt of a vote by e-mail. Note, for example, the specific direction by McMahon’s that proxy forms for the EGM were to be returned in a reply paid envelope. The later e-mail by McMahon’s (not referred to the Council and not authorised by them) replying to the then proprietor of lot 7 does not evidence consent by McMahon’s to the receiving by e-mail of Lot 7’s Purported Dissent. McMahon’s simply state in that e-mailed reply that the e-mail by the then proprietor of lot 7 had been forwarded to ‘the relevant parties’ (which it was not).

This outcome is consistent with the Electronic Transactions (Victoria) Amendment Act 201147. Under electronic transaction legislation of Australia transactions can be conducted electronically only if the parties consent to transact through electronic means. In Terumo Corporation v B Braun Melsungen48 it was held for the application of Electronic Transactions Act, if the parties do not specifically object to the mode of communication then implied conduct can be inferred from their conduct.

46 Ibid para 14.
47 Electronic Transactions (Victoria) Amendment Act 2011.
Similarly, in Aristocrat Technologies Inc v IGT\(^{49}\) it was established that implied consent can be inferred from the conduct of the parties if there is a long history of communication through electronic means. On similar lines, in Tugum Cobaki Alliance Inc v Minister for Planning and RTA.\(^{50}\) It was held that making a document available through electronic link also satisfies the requirement of writing under the electronic transactions Act. While, Department of Health and Human Services v H\(^{51}\) appears to indicate that consent can be determined only if there is evidence to prove it. Likewise, KM Ravich v King Island Council and BH Hassing\(^{52}\) it was held that the writing requirements were not satisfied as there was lack of clear consent. Similar view was also expressed in Illich & Anor and Baystar Corporation Pty Ltd.\(^{53}\) On the other hand, Kim v Minister for Immigration\(^{54}\) on 23 August 2005 indicates that the Electronic Transactions Act does not apply to the practice and procedures of the court. Similarly, in Re Ryan and Secretary, Department of Employment and Workplace Relations\(^{55}\) it was held that Electronic Transactions Regulation 2000(Cth) Specifically Exempts applicability of Administrative Appeals Tribunal Act 1975.

The electronic transaction legislation provides basic criteria for satisfying the writing requirement. It states that the requirement to provide information can be met in an electronic form. It also states that the person to whom information is provided in an electronic form must consent to receive that information. However it does not specifically defines what amounts to consent.\(^{56}\) Although the new criteria specifically makes reference to contracts it does not provide any criteria for satisfying ‘consent’ requirements. Therefore like the current legislation the proposed amendments are also unsatisfactory.

The criteria dealing with writing is primarily concerned with the inadequacies created due to electronic form. It does not intent to cover traditional functions of

\(^{49}\) Aristocrat Technologies Inc v IGT (2008) 80 IPR 413.
\(^{50}\) Tugum Cobaki Alliance Inc v Minister for Planning and RTA [2006] NSWLEC 396.
\(^{51}\) Department of Health and Human Services v H (Ref No. 26/2011) [2011] TASWRCT 7.
\(^{52}\) KM Ravich v King Island Council and BH Hassing [2007] TASSRMPAT 226.
\(^{53}\) Illich & Anor and Baystar Corporation Pty Ltd [2004] WASTR 25.
\(^{54}\) Kim v Minister for Immigration BC200608625.
\(^{55}\) Re Ryan and Secretary, Department of Employment and Workplace Relations (2005) 90 ADL 800.
\(^{56}\) Ibid, para 2.4–2.5
writing such as permanent retention of the consents of a document. The Expert Group described the need of the criteria as follows:⁵⁷

The law in Australia includes a number of different form provisions which require a document to be in writing. In a number of instances, it is unlikely that an electronic form of document or signature would satisfy their requirements.

During the preparation of Model Law on Electronic Commerce, UNCITRAL considered various functions performed by traditional writing, such as:⁵⁸

1. enabling parties to be aware of the consequences of entering into a contract
2. ensuring that a document would be legible
3. ensuring that a document would remain unaltered over time
4. providing permanent record of the contents

However, while considering the criteria for writing. The Expert Group outlined the limited scope of the above criteria and stated that it:⁵⁹

Focused upon writing as the lowest level in hierarchy of form requirements which provide for distinct levels of reliability, traceability and inalterability with respect to a paper document…

Particularly, by being minimalist in nature, it avoids comprehensive requirements. In fact, the writing requirement prescribed under the Australian electronic transaction legislation only provides basic standards to be met by an electronic document. As mentioned above, traditional paper-based writing provides a permanent record of terms and conditions agreed between the contracting parties. It is worth noting that permanent retaining of record is not the prerequisite of the legislation. The legislation has sidestepped the requirement. It solely requires ‘accessibility’ and ‘usability’. It appears that there is no intention to extend terms such as ‘accessibility’ and ‘usability’ to cover specific retention of the contents. While electronic writing has been validated under the legislation, it does not address the issue of integrity of the

---

contents of the document, which can have much broader implications. Therefore, the criteria leaves wide scope for ambiguity for instance, In *Re David Scott Ellis; Ex Parte Triple M Mechanical Services Pty Ltd* it was argued that the email attachment was not accessible as the email attachment was sent as a compressed file and the receiver did not have the necessary decompressing software. In *Curtis v Singtel Optus Pty Ltd and Anor*, it was noted that requirement to produce document in writing will be satisfied only when the electronic document is downloaded and printed out in a paper form.

The criteria provided under the legislation wide enough to cover any storage device cable of retaining the information. These broad requirements leave more scope for disagreement regarding what terms and conditions were agreed between the parties. Arguably, in an online environment additional factors such as technological developments and easy alterable ability of electronic documents make traditional paper-based safeguards even more crucial. The guidance provided under the legislation will be of little help from the perspective of agreed terms of a contract. Unfortunately, non-assurance of agreed terms and condition of an electronic contract can discourage contracting parties from effectively using electronic media for contract formation. Therefore, although the legislation intends to facilitate effective formation of electronic contracts, it cannot be regarded as an adequate facilitator due to these limitations. It appears clear that gaps in relation to agreed terms of a contract persist.

Additionally, examination of issue in relation to electronic contracts formed through mobile phones illustrate further difficulties. Data stored in a mobile phone in the form of a text SMS or in the memory of a SIM card (subscriber Identity Module) can also amount to writing under the broad criteria provided under the electronic transactions legislation of Australia discussed above. Mobile phones can be stolen easily thereby making data tampering relatively easy and also leading to easy data

---

60 *Electronic Transactions Act 2000* (Vic) s 8(5).
61 *Re David Scott Ellis; Ex Parte Triple M Mechanical Services Pty Ltd* [No 2] [2013] WASC 161 (2 May 2013).
63 *Electronic Transactions Act 2000* (Vic) s 8(5).
loss. Mobile phones can be easily stolen as seen in *Hayek v R*, *Johnson v R*, *Director of Public Prosecutions (DPP) v Malikovaski*, *Joyce v Gee*, *Nanai v R*, *Dolan v R*, *Devine v R*, *Director of Public Prosecutions (DPP) v Kuru*, *R v Mann* and *R v Harris*. Thus, data can be more easily tampered, destroyed and lost in case of mobile phones. Hence, all the above shortcomings do not assure enforceability of electronic contracts in the same way as paper-based contracts do. Thus, broad writing requirements do not appear to be appropriate for electronic contracts.

Moreover, in case of electronic contracts formed through mobile phones, evidence of text message from a mobile phone and memory of a SIM card appears to be acceptable as evidence only if the data is accurate as seen in *Bevan v The State of Western Australia*. Clearly, this can add another layer of issue in the context of electronic writing by creating evidentiary issues.

7.3 The Validity of Electronic Signatures and the Effect of Electronic Signatures

Before examining the effect of electronic transaction legislation in Australia on electronic signatures, it is necessary define the terms authenticity, trust, non-repudiation and integrity. It is also necessary to explain the relationship between these terms. Further, it is important to analyse the reliability of different types of electronic signatures.

Moreover, under a cloud computing infrastructure a user will not know who is accessing their document and the data cannot be monitored in any way. The user cannot be sure that a confidential file which they delete has in fact been deleted from

---

64 *Hayek v R* [2010] NSWCCA 139.
66 *Director of Public Prosecutions (DPP) v Malikovaski* [2010] VSCA 130.
67 *Joyce v Gee* [2010] WASC 76.
70 *Devine v R* [2009] NSWCCA 261.
71 *Director of Public Prosecutions (DPP) v Kuru* [2009] VSCA 206.
72 *R v Mann* [2009] VSC 536.
73 *R v Harris* [2009] VSCA 189.
74 *Australia Bevan v The State of Western Australia* [2010] WASCA 101 paras 15–16.
the system. As the cloud computing technology can always store a backup file. Cloud computing fully depends upon the internet for access and is therefore prone to security risks twenty four hours a day. Documents and data are processed outside the company therefore inherent risks are always involved. In cloud computing technology outsourced services bypass the physical, logical and personal controls. In desktop based documents data can be recovered from the hard drive of the laptop or desktop computer. In contrast, in case of cloud computing data is stored online hard drive cannot be removed to recover data.

Under traditional desktop based models administrative access to servers and is controlled though on premises. While in cloud computing administrative access is though internet exposing the organisation to risks. Many times user credentials are stored outside the organisation in cloud infrastructure. Therefore companies must ensure that the accounts of employees are removed from the cloud infrastructure once they leave the company. Virtualization is one of the key components of cloud computing. Virtualised machines can be paused, restarted and reverted to earlier instances. Due to this dynamic structure of cloud computing security cannot be maintained constantly.

Under s 8 of the electronic transaction legislation, the requirement to give information in writing is satisfied if the information provided is accessible and usable for subsequent reference. It merely focuses on ‘accessibility’ and ‘usability’. It does not specifically deal with retaining contents in a stable manner. Electronic documents differ from paper based documents they are not only created but also processed through the cloud infrastructure. Online writing becomes accessible via various levels of cloud infrastructure unlike paper based writing. The criteria is wide enough to cover any storage device cable of retaining the information. These broad requirements leave more scope for disagreement regarding what terms and conditions were agreed between the parties. Arguably, in an online environment

75 Stanford School of Medicine, above n 8.
76 Gartner, above n 9.
77 Dwachira, above n 10.
78 Padhy et al, above n 11.
79 Electronic Transactions (Victoria) Amendment Act 2011.
80 Mik, above n 6.
additional factors such as technological variations and easy alterable ability of electronic documents make traditional paper-based safeguards even more crucial. The guidance provided under the legislation will be of little help from the perspective of agreed terms of a contract.

Before examining the effect of electronic transaction legislation in Australia on electronic signatures, it is necessary define the terms authenticity, trust, non-repudiation and integrity. It is also necessary to explain the relationship between these terms. Further, it is important to analyse the reliability of different types of electronic signatures.

7.3.1 Trust

The existence of trust between parties for the success of an electronic contract or transaction with an electronic signature is very important. In order to conduct efficient business transactions, parties must be satisfied with the trustworthiness of the medium. According to the Commission of the European Communities, trust is of great significance and the Commission of the European Communities states as follows:

The first objective is to build trust and confidence. For e-commerce to develop, both consumer and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce.


In order to prove that the electronic contract is trustworthy, it is necessary to consider interrelated concepts of authenticity, integrity and non-repudiation.84

Authenticity deals with the source or origin of a communication and identifies the sender of the message.85 The importance of a traditional signature lies in the fact that the contracting parties can use signatures as a means to identify the parties in a traditional contract. Such an identification of a traditional signature and authentication of a traditional contract is much easier because in most instances, such signatures or seals are affixed physically in the presence of the parties to a contract in traditional contracts.86

Integrity in an electronic contract deals with the accuracy and completeness of the electronic transaction or electronic communication.87 In the case of an electronic signature, integrity establishes the accuracy and completeness of the signature. Integrity concerns with the complete document and highlights if the recipient has received the same document as the one sent by the sender. The recipient of an electronic contract must be confident of the integrity of electronic communication before the recipient relies and acts on the electronic contract.88

Non repudiation prevents a party from denying a communication that has been sent by the same party.89 It is the ability to hold the sender responsible for sending the communication and prevent the sender from denying that he or she has sent the communication. In an electronic contract, a party’s confidence to rely on a contract is based upon knowing that the party can prevent the sender of the electronic

86 L Fuller, ‘Consideration and Form’ (1941) 41 Columbia Law Review 799, 800.
87 Lawrence and Saurajen, above n 82; Smedinghoff and Bro, above n 84.
communication from denying the fact that he or she has sent the electronic communication.  

7.3.2 Features of Electronic Signatures

There are different types of electronic signatures. In the simplest electronic signature, the signatory can type his or her name at the bottom of the electronic document. There are various other types of electronic signatures such as biometric signatures, passwords, personal identification number (PIN), typed name or scanned bitmap signature and names typed at the end of an email. Many businesses offer commercial websites that display terms and conditions of business and require the user to accept the offer by clicking on an ‘I accept’ or ‘proceed’ button. Further, a traditional signature can be scanned and attached to an electronic document. The reliability of the Biometrical systems and devices can be tampered if a low threshold is set for the reference template. Identification information of a person such as passwords and public keys can also be stolen easily. Similarly, other types of electronic signatures can be easily tampered.

---


None of the electronic signatures or technologies connected with electronic signatures display qualities of handwritten signatures and this nature of the electronic signatures affects their ability to perform the functions of the handwritten signatures. Some of the functions of the handwritten signatures include, identification of author or sender or signatory of a document; authentication of statements in a document so that the facts are confirmed; declaration of intention to be legally bound; representation that the signatory was authorised to perform any legal act; safeguard against undue haste or thoughtlessness; and confirmation that the signatory had notice of the contents of the document and acknowledgment that the document is original. If businesses and consumers cannot be satisfied about the authenticity of electronic signatures, there is little likelihood of electronic commerce becoming the standard and benchmark mark of international transactions.

7.3.3 Electronic Transaction Legislation, Signatures and Response to the international norms

The Electronic Transactions (Victoria) Amendment Act 2011 made amendments to the Electronic Transactions (Victoria) Act 2000 to include a new criteria dealing with the signature requirement.

The basic rules of the electronic transaction legislation are based upon the approach of functional equivalence. Requirement for paper was used to study whether


electronic contracts meet functional equivalence and serve the same purpose as that of a traditional contract made on paper. Accordingly, few amendments were recommended. For validity of a contract under common law, a signature is not a requirement. Similar to the current electronic transaction legislation, Article 9.3 of the Convention recognises the principles of technology neutrality.  

The overall minimum requirements to be met by a signature in electronic media for satisfying the criteria of traditional or paper based signature is similar to the requirement under the old electronic transaction legislation. The old electronic transaction legislation used the term ‘approval’ instead of ‘intention’ because the only purpose of signature is to identify the signatory. Accordingly, the consultation paper suggested that:  

2) The ETAs should be amended to change the wording in the signature provisions from ‘indicate the person’s approval’ to ‘indicate the party’s intention’ in respect of the information communicated. 

Additionally, in relation to signature requirements the report proposed additional test as follows:  

3) There should be an additional provision to the signature provisions as a safeguard to prevent parties from arguing that a signature fails the objective reliability test. This is where the method can be proven in fact to have identified the signatory and indicated the signatory’s intention in respect of the information contained in the electronic communication. 

Further, the signature requirements are fine tuned by means of a refined test which add another layer of protection. The refined test for the signatures is presented as follows:  

Third, the ETAs do not contain equivalent provision to article 9.3 (b) (ii). The explanatory note to the Convention indicates that a party should not be allowed to invoke the ‘reliability test’ in bad faith to repudiate its signature. 

---

100 Ibid para 2.10.  
102 Ibid 16.  
103 Ibid 17.  
should not be able to be invalidated on the ground that the electronic signature was not appropriately reliable for the circumstances if there is no dispute in fact about the identity of the person signing or the fact of signing.

Accordingly, the new signature criterion slightly improves the criteria provided for signature under the old electronic transaction legislation. It further clarifies the minimalist criteria provided under the old Act and also enables the introduction of evidence to prove the signature method. Again, by being minimalist in nature it has not specifically dealt with authenticity and integrity. However, it appears to have slightly reduced the risk of non-repudiation, as it prevents parties from an argument that signature does not satisfy reliability. Notably, this criterion is not completely convincing. The amendment only states that a contract should not be repudiated if identity is not disputed. This test can only apply if the identity of the party is not really in dispute.\textsuperscript{105} It is not concerned with situations when a signature is impersonated. Therefore, it is not adequate and its usefulness can be questioned.

The criteria dealing with signature is primarily concerned with the inadequacies created due to electronic form. It was not intended to address the issues associated with authenticity, integrity and non-repudiation. The Expert Group states: \textsuperscript{106}

It is our view that the enactment of legislation which creates a detailed legislative regime for electronic signatures needs to be considered with caution. There is the risk particularly given the lack of any internationally uniform legislative approach, that an inappropriate legislative regime may be adopted without regard to market-oriented solutions. Given the pace of technological development and change in this area, it is more appropriate for the market to determine issues other than legal effect, such as the levels of security and reliability required for electronic signatures. Accordingly, we have recommended that legislation should deal simply with legal effect of electronic signatures.

The electronic transaction legislation suffers from many drawbacks. For example, the \textit{Electronic Transactions Act 2000} (Victoria) covers all electronic signatures and also

\textsuperscript{105} Ibid.

covers digital signatures and focuses on the functionality of the signature. However, the electronic transaction legislation does not expressly state that the signature method must be contained in the electronic communication. The requirement of signature method is that it indicates approval by the sender of the contents of the communication means. To fulfil this requirement, there must be some nexus between the signature and the communication.

Difficulties can arise when certain signature technology becomes obsolete due to technological innovations. In such a situation, the onus lies on the signatory to keep up-to-date with technological developments. The difficulty of this requirement may be overcome by making the signature method appropriate only at the time it was used. The appropriateness of a signature method depends on a number of legal and technical factors, which include:

1. The function of signature requirements in relevant statutory environment;
2. The type of transaction;
3. The capability and sophistication of the relevant communication systems;
4. The value and importance of the information in the electronic communication

In order to use an electronic signature, the electronic transaction legislation also requires the consent of a person. This was based on general policy that a person must not be forced to use an electronic communication to form a contract or conduct any transaction electronically to satisfy the requirement of traditional laws. Instead, a person must have a choice to conduct transactions electronically.

---


110 Lawrence, above n 107; Lawrence and Williams, above n 107.

explanatory memorandum of the bill, consent can be determined from the conduct of
the parties.\textsuperscript{112}

An analysis of signature cases indicates how doctrines are being developed to
recognise electronic signatures and how they are limited. The intention of the
signatory is important, a signature may appear on a document but the signer will not
be regarded as bound if the intention is lacking.\textsuperscript{113} Electronic signatures can be
tampered easily and may appear to be from some other person as discussed above.
Hence, intention of a signatory cannot be easily determined when electronic
signatures are used. However, electronic signatures can be authenticated with the
help of facts and circumstances of the case as seen in \textit{R v Frolchenko}.\textsuperscript{114} In \textit{R v
Frolchenko}\textsuperscript{115} Williams J recognised that modern means of communications may not
contain a personal signature and stressed the importance of authenticating such
communications based on facts of the case as follows:\textsuperscript{116}

One incidental argument raised by counsel for the appellant was that the
document in issue was not signed, in the sense that there was no personal
handwritten signature. However, at the conclusion of the document the name of
a firm of solicitors appeared in typescript. Particularly given modern methods of
communication (for example, E-mail) many communications in writing will not
bear either the original or the facsimile of a personal signature. What remains of
importance in all cases is that the document be authenticated, and that it be
established as a fact, where relevant, that a particular party to the litigation was
responsible for the communication.

Thus, a combination of factors such as conduct of parties and spoken words can help
in determining the intention of the signatory. However, in rare situations

\textsuperscript{112} \textit{Electronic Transactions Bill 2000} (Vic) Explanatory Memorandum.
\textsuperscript{113} \textit{R v Moore; Ex parte Myers} (1884) 10 VLR 322; \textit{R v Moore; Ex parte Myers} (1884) 10 VLR 322;
17 August 2009.
\textsuperscript{114} \textit{R v Frolchenko} (1998) QCA 34; \textit{The Queen v Stefanie Frolchenko} (Unreported, Supreme Court of
Queensland Court of Appeal P Fitzgerald, J A McPherson and J Williams, 3 March 1998, 20 March
1998); Davidson, above n 113.
\textsuperscript{115} \textit{R v Frolchenko} (1998) QCA 34; \textit{The Queen v Stefanie Frolchenko} (Unreported, Supreme Court of
Queensland Court of Appeal P Fitzgerald, J A McPherson and J Williams, 3 March 1998, 20 March
1998).
\textsuperscript{116} \textit{The Queen v Stefanie Frolchenko} (Unreported, Supreme Court of Queensland Court of Appeal P
determination of intent may rely solely on electronic signature alone. Electronic transaction legislation is not concerned with such situations. Further, the approach adopted in *R v Frolchenko* can also be problematic if there are no surrounding external circumstances to recognise a person and the available electronic signature is also impersonated. This approach can only apply if there are external offline circumstantiates surrounding the issue. Hence, suffers from limitations. This approach cannot apply in the absence of adequate offline surrounding circumstances associated with the signatory.

Similarly, in *McGuren v Simpson*, the court considered whether correspondence by email could be acknowledged as a written and signed transaction or communication or document for the purpose of the *Limitation Act 1969* (NSW). The only legal decision in Australia about whether general law principles allow an electronic signature to satisfy the signing requirement under statutory law is seen in *McGuren v Simpson*, which considered whether an email was capable of constituting an acknowledgement in writing and signed for the purposes of the *Limitation Act 1969* (NSW) because the defendant was able to produce a printed email sent to him by the plaintiff, which contained the plaintiff’s typewritten name. While the court held that this constituted a sufficient signature, the court applied the ‘authenticated signature fiction’ in *McGuren v Simpson*, which is as follows:

Where the name of the party to be charged appears on the alleged note or memorandum, for example, because it has been typed in by the other party, the so-called ‘authenticated signature fiction’ will apply where the party to be charged expressly or impliedly acknowledges the writing as an authenticated expression of the contract so that the typed words will be deemed to be his or her signature. This principle has no application to a document which is not in

---

117 Davidson, above n 193.
123 Christensen et al, above n 201, 29.
some way or other recognisable as a note or memorandum of a concluded agreement.

Since the plaintiff’s name appeared in the email and the email contained authentication of a prior agreement, the email was considered a note of a concluded agreement and hence, the plaintiff’s typewritten name was held to be a ‘signature’. However, ‘authenticated signature fiction’ will apply only when the party expressly or impliedly acknowledge the writing as an authenticated expression of the contact. Hence, this approach suffers from limitations. It cannot apply in situations when a person denies a signature and makes a claim of fraud.

Further, in traditional signatures and traditional contracts that are paper-based, a party can rely on a number of indications of trust in order to determine that the signature is authentic and the document or traditional contract has not been altered. These indicators include the use of paper on which the transaction or contract is written and that cannot be easily altered. Letterheads, ink signatures of parties affixed personally, sealed envelopes delivered through trusted parties and personal contact between the parties to a contract act as indicators of trust. Such indicators of trust do not exist in electronic contracts and electronic signatures. Electronic contracts and electronic signatures are mostly in bits and pieces, which are identical and they can be easily modified and copied.

However, even in traditional offline transactions, parties of a contract have no authentication of traditional signatures until a dispute arises. Thus, even in traditional transactions, contracting parties accept the risk factor. However, the risk factor is further increased in online transactions due to the inherent insecure nature of these transactions.

---

126 Christensen et al, above n 201, 29.
128 Ibid.
129 Davidson, above n 113.
130 Electronic Transactions Act 2000 (Vic).
In *Faulks v Cameron*, the Supreme Court of Northern Territory considered the effectiveness of an electronic signature under the Australia’s electronic transaction legislation. *Faulks v Cameron* involved an action for an adjustment of property interests under Division 3 of Part 2 of the *De Facto Relationships Act 1991* (NT). After living together for 2 years in a *de facto* relationship, the parties separated and in 2003, the plaintiff informed her former partner that she was preparing a separation statement. In the meantime, the defendant had moved out of the country and the only means of communication between the plaintiff and the defendant took place though emails because the defendant did not provide his postal address. One of the issues raised in *Faulks v Cameron* was whether a separation agreement between two *de facto* partners had been formed for the purposes of the *De Facto Relationships Act 1991* (NT). Under s 45(2) of the *De Facto Relationships Act 1991* (NT), where the court is satisfied that there is a separation agreement between the partners and the agreement is in writing and signed by the other partner, then the court may make an order under Division 3 or 5 of Part 2, but the court may not make an order that is inconsistent with the agreement.

In the application, the plaintiff submitted that the correspondence by email amounted to a separation agreement. She also submitted that if the court did not consider the correspondence by email constituted a separation agreement then the court may consider what was agreed by email correspondence. The learned judge concluded first that even though the evidence was not overwhelming, there was an agreement between the former partners and that it was enforceable at common law. The second issue in *Faulks v Cameron* was whether the correspondence by email was signed. In the email, the defendant signed his name at the bottom of the text as ‘Regards, Angus’. While applying the provisions of s 9 of the *Electronic Transactions Act 2000* (NT) to the name, that was typed at the bottom of the email, Acting Master Young concluded as follows:

---

132 Ibid.
133 Mason, above n 119, 281.
135 Mason, above n 133, 281.
137 Mason, above n 133, 281.
I am satisfied that the printed signature on the defendant’s emails identifies him and indicates his approval of the information communicated, that the method was as reliable as was appropriate and that the plaintiff consented to the method. I am satisfied that the agreement is ‘signed for the purpose of s45(2).

The decision in *Faulks v Cameron* has been criticised for failing to offer any guidance on the potential scope and application of the legislation. However, it is debatable whether there was a requirement for any further analysis. The *Electronic Transactions Act 2001* (Queensland) and other related uniform Electronic transaction legislation in Australia do not apply to any transaction that has taken place before the legislation came into operation as seen in *McGuren v Simpson*. The court considered whether correspondence by email could be acknowledged as a written and signed transaction or communication or document for the purpose of the *Limitation Act 1969* (NSW).

Emails address can also be regarded as a signature under the electronic transaction legislation of Australia. *Points North* highlights the difficulties which can arise from such a liberal view. In this case Points North title scheme was registered as a building units plan consisting of 141 lots. It operated under the. On 1 April 2006 owners of lot 33 and lot 65 sent emails to the body corporate manager. The emails notified the lot owner’s withdrawal of their nominations. On 3 April 2006 the body corporate manager acknowledge receipt of withdrawal of nomination. On the same day the owner of lot 65 informed the body corporate manager that he wishes to reestablish the nomination. While, the owner of lot 33 informed the body corporate manager that she has no knowledge of withdrawal of nomination although both the emails were received from the same email address alanf1936@hotmail.com. The body corporate manager notified both the owners that their withdrawals were accepted and will not be included in the secret ballot for elections of the committee.

---

141 Mason, above n 133, 281.
143 *Body Corporate and Community Management (Standard Module) Regulation 1997 Points North* [2006] QBCCM 212.
144 Ibid.
The body corporate manager relied on *Electronic Transactions Act 2001* (ACT) for accepting information in electronic form from the owners. It was held that the notice of nomination of the owner of lot 33 was not cancelled while the notice of withdrawal of the owner of lot 65 was cancelled as no allegations of email tampering were made by him as follows:¹⁴⁵

On the face of the evidentiary material, I can understand why the applicant believes it is entitled to reject the nomination by the owner of lot 33. Indeed, under the Electronic Transactions Act, in the absence of evidence to the contrary, a person is entitled to rely upon an e-mail communication as if it were a written communication. However, the owner of lot 33 has submitted a statutory declaration denying that she requested the withdrawal of her nomination. It would appear to me that the only explanation is that someone has accessed the lot owner’s e-mail account without her consent. No such allegation has been made by the owner of lot 65, and consequently, I believe that the nomination by lot 65 has been withdrawn and cannot be reinstated. Given the limited time available, the absence of power to cross examine the parties and otherwise “test the evidence”, it is difficult to me to make specific findings of fact as to whether the applicant did, or did not, send the subject e-mail withdrawing her nomination.

Relevance of electronic transactions legislation was discussed in *Asher v Seabrook*¹⁴⁶ the first respondent file petition under the *Bankruptcy Act* 1966. The Second responded was the trustee.¹⁴⁷ The applicant argued that the proposal of Seabrook was inappropriate as it was sent by email and was not signed by Seabrook. Section 10 of the *Electronic Transactions Act 1999* (Cth) was considered to assess the validity of the signature. While considering s 10 of the Act Wilson Fm Stated:¹⁴⁸

….in my view, the application of that section probably saves the proposal in this case, although that argument is best left for another day. The learned authors of McDonald, Henry & Meek Australian Bankruptcy Law &Practice at [73.1.05] say the requirement for personal signature is explicit (citing Re Blucher (Prince); ; Ex parte Debtor [1931] 2 Ch 70). However, no regard has been given to the statute to which I have been referred

---

¹⁴⁵ Ibid.
¹⁴⁷ Ibid para 1.
¹⁴⁸ Ibid para 23.
Harding v Brisbane City Council & Ors\(^{149}\) this case was regarding submitter appeal. An online service was established by the council through which submissions could be made. There were some mandatory fields in the system which required some identification such as a driver’s license number. Driver’s license number was wrongly entered by Mr Harding. The court considered the *Electronic Transactions Act 2001* (Qld) which states the requirement for a signature can be met in an electronic form. Wrong reproduction of few digits might be regarded as inappropriate for the signature requirements provided under s 14(a) and (b) of the Act. However, it was held that mere reproduction of one wrong digit did not raise any concern in the present case.

Importance of electronic signature was discussed in *Corneloup v Adelaide City Council*\(^{150}\) By laws were passed by the Adelaide City Council which prohibited preaching and Canvassing on trees.\(^ {151}\) Caleb Corneloup is the president of an incorporated association. The association perches and administers gospel around the city.\(^ {152}\) The association submitted applications to the Adelaide city council which sought permission for preaching.\(^ {153}\) The association also claimed that the bylaws were invalid under the *Local Governments Act 1999* (SA).\(^ {154}\) The Responded had the authority to make by laws under the *Local Governments Act 1999* (SA).\(^ {155}\) Section 249 (4) of the Act states that a council can make a bylaw only after obtaining a certificate in the prescribed form signed by a solicitor which must certify that in the opinion of the solicitor the council has the authority to make such by laws.\(^ {156}\) As per the requirements of the Act, the Adelaide city council requested a solicitor to prepare certificates of validity, reports to the legislative Review Committee on the application of the by- laws. Solicitor was also instructed to prepare reports for the consideration of the council regarding the implications of by laws in the light of the National Competition policy. The Solicitor prepared the required documents between

\(^{149}\) Harding v Brisbane City Council & Ors [2009] QPELR 207.

\(^{150}\) City Council Corneloup v Adelaide City Council [2010] SADC 144.

\(^{151}\) Ibid para 1.

\(^{152}\) Ibid para 2.

\(^{153}\) Ibid para 3.

\(^{154}\) Ibid para 5.

\(^{155}\) Ibid para 67.

\(^{156}\) Ibid para 41.
29 April and 3 May 2004. Another member of Adelaide city council instructed the Solicitor to send these documents electronically to him. According to s 9 of the *Electronic Transactions Act 2000*(SA) each certificate of validity included the name of the solicitor as a method of identification and approval.\(^{157}\) The council member decided to create a new document by cutting and pasting parts of the document received from the solicitor.\(^{158}\) Thus, requirements of s 249 (4) of the *Local Governments Act 1999* (SA) which requires a council to give a certificate signed under the *Electronic Transactions Act 2000*(SA) was not fulfilled. A new subsequent document was created by the council member after receiving the electronic document from the solicitor.\(^{159}\) The respondent argued that that the requirements of signatures provided under s 9 of the *Electronic Transactions Act 2000*(SA) were fulfilled.\(^{160}\) Under s 9 (1) 9a) of the Act a signature method must identify a person and indicate a person’s approval. In this case an email was sent by the solicitor to the council member which enclosed the documents without substantive comments. The document had a specific the place for signature but there was no signature, there was a place for date but there was no date written in the document. Further, the electronic document was converted into a new different document by the council member and was included in the agenda papers of the council meeting.\(^{161}\) Judge Stretton concluded that the signature was not valid under the under s 9 of the *Electronic Transactions Act 2000*(SA).\(^{162}\)

Here, the Council were provided with what looked like an unsigned and undated draft, with only a moderate indirect inference in the agenda papers that it was a certificate signed by the solicitor. The form the agenda papers took was to cite the legislative requirements for a certificate, then just say “(attachment E)”. Attachment E was then, as it appeared to Council, an apparently unsigned and undated draft, with only a moderate indirect inference in the agenda papers that it was a certificate signed by the solicitor. The form the agenda papers that it was a certificate signed by the solicitor. The form the agenda papers took was to cite the legislative requirement for a certificate, then just say “(attachment E)”. Attachment E was then, as it appeared to Council, an apparently unsigned and undated draft, with only a moderate indirect inference in the agenda papers that it was a certificate signed by the solicitor.

---

\(^{157}\) Ibid para 77.  
\(^{158}\) Ibid para 92.  
\(^{159}\) Ibid para 93.  
\(^{160}\) Ibid para 96.  
\(^{161}\) Ibid para 98.  
\(^{162}\) Ibid para 99.
undated document. The document had a place signified by dotted lines for a signature, with no signature on those dotted lines. To be satisfied that the certificate and contents therein was approved of by the solicitor required a range of assumptions. In particular, that despite the absence of any information from the solicitor or from the agenda papers, the document was not the draft it appeared to be, and that the solicitor had approved the information. That required accepting that what was there was what had been provided by the Council solicitor to the council employee drawing up the minutes. Paradoxically I believe that was a reasonable inference, although only Just, notwithstanding that the evidence shows that was not actually the case.

Judge Stretton then found that in relation to s 9 (1) (b) of the *Electronic Transactions Act 2000* (SA) signature method was not appropriate and reliable in this case:

Secondly, per section 9(1) (b) , that having regard to all relevant circumstances at the time the method was used, the method was reliable as was appropriate for the purpose for which the information was communicated. For the following reasons, I do not believe this was the case. As a matter of fact, the method adopted here, that of an unsigned certificate being provided in a readily alterable Word format to a Council employee, who regarded it as acceptable to alter the document and provide a new document to a Council employee, who regarded it as acceptable to alter the document and provide a new document to Council, resulted in a new altered document being provided to Council with no indication of date or signature. In this situation where the statute plainly requires a signed document in a specific prescribed form to be provided to Council as an important safeguard for both the Council and the wider community against invalid by-laws, the method adopted was at least casual, if not risky and haphazard. It would have been a very simple matter for the Form 8 pro forma to have been correctly drafted, then actually signed and dated, then either conveyed the very short distance from the solicitor’s office to the Council’s office, or sent electronically in any number of unalterable electronic formats which allow the receiver to see a true image of the original signed Certificate of Validity.

163 Ibid para 100.
Judge Stretton highlighted that the consent requirements provided under s 9(1) (c) of the *Electronic Transactions Act 2000*(SA) were not fulfilled.\(^{164}\) While upholding that the consent requirements prescribed under s 9(1) (c) of the *Electronic Transactions Act 2000*(SA) were not satisfied Judge Stretton stated:\(^{165}\)

Thirdly, per section 9(1) (C), that the person to whom the signature is required to be given consents to that requirement being met by way of the use of the method mentioned. It is clear that the Council never considered this issue, let alone consented to the method used. The Council would not have known the method used, from the very sparse information contained in the agenda material provided to them to which I have referred. They did not know that an unsigned undated word document was sent to a Council employee, which was then altered, and a new and different document provided by that Council employee, and that the document they received was not in the required prescribed form. It is clear that the person in this case who must receive the signature is the decision-making entity that either is to approve or not approve the recommended by-law, ie the Council in its decision making forum. That is also the forum that would need to know about, consider and consent for the purposes of section 9(1) (c).

The emphasis in Australia and also under *Electronic Transactions Act 1999* (Cth) is on the manifestation of intention and appropriate method for a particular transaction. Seen from this perspective, *Faulks v Cameron*\(^ {166}\) highlighted the method and the appropriateness of the method for the particular transaction. In this case, two persons who were separated exchanged emails and the plaintiff successfully sought that the correspondence by email constituted a separation agreement.\(^ {167}\) In *Getup Ltd v Electoral Commissioner*.\(^ {168}\) Electronic enrolment was lodged with electoral commissioner. Electronic signature fixed to the form was not regarded as sufficient as it consisted of broken lines and was not an exact match of the original signature. The validity of electronic signature was upheld in these cases as the commissioner had accepted similar pixilated signatures sent by means of email and fax on earlier

\(^{164}\) Ibid para 102.
\(^{165}\) Ibid para 101.
\(^{167}\) Mason, above n 133, 241–2.
occasions. These case has only established that electronic signatures are valid. In *Lang v The Leasing Centre (Aust) Pty Limited and Anor*,\(^{169}\) the signature was regarded as valid only because no allegation of fraud, duress or misleading conduct was made.

Protection extended to electronic signatures and electronic communication such as email is not adequate. The security of electronic communications and emails have raised concerns in *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson*,\(^ {170}\) and *CSX Transportation, Inc. v Recovery Express, Inc.*\(^ {171}\) These cases have demonstrated that those who enter into contracts electronically must take necessary level of care to avoid adverse consequences that is required in the paper-based contracts. Similar concerns and problems regarding the integrity and reliability of emails and electronic signatures can arise in Australia.

Protection extended to electronic signatures and electronic communication such as email is not adequate. The security of electronic communications and emails have raised concerns in *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson*,\(^ {172}\) and *CSX Transportation, Inc. v Recovery Express, Inc.*\(^ {173}\) These cases have demonstrated that those who enter into contracts electronically must take necessary level of care to avoid adverse consequences that is required in the paper-based contracts. Similar concerns and problems regarding the integrity and reliability of emails and electronic signatures can arise in Australia.

In *CSX Transportation, Inc. v Recovery Express, Inc.*,\(^ {174}\) the issue related to an email that could constitute a binding signature. In this case, *CSX Transportation, Inc. v Recovery Express, Inc.*,\(^ {175}\) the buyer Albert Arillotta sent CSX and email expressing an interest in buying out of service railroad cars. He represented himself to be from

\(^{169}\) *Lang v The Leasing Centre (Aust) Pty Limited and Anor* [2014] VCC 910 (20 June 2014).


\(^{172}\) *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Martenson*, Case No 1: 2008cv07833 (NYSD, 2008).


\(^{174}\) Ibid.

\(^{175}\) Ibid.
Interstate Demolition and Recovery Express and his email was albert@recoveryexpress.com. When Arillotta’s cheque bounced, CSX attempted to recover the purchase price from Recovery Express. CSX filed its claim for breach of contract against recovery Express and Recovery Express moved for summary judgment. In fact, Arillotta never worked for Recovery Express but he was affiliated with Interstate Demolition. Both the companies shared office space and the employees of these two companies shared email services.176

Len Whitehead, who entered the contract electronically on behalf of CSX, argued that he believed that Arillotta was authorised to make transactions on behalf of Recovery Express and this belief was based upon Arillotta’s email address that contained the terms ‘Recovery Express’. While granting judgment filed by recovery Express, the court expressed that CSX allowed itself to be duped by Arillotta. However, CSX argued that by giving Arillotta an email address in the domain recoveryexpress.com, Recovery Express had granted Arillotta apparent authority to enter into business transactions on behalf of ‘Recovery Express’. Further, the court noted that there were flaws in the reasoning of CSX because their argument meant that:177 ‘Every subordinate employee with a company email address – down to the night watchman – could bind a company to the same contracts as the president.’

The court also noted that the problems faced by the parties in this case CSX Transportation, Inc. v Recovery Express, Inc.,178 regarding electronic contracts are similar to the paper-based contracts, in which apparent authority was not necessarily conferred on a purported principal by the purported agent’s use of business cards, company cars and letter heads. The court also noted that a wise business executive always looked behind the claim of authority, but the failure of CSX to do so defeated its own claim of reliance.179 The court also stressed that CSX could have protected itself by taking precautionary measures. Since there is anonymity in the internet transactions, the company making a significant transaction must not rely solely on an email address as the signature of a contracting party but it should request a more

178 Ibid.
179 Moringiello and Reynolds, above n 176, 196–9.
reliable form of authentication. *CSX Transportation, Inc. v Recovery Express, Inc.*, *CSX Transportation*. The internet is an anonymous medium and parties making significant transactions must take precautions as seen in *CSX Transportation, Inc. v Recovery Express*. The electronic transaction legislation only provides general validity to electronic signatures and leaves scope for issues what level of care is required when electronic signatures are used as seen in *CSX Transportation, Inc. v Recovery Express*.

*Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson*, came up for hearing before Justice P. Kevin Castel in New York. In this case, *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson*, Macquarie Group sued a former executive alleging that he impersonated the senior managers of a rival private equity firm. Documents were filed in the Southern District Court of New York. Accordingly, Macquarie alleged that Peter Martenson, a former division director in its US business caused Macquarie irreparable harm by providing confidential information to a competitor called Pacific Corporate Group (PCG) for the personal gain of Mr. Peter Martenson. Macquarie prayed for injunction to stop Mr. Martenson from continuing to disclose confidential information and also to award damages for deceitful and dishonest acts that continued to expose the bank to a great reputational harm.

Macquarie Bank is a Sydney-based bank that is also involved in two separate law suits against the Pacific Corporate Group (PCG) regarding Mr. Martenson’s conduct. Mr. Martenson was hired by Macquarie Bank in 2005 and he was paid US$205,000, which is equivalent to AUS$250,000, per annum plus options and bonuses as a division director. However, he left the bank in February 2008. As per the court documents, Mr. Martenson sent emails to the employees of PCG by falsely

181 Ibid; Moringiello and Reynolds, above n 176.
184 Ibid.
identifying himself as PCG’s Chairman, Christopher Bower. As Mr. Bower, Mr. Martenson insisted that the employees were under non-compete agreements and he also wrote in the same capacity that ‘I need loyal employees’. On another occasion, he adopted the identity of PCG’s former President Monte Brem and sent an email to a Reporter from Dow Jones stating as follows: 186

The entire senior management group is gone [sic].

According to Macquarie, Mr. Mortenson has breached the duty of confidentiality outlined in the employment agreement and he never requested or received permission from Macquarie to impersonate any PCG employee. Eventually, it was Mr. Bower, who informed Macquarie of the alleged illegal behaviour of Mr. Martenson that involved the theft of identity and fraud, which cost PCG a sum of US$30 million. Macquarie has made allegations that Mr. Martenson did not provide full disclosure and Macquarie is seeking indemnification from any liability caused by Mr. Martenson’s actions. 187

However, Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson 188, has raised federal questions regarding contract and on 15 January 2009, has been filed in the Southern District Court of California before Dana M. Sabraw and Louisa S. Porter JJ. 189 Email addresses can be easily impersonated as seen in Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson 190 The electronic transaction legislation only provides general validity to electronic signatures and leaves scope uncertainties regarding impersonation of electronic signatures and identity theft from the perspective of electronic signatures as seen in Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson. 191

186 Ibid.
187 Ibid.
188 Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Martenson, Case No 3: 2009cv00093.
189 Moringiello and Reynolds, above n 176.
190 Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Martenson, Case No 3: 2009cv00093.
191 Ibid.
The requirement focuses on the basic function of a signature such as to identify the person and to indicate the person’s intention. 192 According to the explanatory memorandum to the Victoria bill, the signature method is not required to uniquely identify the persons, instead it must sufficiently identify the person for the electronic communication or the contract. 193 Based on functional equivalence principle signatures are considered same as traditional paper based signature without transposing all their functions in an electronic media. Based on technology neutral principle all the signatures are provided equal validity although different signatures require different legal analysis. Paper based signatures are stable and inscribed on a static and stable medium. Electronic signatures are transient.194

Moreover, transactions carried out through cloud technology is highly insecure therefore it is necessary to re-evaluate the effect of electronic signatures. In an online environment identities take the form of numbers and digits and lack physical identification. In an electronic medium means of verifying and ascertaining the identity of a person are limited and unreliable. In an offline environment a person is recognised by his name and physical appearance but in the online world the correlation between, name and physical appearance of a person is lost. Different electronic signatures provide varying degree of identification. In an online environment a person can have multiple identities. In an online environment a person can impersonate someone else or can cheat by claiming to be a person who is non-existent.195 Means available in an electronic environment are email address, clicks, Internet Protocol (IP) addresses which can be easily manipulated. The issue is enhanced due to the fact that cloud computing enables remote identification and false identity can easily be obtained. It therefore makes identification and verification of signatures more difficult unlike signatures which are stored on the desktop. If a signatory denies a signature he cannot be easily made accountable. Signature cannot be uniquely associated with a person under the cloud computing infrastructure and provide significant scope for identity theft. Anyone who has access to the document...
can adopt the identity of another person. In addition cloud infrastructure also lack interoperable standards. As a result a signature may also loose its effect due to lack of inter operable standards.

Electronic signature criteria provides legal validity to electronic signatures without providing means for linking the signature to a specific person. Providing validity in this manner will be of little help if it cannot be enforced against the person who created it. Unlike traditional transactions ‘identity’ cannot be used effectively to distinguish between people and therefore does not have same value as in the case of offline transactions. Justifications made in relation to online identity loose their importance further in relation to cloud computing. Reliable means of determining the identity of a person are further reduced in a cloud infrastructure. Further, indication of personas intention with respect to a particular transaction cannot be determined. Cloud infrastructures are difficult to investigate. Investigation of unauthorised activity may be almost impossible in cloud computing as it consists of co located data of several customers and spread across an every changing set of host and data centers. Long term viability of data can also be an issue availability of data in a replacement application can be difficult to ascertain. In addition an user of a computing infrastructure cannot precisely determine where the data is located and how it is protected. It may be located at various servers involving geographically dispersed data centers.

7.4 Position in the US

Like the model law, UETA focuses primarily on removing traditional barriers to enable formation of electronic contracts. Section 3 of UETA states that the Act applies to electronic records as well as electronic signatures in their relation to a

---

197 Gartner, above n 9.
198 Ibid.
transaction. The term ‘transaction’ is defined as action which occur between two or more people relating to commercial matters or governmental affairs. Section 7(b) of the Act deals with formation of contracts. Under Section 7 (b) a contract formed electronically must not be denied legal effect for being in an electronic form. In *Campbell v General Dynamics Government Systems Corp*, web based content was liberally interpreted as writing. The legislation not only recognises contracts formed through electronic means but also acknowledges the differences between electronic and paper-based media by specifically referring to electronic records. The term ‘electronic record’ is defined as ‘record created, generated, sent, communicated, received, or stored by electronic means’. The definition of the term ‘record’ requires information stored on an electronic medium to be ‘retrievable in a perceivable form’. Although the Act acknowledges the technical difference between a paper based medium and electronic media it is not technology sensitive to an adequate extent. In contrast, the Australian electronic transaction legislation only requires the electronic document to be accessible and usable and therefore appears to be more liberal.

Electronic record and writing are interrelated concepts. Writing is inscribed on an electronic record. In relation to cloud computing what should be regarded as the electronic record is it the Iaas, Paas, Daas or the entire hard ware of cloud infrastructure. Electronic records stored in a cloud may be out sourced and scattered over various servers. Hence cloud computing technology makes it difficult to confine the scope of the electronic record. Can the web browser be regarded as the electronic record. However, the stored version or printable version of a web document may appear different from the document accessed online. Cloud infrastructure also allows establishment of mash up web application. It combines

---

201 *Uniform Electronic Transactions Act 1999*, § 3.
202 Ibid § 2(16).
203 Ibid § 7.
204 *Campbell v General Dynamics Government Systems Corp* 407 F. 3 d 546, 556 (1st Cir. 2005).
206 Ibid.
data from more than one source into a single integrated document. Therefore unlike traditional paper based documents scope of a web based document cannot be determined. 209

Furthermore, cloud computing facilitates establishment of virtualization software. Analysis of electronic records from the perspective of virtualisation software provide additional insights regarding the issue. By means of virtualization software multiple software applications can be run on a single computer simultaneously. In virtualization infrastructure the main operating system is called the host and the secondary systems are called guest. When virtualization software is running each subsequent system installed on the computer will act like a new computer. Different applications such as windows, linux can be run simultaneously. Traditional paper based documents maintain the contents of a document in a stable manner. When a single document is viewed by means of different software it may appear differently and may not incorporate all the features of a particular website. As a result electronic records cannot be regarded as stable like traditional paper based documents. 210

UETA broadly defines ‘electronic signature’ as a symbol with intent to sign the record. s 2(8) of UETA defines an ‘electronic signature’ as electronic sound, symbol or process associated with a record. It also requires the signature to be adopted by a person with the intent to sign the record. 211 A critical element in UETA is the presence of intention to execute or adopt the sound or symbol or process for the purpose of signing the related record. Hence, under UETA, any form of electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with an intention to sign the record will constitute and ‘electronic signature’ as long as some affirmative step is taken by the signer with an intent to sign the record and the electronic signature is linked or logically associated with a record. However, the UETA does not specify as to how this intention can be exhibited. The commentary on UETA only states that the critical element is the intent to sign. However, from the prospective of vertulization

211 Uniform Electronic Transactions Act 1999, § 2(8).
software discussed above, the criteria appears to be too simple.\textsuperscript{212} In comparison, the Australian electronic transaction legislation merely requires the signature method to be reliable and appropriate for the purpose used. When accessed in the light of virtualization software the term reliable and appropriate appears to be significantly uncertain.\textsuperscript{213}

Most cloud computing infrastructure make use of HTML (Hyper Text Mark Up Language). By means of HTML various pages can be linked together. Therefore, contents of electronic contracts cannot be confined and restricted unlike traditional contracts. In addition websites can also be linked to other websites which makes it difficult to determine the scope of the document. Hyperlinks also create ambiguity reading the source of the documents. Contents from different sites may appear as if they belong to a single web site.\textsuperscript{214} Therefore, intent to sign the record can be easily denied. In addition, webpages can be easily updated and the contents of a web site can be easily changed. Due to this inherent quality of websites logical association of intention with the electronic record as required by the Act cannot be determined easily. In comparison, the Australian electronic transaction legislation requires the signature method to be reliable and appropriate. The reliability and appropriateness of the signature method can be easily questioned in relation to HTML.\textsuperscript{215}

Electronic signatures were liberally interpreted and were provided validity in \textit{Shattuck v Klotzbach}\textsuperscript{216} Discussion on validity of electronic signature was also made in \textit{Richard S Berger v Robert Newhouse}\textsuperscript{217} it was held that the form consisting of electronic signature was filed in error because the board member had not adopted, executed or authorized the electronic signature. Court noted that the Delaware’s \textit{Uniform Electronic Transactions Act} enables a board member to challenge the form on those grounds. Similar view was expressed in \textit{Hepfinger v White}.\textsuperscript{218} Overall,

\begin{itemize}
\item \textsuperscript{212}Ibid § 9(a); Ibid § 2 Comment 7; M R Hariss and N Singhvi, ‘Electronic Contracts More Than A “Virtual” Reality’ (2000) 19(13) Banking and Financial Services Policy Report 7, 7–8.
\item \textsuperscript{213} \textit{Electronic Transactions Act} 2000, \textit{Electronic Transactions (Victoria) Amendment Act 2011}.
\item \textsuperscript{214} Mik, above n 196.
\item \textsuperscript{215} \textit{Electronic Transactions Act} 2000, \textit{Electronic Transactions (Victoria) Amendment Act 2011}.
\item \textsuperscript{216} \textit{Shattuck v Klotzbach}, 14 Mass L Rptr 360 (Massachusetts Superior Court, 2001).
\item \textsuperscript{218} \textit{Hepfinger v White} 2005 Mich App. LEXIS 2192.
\end{itemize}
electronic signatures are being provided validity liberally. They are not being enforced only if the signatory fails to authorise the use of electronic documents.

7.5 Position in the UK

The EU Directive on Electronic Commerce 2000\(^{219}\) was implemented by the Electronic Commerce (EC Directive) Regulations 2002.\(^{220}\) Regulation 9 states that information that a service provides must be provided to the recipient of the service when electronic contracts are formed.\(^{221}\) It requires service providers to provide information such as technical steps that must be followed for the formation of contracts, technical means for correcting input errors, availability of terms and conditions of the contract.\(^{222}\)

Section 8 of the UK Electronic Communications Act 2000 grants authority to appropriate ministers to modify the provisions of any legislation to remove the barriers related with traditional writing requirements for facilitating electronic commerce. It states:\(^{223}\)

1) Subject to subsection (3), the appropriate Minister may by order made by statutory instrument modify the provisions of—
   (a) any enactment or subordinate legislation, or
   (b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation,
   in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).

2) Those purposes are—
   (a) the doing of anything which under any such provisions is required to be or may be done or evidenced in writing or otherwise using a document, notice or instrument;

\(^{222}\) Ibid.
\(^{223}\) Electronic Communications Act 2000 (UK) c 8.
(b) the doing of anything which under any such provisions is required to be or may be done by post or other specified means of delivery;

(c) the doing of anything which under any such provisions is required to be or may be authorised by a person’s signature or seal, or is required to be delivered as a deed or witnessed;

(d) the making of any statement or declaration which under any such provisions is required to be made under oath or to be contained in a statutory declaration;

Although this section facilitates fulfilment of writing requirement, it does not provide any information about accessibility and storage of electronic documents, as the Model Law on Electronic Commerce does.\(^\text{224}\) Further, unlike Australian legislation, this requirement neither provides specific guidance nor specifies accessibility and usability requirement.\(^\text{225}\) Hence, it suffers from limitations.

However, like the European Directive, Regulation 9 (3) Talks about storage of terms and conditions as follows:\(^\text{226}\)

> Where the service provider provides terms and conditions applicable to the contract to the recipient, the service provider shall make them available to him in a way that allows him to store and reproduce them.

This provision does not specifically deal with click wrap agreements but vaguely talks about storage of terms like the European directive. The electronic transaction legislation of Australia does not have an equivalent provision.\(^\text{227}\)

*\(R \text{ (on the application of Software Solutions Partners Ltd) v Revenue and Customs Commissioners}\)\(^\text{228}\) highlights the importance of Electronic Commerce (EC Directive) Regulations 2002. In this case Kenneth Parker QC explained the contract formation process under reg 11 of the *Electronic Commerce (EC Directive) Regulations 2002* as follows:\(^\text{229}\)

\(^\text{224}\) Ibid.

\(^\text{225}\) *Electronic Transactions Act 2000* (Vic) s 8.


\(^\text{227}\) *Electronic Transactions Act 2000* (Vic).

\(^\text{228}\) *R (on the application of Software Solutions Partners Ltd) v Revenue and Customs Commissioners* [2007] EWHC 971.

\(^\text{229}\) Ibid para19.
I do not believe that anything in this application turns upon a precise analysis of the electronic contact formation as such, although it would appear from Mr Bate’s description that in legal terms it is insurer which makes the binding offer of insurance (rather than a mere invitation to treat) and that it is the broker, on behalf of his principal, which gives acceptance, such acceptance being presumably effective when received on SSP’s information system, or on the information system of such other party as might be stipulated in any operating protocol to which SSP, broker and insurer may be party. I mention this simply because, by contrast to the position here under consideration, in most business to consumer transactions by email or over the internet it is the customer that makes the offer and the business supplier that reserves the right to accept or reject (see Chissick and Kelman, Electronic Commerce, Law and Practice, 3rd edition, Paras 3.29.3.33; and art 11 (1) of EC Council Directive 2000/31/EC on Electronic Commerce, as implemented by reg 11 of the Electronic Commerce (EC Directive) regulations 2002, which seem predicated on this sequence of offer and acceptance).

7.5.1 Electronic Signatures: UK

The *Electronic Communications Act 2000* deals with the legal status of electronic signatures and empowers the government to modernise outdated legislation in such a way that an option to use electronic communication and to provide storage is offered as an alternative to paper-based transactions. The *Electronic Communications Act 2000* also recognises self-regulatory schemes that ensure the quality of electronic signatures and cryptography support services. The *Electronic Signatures Regulations 2002* were introduced to implement the European Directive on electronic signatures that was enforced on 8 March 2002. The EU Electronic Signatures Directive facilitates the use of electronic signatures and contributes towards the legal recognition of electronic signatures.

---


The *Electronic Signatures Regulations 2002* incorporates the EU Directive provisions related to the supervision of certification and data protection requirements, whereas the provisions on the admissibility of electronic signatures under legal proceedings are implemented in the *Electronic Communications Act 2000*.\(^2\) Under s 7(2) of the *Electronic Communications Act 2000* and s 2 of the *Electronic Signatures Regulations 2002*, electronic signature can be represented in multiple forms and serves as a method of authentication. However, the *Electronic Communications Act 2000* does not describe the legal effects of electronic signatures. The Act only states that electronic signatures, the certification and the process under which such signatures and certificates are created, issued and used shall be admissible in evidence in terms of the authenticity of the communication or data or the integrity of the communication or data.\(^3\) However, the evidential value of an electronic signature is decided by the court based upon the facts of a particular case and the Act does not define any requirements for acceptance of electronic signature.\(^4\) Hence, the legislation in UK in this respect is different from the European Directive on electronic signatures, because the EU Directive gives qualified electronic signatures the same legal effect as that of a handwritten signature. The UK does not implement this Directive because it holds that handwritten signatures have no special evidential status under the UK legislation.\(^5\) However, under s 7 of the *Electronic Communications Act 2000*, the parties may decide about the legal status of electronic signatures between them.\(^6\)

Under s 7(2) of the *Electronic Communications Act 2000* and s 2 of the *Electronic Signatures Regulations 2002*, electronic signature can be represented in multiple forms and serves as a method of authentication.\(^7\) However, the *Electronic Communications Act 2000* does not describe the legal effects of electronic signatures. The Act only states that electronic signatures, the certification and the process under

\[^2\] Wang, above n 230.
\[^3\] Electronic Communications Act 2000 (UK) c 7.
\[^7\] Electronic Communications Act 2000 (UK) c 2; Electronic Signatures Regulations 2002, s 7(2).
which such signatures and certificates are created, issued and used shall be admissible in evidence in terms of the authenticity of the communication or data or the integrity of the communication or data.\textsuperscript{238} Section 7(1) of the Act deals with admissibility of electronic signatures as follows:\textsuperscript{239}

(1) In any legal proceedings—
(a) an electronic signature incorporated into or logically associated with a particular electronic communication or particular electronic data, and
(b) the certification by any person of such a signature, shall each be admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.

However, the evidential value of an electronic signature is decided by the court based upon the facts of a particular case and the Act does not define any requirements for acceptance of electronic signature.\textsuperscript{240} Hence, the legislation in the UK in this respect is different from the European Directive on electronic signatures, because the EU Directive gives qualified electronic signatures the same legal effect as that of a handwritten signature. The UK does not implement this Directive because it holds that had written signatures have no special evidential status under UK legislation.\textsuperscript{241} the parties may decide about the legal status of electronic signatures between them.\textsuperscript{242} It is important to note that if the law requires signature in paper form, under the UK legislation, electronic signatures will not be permitted legally. It is questionable whether the electronic signatures created by cloud computing will be provided validity under the legislation of UK.\textsuperscript{243} In contrast, it is likely that the broad provisions of the electronic transaction legislation of Australia will readily provide validity to even the most insecure electronic signatures such as the signatures created by cloud computing.\textsuperscript{244}

\begin{thebibliography}{99}

\bibitem{238} \textit{Electronic Communications Act 2000 (UK) c 7}.
\bibitem{239} \textit{Electronic Communications Act 2000 (UK) c 7(1)}.
\bibitem{240} DTI, above n 236.
\bibitem{241} Reed, above n 235.
\bibitem{242} DTI, above n 236.
\bibitem{244} \textit{Electronic Transactions Act 2000, Electronic Transactions (Victoria) Amendment Act 2011}.
\end{thebibliography}
The *Electronic Signatures Regulations 2002* does not regulate the conduct of either
the signatory or the other party to an electronic contract, but it prescribes the
liabilities of Certification Authority, which issues qualified certificates to the public.
Under s 4 of the *Electronic Signatures Regulations 2002*, the Certification
Authorities will be liable for any loss suffered by a person who reasonably relied on
such a certificate, unless the Certification Authority proves that it was not
negligent. These provisions are not flexible enough to accommodate modern
technologies such as virtualization softwares and HTML technology discussed
above in terms of allocation of liabilities. The Australian electronic transaction
legislation does not have an equivalent provision. However, neither the *Electronic
Communications Act 2000* nor the *Electronic Signatures Regulations 2002* address
the issue of cross-border recognition of certificates and electronic signatures.
According to Article 3 and 4 of the EU Directive on Electronic Signatures, the UK
will implement the legal framework for the use of electronic signatures across the
EU. Under Article 4 of the EU Directive on electronic signatures, the Member
States shall not restrict circulation of electronic signature products that comply with
the Directive and they must give same treatment to a certification service issued by a
provider established in another Member State. Further, under Article 3(7) of the EU
Directive, Member States shall not impose additional requirements on the use of
electronic signatures in public sector that may constitute an obstacle in the cross-
border services for citizens.

In England, where an agreement requires that variations made must be in writing and
signed by the parties, it has been held that typewritten names at the foot of an email
amounted to a sufficient signature as seen in *Hall v Cognos Ltd*. However, email
address was not considered a signature in *J Periera Fernandes S.A. v Nilesh Mehta*.
In *J Periera Fernandes S.A. v Nilesh Mehta*, it was held that an automatic insertion
of a party’s email address at the beginning of an email did not constitute a signature

---

248 Ibid art 3(7); Wang, above n 230.
249 *Hall v Cognos Ltd* (Industrial Tribunal Case No 1803325/97).
251 Ibid.
for the purpose of the Statute of Frauds.\textsuperscript{252} In \textit{J Periera Fernandes S.A. v Nilesh Mehta}\textsuperscript{253} the issue was whether the name forming part of an email address could be considered a signature. In this case, In \textit{J Periera Fernandes S.A. v Nilesh Mehta}\textsuperscript{254} In July 2002, J Pereira Fernandes SA was a Portuguese company that supplied bedding products to Bedcare (UK) Limited, a company in which Mr. Nilesh Mehta was a director. However, Bedcare (UK) Limited failed to pay for the products it received and it was wound up on a petition made by J Periera Fernandes SA by an Order dated 7 March 2005. The cause of the Appeal that came before the judge Pelling QC related to the winding up petition made by J Periera Fernandes SA on 12 January 2005. On 20 February 2005, an email was sent from the email address Nelmehta@aol.com to Ian Simpson & Co, solicitors acting for J Periera Fernandes SA, but Mr. Mehta’s name was not typed at the end of the email. District Judge Harrison gave summary judgment on 9 November 2005 to J Periera Fernandes SA for a sum of £24,985.53 and ordered Mr. Nilesh Mehta to pay the costs of the claim, summarily assessed for £1,080.00. On 20 February 2006, Holman J subsequently permitted Mr. Nilesh Mehta to appeal. Contents of the email text identified above were as follows:\textsuperscript{255}

I would be grateful if you could kindly consider the following:

If the hearing of the Petition can be adjourned for a period of 7 days subject to the following:

a. A Personal Guarantee to be given in the amount of £25,000 in favour of your client – together with a list of my personal assets provided to you by my solicitor

b. A repayment schedule to be redrawn over a period of six months with a payment of £5000.00 drawn from my personal funds to be made before the adjourned hearing.

I am also prepared to give a company undertaking not to sell market or dispose of any company assets without prior consent from your client pending the signing of the Personal Guarantee.’

\textsuperscript{252} Christensen et al, above n 118, 28–9.
\textsuperscript{253} Fernandes SA v Mehta (2006) 1 WLR 1543.
\textsuperscript{254} Ibid.
\textsuperscript{255} Ibid.
The relevance of this email is important in *J Periera Fernandes S.A. v Nilesh Mehta* and it must be noted that the email address that appeared on this email also appeared on other emails sent to Ian Simpson & Co by Mr. Nilesh Mehta that did not include his name typed at the end of the email. The two important issues of relevance to be considered here were as follows:

1. Whether the email could be considered a sufficient note or memorandum under section 4 and if so,
2. Whether it was signed by the party charged, that is on behalf of Mr. Nilesh Mehta.

Judge Pelling QC summarised the effect of the emails as follows:

28. … Here the issue is whether the automatic insertion of a person’s email address after the document has been transmitted by either the sending and/or receiving ISP constitutes a signature for the purpose of Section 4.

29. In my judgment the inclusion of an email address in such circumstances is a clear example of the inclusion of a name which is incidental in the sense identified by Lord Westbury in the absence of evidence of a contrary intention. Its appearance divorced from the main body of the text of the message emphasises this to be so. Absent evidence to the contrary, in my view it is not possible to hold that the automatic insertion of an email address is, to use Cave J’s language, ‘…intended for a signature…’. To conclude that the automatic insertion of an email address in the circumstances I have described constituted a signature for the purposes of Section 4 would I think undermine or potentially undermine what I understand to be the Act’s purpose, would be contrary to the underlying principle to be derived from the cases to which I have referred and would have widespread and wholly unintended legal and commercial effects. In those circumstances, I conclude that the email referred to in Paragraph 3 above did not bear a signature sufficient to satisfy the requirement of Section 4.

The email in this case is a relatively rare example of a document brought into the purview of s 4 of the Statute of Frauds, 1677, that is because s 4 applies to contracts of guarantee and the content of this email offered a guarantee in which Mr. Nilesh

---

Mehta offered to personally cover debts owed by the company. Section 4 of the Statutes of Fraud reads as follows:\textsuperscript{258}

\begin{quote}
No action shall be brought…whereby to charge the defendants upon any special promise to answer for the debt default or miscarriages of another person…unless the agreement upon which such action shall be brought or some memorandum or note thereof shall be in writing and signed by the party to be charged therewith or some other person thereunto by him lawfully authorised.
\end{quote}

While giving summary judgment, District Judge Harrison stated that the email did amount to a note or a memorandum of guarantee, although he did not comment on whether the names in the email address amounted to a signature. Judge Pelling QC agreed with District Judge Harrison and held the email to be a note or memorandum that brought it within s 4 of the Statute of Frauds. Regarding the purpose of the Statute of Frauds, he commented as follows:\textsuperscript{259}

\begin{quote}
The purpose of the statute of frauds is to protect people from being held liable on informal communications because they may be made without sufficient consideration or expressed ambiguously or because such a communication might be fraudulently alleged against the party to be charged. That being so, the logic underlying the authorities I have referred to would appear to be that where (as in this case) there is an offer in writing made by the party to be bound which contains the essential terms of what is offered and the party to be bound accepts that his offer has been accepted unconditionally, albeit orally, there is a sufficient note or memorandum to satisfy section 4.
\end{quote}

The second issue that arose in this case was whether the email had been signed. The solicitors of the company J Periera Fernandes SA received a number of emails from Mr. Nilesh Mehta in which he included his name, which was typed at the bottom of the text of the email. Thus, the evidence of a number of email communications from the same address demonstrated that these emails were authentic. Further, Mr. Nilesh Mehta did not dispute that the emails were sent. Thus, the evidence upon which a decision could be made was greater than the evidence that Prakash J dealt with in Singapore in relation to \textit{SM Integrated Transware Ltd v Schenker Singapore (Pte)}

\textsuperscript{258} Statute of Frauds 1677 s 4.
\textsuperscript{259} Mehta v Fernandes SA (2006) 2 All ER 891, 16.
However, the learned judge took the view that the email address was similar to an automatically generated name and facsimile number of the sender of a facsimile transmission. In *J Periera Fernandes S.A. v Nilesh Mehta*, the Counsel for J Periera Fernandes S.A. submitted that the intent to sign was not relevant and mentioned *Elpis Maritime Co. Ltd v Marti Chartering Co. Inc* that had different facts and also emphasised the decision in *Evans v Hoare*, where the name and address were relied upon to serve as a signature. However, the judge Pelling QC stated that Cave J clarified in *Evans v Hoare* that the place of the signature was not relevant as seen below:

> Whether the name occurs in the body of the memorandum, or at the beginning, or at the end, if it is intended for a signature there is a memorandum of the agreement within the meaning of the statute.

The learned judge then went on to indicate that the name of the party to be bound must be intended for a signature, but it is important to note further comments made by Cave J after the text quoted by Pelling QC, which is as follows:

> In the present case it is true that the name of the defendants occurs in the agreement; but it is suggested on behalf of the defendants that it was only put in to show who the persons were to whom the letter was addressed. The answer is that there is the name, and it was inserted by the defendants’ agent in a contract which was undoubtedly intended by the defendants to be binding on the plaintiff; and, therefore, the fact that it is only in the form of an address is immaterial.

Cave J then referred to the decision in *Schneider v Norris*. While refusing to accept that emails constituted signature of Mr. Mehta in *Nilesh Mehta v J Periera*...
Fernandes S.A, Pelling QC in the High Court of Justice Chancery Division in Manchester stated as follows:

30. Before leaving this issue I ought to mention the Electronic Communications Act 2000. This Act empowers the appropriate Minister to issue statutory instruments in order to modify any other statute or statutory instrument in order to facilitate electronic communications. My understanding is that this Act was enacted in order to give effect to the EU Directive on E Commerce (2000/31/EC). No relevant statutory instrument made under this Act has been drawn to my attention. It is noteworthy that the Law Commission’s view in relation to this Directive is that no significant changes are necessary in relation to statutes that require signatures because whether those requirements have been satisfied can be tested in a functional way by asking whether the conduct of the would be signatory indicates an authenticating intention to a reasonable person. This approach is consistent with what I have said so far in this Judgment. Thus, as I have already said, if a party or a party’s agent sending an email types his or her or his or her principal’s name to the extent required or permitted by existing case law in the body of an email, then in my view that would be a sufficient signature for the purposes of Section 4. However, that is not this case.

31. In those circumstances, whilst I conclude that the email referred to in Paragraph 3 above is in principle capable of being a Section 4 note or memorandum notwithstanding that it contains an offer and thus came into existence before not after the contract which it is said to memorialise, it does not bear the signature within the meaning of Section 4 of the Statute of Frauds of either Mr Mehta or his duly authorized agent.

Based on the above conclusion, Pelling QC allowed the appeal of Mr. Nilesh Mehta and dismissed the application for summary judgment on the guarantee point. Thus, Judge Pelling QC evidently used his own knowledge as a user of email to confirm that Mr. Mehta’s email address had been inserted automatically without a deliberate act on the part of the person, who prepared and sent the email. Finally, based upon

---

269 Ibid para 30–1.
Evans v Hoare\textsuperscript{270} and Canton v Canton\textsuperscript{271}. Pelling QC decided that the email had not been signed by or on behalf of Mr. Mehta.

However, in Hall v Cognos Limited,\textsuperscript{272} an email was accepted as an evidence of writing and signature. In this case, Hall v Cognos Limited,\textsuperscript{273} Cognos employed Mr. Hall as a Sales Executive under the terms of the Standard Employment Agreement of Cognos and he was provided with a car for business and personal use. Further, Mr. Hall was reimbursed for all reasonable expenses of travel, accommodation and related costs that were incorporated into a contract, but under the policy expenses over six months old would not be paid. Mr. Hall failed to submit travel expenses between 1 December 1995 and 3 June 1996 and by January 1997 wanted his expenses to be paid. As a result, on 15 January, a series of emails were exchanged between Mr. Hall, Sarah McGoun and Keith Schroeder, who was Mr. Hall’s Line Manager. Due to the delay, Mr. Hall asked if he could submit a late expense claim to Ms. McGoun and Ms. McGoun in turn referred Mr. Hall to Keith Schroeder and Mr. Schroeder replied that being late was okay and stated, ‘Yes, it is OK’. Mr. Hall submitted his expenses thereafter but he did not provide all forms immediately and he even inflated his claims. The employers refused to make any payment and even dismissed him. Cognos argued that an email was not in writing and signed, hence the exchange of emails did not have any effect on the terms of the employment agreement.\textsuperscript{274}

Mr. C.T.Grazin, the Chairman, did not agree with Cognos and held that the emails were in writing and signed once they were printed out and despite there being no statutory definition of writing and document, the Chairman concluded as follows:\textsuperscript{275}

I am satisfied that an email is ‘in writing and signed by the parties’ once it is printed out. The position might (it is not necessary to make any finding on this point) be different if the email was only retained temporarily on the computer’s hard disk storage system. The documents that were, however, produced from

\textsuperscript{270} Evans v Hoare (1892) 1 QB 593, 597–8.
\textsuperscript{271} Canton v Canton (1867) LR 2 HL, 127.
\textsuperscript{272} Hall v Cognos Limited, Industrial Tribunal Case No.1803325/97.
\textsuperscript{273} Ibid.
\textsuperscript{274} Mason, above n 133, 282–3.
\textsuperscript{275} Hall v Cognos Limited, Industrial Tribunal Case No.1803325/97, 5.
the computer are clearly in writing and bear the signatures of both ‘Sarah’ and ‘Keith’. The fact that those signatures are printed, rather than hand written, is not in my view material. For those reasons, I reject Mr. Pym’s submission that the relevant email messages are incapable, as a matter of law, of having any modifying effect on the specific contract between the parties.

Cognos also argued that Mr. Schroeder did not have authority to respond to Mr. Hall’s request, nor was he authorised to agree to it. This argument was rejected because Mr. Schroeder was Mr. Hall’s Line Manager and in this capacity he was vested with the appropriate authority to deal with such a request and hence Mr. Hall could rely on Mr. Schroeder’s response. Thus, Mr. Schroeder’s response would bind Cognos. Therefore, the exchange of emails between Mr. Hall and Mr. Schroeder acted to vary the policy and Cognos was obliged to pay reasonable expenses to Mr. Hall. Finally, both parties agreed that the claim related to 9,960 miles at 9 pence per mile and the employer was ordered to pay £896.40 to Mr. Hall.276

_Hall v Congas Limited_,277 has established that an email acts as an evidence of a written document and a signature in writing as long as the email is capable of being printed.

In sum, automatic insertion of an email address was not recognised as a valid signature for the purpose of statute of frauds. The reason for not recognising it as a valid signature was lack of intention of the signatory to adapt it as a signature. It appears therefore that automatic insertion of name in an email address will be recognised as a valid signature only if a person’s intent to sign the electronic document is clearly ascertainable, as seen in _Nilesh Mehta v J Periera Fernandes S.A._278 A more restrictive and stricter approach was adopted in _Hall v Cognos Limited_,279 where it was held that only a printed email can be considered signed writing for the reason that it provides stronger evidence. It appears clear that courts are still reluctant to readily provide validity to electronic signatures. It can be seen that mere use of electronic signatures does not assures validity. Overall, it can be said

276 S Mason, above n 133, 282–3.
277 _Hall v Cognos Limited_, Industrial Tribunal Case No.1803325/97.
279 _Hall v Cognos Limited_, Industrial Tribunal Case No.1803325/97.
that different approaches are being adopted to recognise electronic signatures, which can give rise to disparity. In comparison, it is likely that in Australia the signature requirements will be more liberally interpreted and electronic signatures will be regarded as valid based on the surrounding facts and circumstances of the case.280

Traditional paper based documents or even the documents saved on the desktop are confined to a specific place they are not scattered and stored over various servers as in the case of cloud computing technology. Therefore cloud infrastructure raises security concerns in relation to writing and signature requirement. Further, by means of new technologies such as mash up documents can be linked together raising concerns regarding scope of the document. The laws of the UK, the UETA and electronic transaction legislation of Australia has side stepped these aspects while addressing the criteria dealing with writing and signature. In order to address the issues raised in this chapter the changes brought about by the new technologies must be closely epitomized

7.6 Conclusion

The chapter examined the legal effect of electronic contracts from the prospective of writing and signature requirements. A comparative analysis of the laws of Australia, the US and the UK was carried out to gain additional insights. The overall discussion of the chapter leads to the consideration of deficiencies in relation to writing and signature. Comparative analysis of the laws of USA and Australia indicate that the laws of the US and UK have fallen behind. The electronic transaction legislation of Australia attempts to keep pace with the latest international developments unlike the US and the UK. However, the law of Australia is not completely satisfying. For instance, Traditional paper based documents or even the documents saved on the desktop are confined to a specific place they are not scattered and stored over various servers as in the case of cloud computing technology. Therefore cloud infrastructure raises security concerns in relation to writing and signature requirement. Further, by means of new technologies such as mash up documents can be linked together raising concerns regarding scope of the document. The laws of Australia, the UK

and the US have side stepped these aspects while addressing the criteria dealing with writing and signature. In order to address the issues raised in this chapter the changes brought about by the new technologies must be closely epitomized
CHAPTER 8
ENFORCEABILITY OF ELECTRONIC CONTRACTS: ISSUES ASSOCIATED WITH CLICKWRAP AGREEMENTS

8.1 Introduction
8.2 Online transactions and impact of privacy concerns
8.3 Click Wrap Agreements and Privacy Terms
8.4 Click Wrap Agreements and Privacy Policies
8.5 Position in the US
8.6 Position in the UK
8.7 Conclusion

8.1 Introduction

Previous chapter examined the issues associated with wiring and signature requirement of an electronic contract. This chapter advances the argument by evaluating the issues associated with click wrap agreements. Websites make terms and conditions available to consumers in the form of click wrap agreements. They generally take the form of non-negotiable, standard form agreements. Terms and conditions related to privacy of the users are also incorporated through click wrap agreements. The contract formation process unduly restricts buyer’s freedom and the website owner exploits this contract formation process to impose terms which deprive consumers important privacy rights. Website owners exploit consumers to impose terms which unacceptably compromise website user’s privacy.\(^1\) This chapter will assess the enforceability of click wrap agreements to see whether click wrap agreements will be enforced even if they do not provide opportunity to the customers to bargain the terms and conditions of the website. The chapter will evaluate whether such one sided terms and condition will be enforced even if they include one sided terms related to the privacy of the users.\(^2\) This thesis deals specifically with electronic contracts therefore the effectiveness of the Privacy

\(^1\) J S Livingston, ‘Invasion Contracts: The Privacy Implications of Terms of Use Agreements in the Online Social Media Setting’ (2011) \textit{ALB L J SCI and TEC} 612–617.

Amendment (Enhancing Privacy Protection) Act 2012 will not be evaluated although the Act is inadequate.³

Before making an assessment it is necessary to evaluate the impact of privacy on electronic contract formation. Online activities generate vast amount of data and give rise to privacy concerns. This issue has gained a new momentum in the age of big data where the online activities leave behind expounding trails of personal information. Therefore, an analysis of privacy concerns will be made first. The analytical framework of click wrap agreements will then be used to assess whether one sided terms and condition will be enforced even if they include one sided terms related to the privacy of the users.

8.2 Online Transactions and Impact of Privacy Concerns

In today’s electronic world businesses heavily rely on information technology for carrying out different transactions. Smart phones and tablets provide easy access to information. Everyday vast amount of data is being created which represents a new era in data exploration and utilization. Management of big data created like this is more than a challenge as businesses now have more valuable information within their electronic systems which needs to be protected⁴.

Big Data deals with collating huge amount of information especially about individuals. Data from various sources such as web pages, browsing habits, sensor signals combined with specialised software can be used to extract valuable information. It has immense economic and social value. Vast amount of data when pieced together can easily reveal who the individual is even if the name and specific identity is not disclosed.⁵

3 Privacy Amendment (Enhancing Privacy Protection) Act 2012; Livingston, above n 1.
Advances in data mining have expanded the scope of information available for businesses and researchers. Now data is also available in raw form. It is not limited to structured databases thereby enhancing researchers ability to use the data in various unanticipated ways. 6 Big data can be used for various purposes. Organisations create and store vast amount of transactional data in digital form. The vast amount of information stored over the internet remains their possibly forever. Big data helps organisations in understanding the way in which their products are used in a better manner. Companies can use big data to conduct controlled experiments to make better management decisions. It can help in tailoring products and services precisely. It can also help in the development of new products and services. Manufactures can also use big data to create innovative after sale services. Apart from the retail industry, heath sector and traffic management are the other fields were big data can be used.7 Increasing use of internet is giving rise to more serious privacy issues.8 Moreover, individuals hidden in anonymous data can be reidentified or deanonymize with ease.9

8.3 Click Wrap Agreements and Privacy Terms

Internet web sites generally have privacy policies. Privacy policies notify the users about the information that will be collected, what type of protection will be provided. These policies are made available to the users in the form of click warp agreements. It is therefore necessary to determine the effectiveness of click warp agreements. Analysis of click wrap agreements will be first made. The analytical framework of click wrap agreements will then be used to assess whether they will be enforced even if they contain one sided terms.

Online contracts are also formed by the click wrap method. They are also known as web warp or click through agreements. It enables a buyer to manifest assent to the terms of a contract by clicking on an acceptance button provided by the website. The terms of the agreement are displayed on the computer screen and are available to be read before clicking on the acceptance icon. Hence, if the buyer or the consumer accepts the terms it may indicate explicit manifestation of the terms of the contract. A confirmation of a click wrap agreement indicates that the party in contracts is aware of the terms and conditions of the agreement and the party agrees to the terms unconditionally.

Electronic contracts require that the traditional principles of contract and the contract law are able to be adapted to the electronic transactions and electronic contracts. Most electronic contracts are made on the internet through click wrap contracts, which are also called ‘click and accept’ contracts. Click wrap contracts are usually hypertext order forms containing terms and conditions of sale and purchase and require clicking of the mouse on ‘I accept’ button before the goods can be ordered or services procured or before accessing the electronic transaction. A buyer or a user cannot complete the transaction without clicking on the ‘I accept’ button. It also prevents a user from accessing further web pages provided within the site without accepting the terms. However, the issue in such click wrap contracts is whether these electronic transactions are legally binding. Due to inconsistent decisions of click wrap cases, legal commentaries have noted the need for clarity and certainty.

---

12 Condon, above n 10; Minaham, above n 10.
13 Minaham, above n 10.
17 Pearce, above n 14.
In the ticket cases, a party can incorporate even unsighted standard terms and conditions only by providing a reference to those terms and an offeree may thus contract on that basis as seen in *Thornton v Shoe Lane Parking Ltd*; 19 *Interfoto Picture Library Ltd v Stilletto Visual Programs Ltd*; 20 *MacRobertson Miller Airline Services v Commissioner of State Taxation (WA)* 21 and *Baltic Shipping Co v Dillon (The Michael Lermentov).* 22

The general law principles of contract regarding effective communication of terms and conditions, in an agreement through proper notice to the other party, in order to bind the parties to the terms of an agreement, apply to the electronic contracts also. 23

The use of click wrap agreements is complex as they do not provide scope for user to negotiate the terms of a contract. 24 In click wrap agreements, terms are unilaterally imposed by the vendor and the user cannot proceed with the transaction without accepting the terms so presented to them. Unilateral imposition of terms in this manner provide more scope for an online vendor to include terms which are favourable to them. Click wrap agreements make consumers vulnerable. 25 Clickwrap agreements incorporate terms through hyperlinks. Terms which are incorporated through hyperlinks in turn incorporate documents creating a branching tree of several click wrap agreements. Therefore, use of hyperlinks can make online scenario more complex and complicated. Some online web sites such as the Australian ticket agency, 26 time bound the transaction by allotting specific time for the completion of the transaction. The amount of time allotted to complete the transaction may not permit a consumer to view all the terms of the online transaction.

---

19 *Thornton v Shoe Lane Parking Ltd* (1971) 2 QB 163.
21 *MacRobertson Miller Airline Services v Commissioner of State Taxation (WA)* (1975) 133 CLR 125.
25 Wong and Lawrence, above n 16; Clapperton and Corones, above n 24.
prior to agreeing to the terms. Click wrap agreements also pose some novel problems. For example, if consumer purchases online software, downloads the software and later wishes to return the product there will be no physical product or commodity to obtain refund. In addition, online websites can also be easily upgraded, including new terms which further complicates the online context.27

Although the current laws provide limited protection to the users, the protection available may not be sufficient to facilitate the development of global electronic commerce.

While, in eBay International AG v Creative Festival Entertainment Pty Ltd,28 the scope of s 52 of the Trade Practices Act 1974 (Cth) was discussed. eBay International AG v Creative Festival Entertainment Pty Ltd29 is an important case where, the Federal Court of Australia confirmed the effectiveness of click wraps methods to form online contracts and also dealt with the issue of incorporation of terms by reference. In such a case, the web user signs the contract electronically by clicking ‘I agree’ button or icon. Hence, the issue of enforceability of click wrap agreements poses very few difficulties to the courts. In eBay International AG v Creative Festival Entertainment Pty Ltd30 Rares J considered the conditions that applied to the resale of tickets for the Big Day Out music festival held in different locations in Australia between January and February 2007. The issue was whether Creative Festival had contravened s 52 of the Trade Practices Act 1974 (Cth) by including among the conditions of sale printed on the back of the tickets for the events of 2007, Condition 6. Condition 6 stated that all Big Day Out Tickets that were resold for profit would be cancelled and the holders of such resold tickets would be refused entry. In order to ascertain whether the representations made in Condition 6 printed on the ticket were misleading or deceptive and/or likely to mislead or deceive in trade or commerce, the court was required to determine first of all, the conditions on which the tickets were being sold. The tickets were not only

27 Ibid; Clapperton and Corones, above n 24,156–175.
28 eBay International AG v Creative Festival Entertainment Pty Ltd [2006] FCA 1768 at 28.
29 Ibid.
30 Ibid.
sold over the counter but also sold direct online from the Big Day Out website and the Ticketmaster website.

In eBay International AG v Creative Festival Entertainment Pty Ltd\(^{31}\) Rares J described website user’s experience as follows:\(^{32}\)

A purchaser would enter the Big Day Out website. A webpage appeared which offered the facility of buying tickets online by clicking on a link. The same page of the website also had a link for opening up the terms and conditions of buying tickets online. If one clicked on the button to buy tickets, the purchaser was then redirected seamlessly and unnoticeably to [Creative’s agent] Online Fulfilment’s website. And, it is on the latter website that the transaction which resulted in the dispatch of a ticket was completed...

...The webpage indicated that the order had been confirmed for the relevant ticket(s), the price had been successfully charged to the nominated credit card account and the ticket(s) would be mailed to the address given by the purchaser. An email was sent immediately following this which confirmed that the order had been successfully charged to the credit card and would now be processed and tickets mailed to the purchaser.

Rares J also held that\(^{33}\) a contract for the purchase of Big Day Out tickets was made on the terms displayed on the Big Day Out website. The contract was formed only after the customer clicked on the buttons agreeing to the terms and conditions and provided details of credit card and also other details and clicked on the ‘Send this Order’ button. The ticket was sold on the basis of the terms and conditions that appeared on five successive web pages on the Big Day Out website that had to be accessed by the customer to buy a ticket online. After a detailed review of the steps involved in the process of purchase of ticket on the Ticketmaster website, Rares J held\(^{34}\) that the online transaction was a contract for purchase of the tickets, in writing and signed by the parties. Accordingly, the contract was formed when the purchaser clicked on the ‘Purchase Tickets’ button on the website of Ticketmaster, subject to credit card approval and verification of billing address. During the entire process, the

\(^{32}\) Ibid 11 and 231.
\(^{33}\) Ibid 27.
\(^{34}\) Ibid 44.
purchaser was unable to access any information that set out any of the conditions on the ticket or on the Big Day Out website. An online purchaser of the ticket was unable to see new Condition 6 until the tickets were received and the process took over six weeks after completion of the transaction online.

Finally, Rares J concluded that Condition 6, as it appeared on the tickets that were sent to the purchasers did not apply to any tickets purchased through Ticketmaster website or to purchases made through the Big Day Out website prior to 8 November 2006 (when the website was updated to include the new version of Condition 6). Rares J also held that Condition 6 on the tickets did not have contractual force and it was not relevant to the contracts under which the tickets were purchased. Thus, by sending tickets including Condition 6, Creative had made false representation in trade or commerce, which indicated that it formed a part of the contract under which tickets were purchased and was effective as a condition of sale. Therefore, the representations as to future matters contained in Condition 6 of the Big Day Out tickets contravened s 52 of the Trade Practices Act 1974 (Cth).

Thus, click wrap agreements will be enforced only if a clear notice of the terms is provided to the contracting party at the time when the product is purchased. In addition, as seen in this case, click wrap agreements can turn out to be misleading and deceptive if all the terms and conditions are not brought to the attention of the parties at the time when the transaction is conducted. Online websites can be easily upgraded to include new terms which complicates the online context. Further this novel feature can also more easily mislead consumers. Although s 52 prevents misleading and deceptive conduct, it could go further to protect consumers by specifically addressing complexities involved in an online context. It should be noted that s 52 prevents misleading and deceptive conduct. However, it provides remedy only after a misleading conduct has occurred it does not per se prevents the use of unfair terms.

---

36 Ibid 28.
In *Peter Smythe v Vincent Thomas* 37 a click wrap agreement was merely recognised without evaluating whether the users intended to adopt the underlying terms then presented to them, which were generally presented as part of the registration process. 38 This case 39 can also be cited as an example where the legally binding nature of click wrap contracts was confirmed. 40 This case 41 also confirmed that the click wrap contracts are legally binding and the court has held that agreements entered into by those using the online auction website eBay are legally binding. Rein AJ in the New South Wales Supreme Court held that a binding contract has been formed between the plaintiff Peter Smythe and the defendant, Vincent Thomas and the contract should be specifically enforced. 42

In *Peter Smythe v Vincent Thomas*,  43 on 15 August 2006, the defendant listed a World War II plane, Wirraway Australian Warbird Aircraft, VH-WIR for sale on the website of eBay for 10 days with a minimum bid of $150,000 for 10 days from 15 August 2006 to 25 August 2006. The defendant was a registered user of eBay website. On 25 August 2006, the plaintiff Peter Smythe, who was also a registered eBay user made a bid in accordance with the rules of eBay for $150,000. Both the plaintiff and the defendant received a notification from eBay to the effect that the plaintiff had won the auction of the plane, Wirraway. 44

Plaintiff claimed that a contract for sale of goods was formed between them. The defendant refused to agree that a binding contract was formed. Instead, the defendant argued that the only contract that existed was between eBay and the plaintiff and eBay and the defendant. 45 However, the defendant agreed that both the defendant and the plaintiff had accepted the terms and conditions of the website by clicking on an accept button. The defendant argued that as a consequence of the breach of the terms

---

40 Pearce, above n 14.
44 Ibid, paras 1–2.
45 Ibid.
and conditions of the website, eBay only had a right to terminate his registration as a user of the website.\(^{46}\)

While confirming the binding nature of a click wrap agreement and the validity and enforceability of electronic contract made on the website of eBay, Rein AJ stated as follows:\(^{47}\)

> In circumstances where both the buyer and seller agree to accept the terms and conditions of eBay I see no difficulty in treating the parties as having accepted that the online auction will have features that are both similar and different to auctions conducted in other forums. A live auction may require registration of bidders, and may specify the means by which payment can be made e.g. ‘personal cheques not accepted’, or that bids of a certain type will be accepted e.g. ‘phone bids accepted’. The parties have agreed to allow eBay, or its computer, to automatically close the bidding at a fixed time and have accepted that eBay will have no personal liability to either buyer or seller. The automatic close of bidding at a fixed time and the generation of an eBay advice headed ‘won’ appear to have been accepted by the parties to an eBay auction as the equivalent of the fall of the hammer.

The court recognised the contract formed between the plaintiff and the defendant. Further, the court ordered specific performance of the contract.\(^{48}\) While rejecting the defendant’s contention, Rein AJ stated.\(^{49}\)

> I do not accept the defendant's contention that arising out of the registration and bidding process I have described, there were contracts only between eBay and the buyer and between eBay and the seller. It has been recognised even in relation to traditional auctions that existence of a contract between vendor and auctioneer can sit together with a contract between the vendor and purchaser (and between the auctioneer and purchaser): see Elder Smith Goldsbrough Mort Ltd v McBride & Palmer [1976] 2 NSWLR 631, following Chelmsford Auctions Ltd v Poole [1973] QB 542; [1973] 1 All ER 810. The eBay terms and conditions created a framework for the auction in which the plaintiff and defendant were willing participants.

\(^{46}\) Ibid para 22.  
\(^{47}\) Ibid para 35.  
\(^{48}\) Ibid para 78.  
\(^{49}\) Ibid para 37.
8.4 Click Wrap Agreements and Privacy Policies

Analysis of cases indicate that the click warp agreements which include terms and conditions dealing with users information will be generally enforced. The web sites vaguely address privacy terms. Terms do not specifically warn the uses about the secondary uses of big data. For instance, internet web sites generally have privacy policies. Privacy policies notify the users about the information that will be collected, what type of protection will be provided. These policies usually be presented to users along with other terms and conditions by means of a click wrap agreement.\(^{50}\) Privacy policies provided in this manner may not provide scope for user to negotiate the terms of a contract.\(^{51}\) Contracts are enforced even if they are one sided. Therefore, privacy policies made available through such one sided terms will also be enforce. As a result, electronic contracts cannot stop the sellers from making use of the private information of users.

Privacy terms are unilaterally imposed by the vendor and the user cannot proceed with the transaction without accepting the terms so presented to them. Unilateral imposition of terms in this manner provide more scope for an online vendor to include terms which are favourable to them. Privacy policies provided through click wrap agreements make consumers vulnerable.\(^{52}\) Click wrap agreements may incorporate policies through hyperlinks. Terms which are incorporated through hyperlinks in turn incorporate documents creating a branching tree of several click wrap agreements. Therefore, use of hyperlinks can make online scenario more complex and complicated. Some online web sites such as the Australian ticket agency,\(^{53}\) time bound the transaction by allotting specific time for the completion of the transaction. The amount of time allotted to complete the transaction may not permit a consumer to view all the terms of the online transaction prior to agreeing to the terms. Click wrap agreements also pose some novel problems. For instance,

---

\(^{50}\) Yahoo <www.yahoo.com> 18 June 2013.

\(^{51}\) Clapperton and Corones, above n 24.

\(^{52}\) Wong and Lawrence, above n 16, 65; Clapperton and Corones, above n 24.

online websites can be easily upgraded, including new terms which further complicates the online context.54

Web site vendors usually draft privacy policies to satisfy the requirement of the Privacy legislation.55 For example to use the yahoo mail service the users will be asked to enter personal information such as name, address, email address, telephone number, gender, date of birth. As soon as the sign up bottom is clicked users will be asked to type in some security words. Later the user will be asked to click on the terms and conditions of the web site which also incorporates privacy policy of the website.56

Skype collects vast information such as identification data which includes name, address, telephone number, mobile number, email address, gender, country of residence, electronic IP address, banking and payment information, list of contacts.57 It also collects information such as duration of the call, number of calls made, contact details of people to whom calls were made, contents of instant messages, voice calls and voicemails. The privacy policy of Skype says that the data so collected may be stored and processed in any other country in which Microsoft or its affiliates maintains facilities.58

Generally, web sites only provide general information about the privacy policy which vaguely safeguard the privacy of users. Secondary uses of big data are not generally listed in these terms and conditions. Overall, neither the privacy legislation nor the privacy policies offer appropriate solution. Legislative measures must be taken to address this lacuna. The terms and conditions listed on the web sites may also amount to misleading and deceiving conduct as seen in EBay International AG v Creative Festival Entertainment Pty Ltd59.

The federal government has introduced the new Trade Practices Amendment (Australian Consumer Bill) 2009 (Cth). Now the Competition and Consumer Act

54 Ibid; Clapperton and Corones, above n 24, 156–175.
55 Livingston, above n 1.
57 Skype <skype.com>.
58 Ibid.
2010. The aim of the new law is to harmonise consumer laws of Australia as well as update consumer laws of Australia. It also contains reform to provisions dealing with unfair terms. The Act was passed on 17th March 2010. It focuses more on balance of fairness. In addition, under the proposed reform an action can only be taken only after the consumer suffers loss. The proposed reforms are unsatisfactory as they do not per se prevent the use of unfair terms. One sided imposition of terms and conditions from the prospective of privacy may not amount to unfair practice under the Act.

However, the Competition and Consumer Act 2010 (Cth) has also broadened the scope of misleading and deceptive conduct. A term will be regarded as misleading if it causes significant imbalance to the rights and obligations of the parties, is not reasonably necessary to protect the rights of the sellers and causes detriment financial or non-financial. Secondary uses of big data cannot be adequately protected therefore rigid polices regarding big data can more easily amount to misleading and deceptive conduct under the Competition and Consumer Act 2010 (Cth). Therefore legislative intervention can more clearly guide the website owners. The Electronic Transactions (Victoria) Amendment Act 2011 made amendments to the Electronic Transactions (Victoria) Act 2000 to it into line with the United Nations Convention on the Use of Electronic Communications in International Contracts 2005. Like the United Nations Convention on the Use of Electronic Communications in International Contracts 2005, The Electronic Transaction Legislation of Australia does not deal with clickwap agreements is therefore inadequate.

---

62 Nottage, above n 60; Gray, above n 60, 163–167.
8.5 Position in the US

The courts have ruled in a number of cases such as ProCD, Inc. v Zeidenberg,\(^65\) iLAN Sys., Inc. v Netscout Serv. Level Corp.,\(^66\) Klocek v Gateway, Inc.,\(^67\) M.A. Mortenson Co. v Timberline Software Corp.,\(^68\) that ‘CD click wrap agreements’ binds a consumer only when that consumer is provided with both prior notice that additional terms would be incorporated into the agreement and a right to read and reject terms that are not acceptable to the consumer. Therefore, clicking on an ‘I agree’ icon will be considered ‘explicit assent’ only when the user is given sufficient notice and the user is provided with:\(^69\)

1. an opportunity to inspect the items and also the terms; and
2. an opportunity to reject the terms by returning the product and getting a full refund.

It is clear from the forgoing that only very clear and obvious ways of providing notice is enforced as seen Ticket Master Corp. v Ticket Masters.Com Inc,\(^70\) Pollstar v Gigmania Ltd,\(^71\) Specht v Netscape Communications Corp\(^72\) and Feldman v United Parcel Service, Inc.\(^73\) Courts appear to be reluctant to recognise less obvious ways of including terms through hyperlinks. Such notices have only been enforced if the contracting party is a long time user of the website, as seen in Druyan v Jagger.\(^74\) However, it can be seen that click wrap agreements are being enforced even on the basis of long time use only if a user is provided notice of changed terms beforehand as in Douglas v United States District Court for the Central District of California\(^75\) If

\(^{65}\) ProCD, Inc v Zeidenberg, 86 F 3d 1447, 1451 (7th Cir, 1996).

\(^{66}\) iLAN Sys Inc v Netscout Serv Level Corp, 183 F Supp 2d 328, 336–7 (Mass, 2002).

\(^{67}\) Klocek v Gateway Inc, 104 F Supp 2d 1332, 1341 (Kan, 2000).

\(^{68}\) M A Mortenson Co v Timberline Software Corp, 998 P 2d 305, 312–3 (Wash, 2000).


\(^{71}\) Pollstar v Gigmania 170 F Supp 2d 974 (E D Cal, 2000).


\(^{74}\) Druyan v Jagger, 508 F Supp 2d 228 (SDNY, 2007).

\(^{75}\) Douglas v United States District Court for the Central District of California 495 F 3d 1062 (9th Cir, 2007), cert denied sub nom; Talk Am Inc v Douglas, 128 S Ct 1472 (2008).
this path is followed and if emphasis is placed on obvious or enhanced notices then, in most situations click wrap agreements will be regarded as unenforceable due to lack of obvious notice or enhanced notice. As a result, this approach can have negative implications on online vendors and may not provide enough incentive to conduct online transactions. Hence, this approach must be treated with caution.

Modern technology has redefined the way transactions take place and the manner in which contracts are formed, thereby making it necessary to have legislation such as UETA. Although the legislation has attempted to regulate electronic contracts it is inadequate for the effective formation of electronic contracts as, neither E-SIGN that pre-empts UETA or UETA deals with click wrap agreements. These provisions do not talk about providing specific notice about the terms and conditions of the website and therefore cannot protect the parties from the adverse effects of click warp agreements identified above.

8.6 Position in the UK

The EU Directive on Electronic Commerce 2000 was implemented by the Electronic Commerce (EC Directive) Regulations 2002. Regulation 9 states that information that a service provides must be provided to the recipient of the service when electronic contracts are formed. It requires service providers to provide information such as technical steps that must be followed for the formation of contracts, technical means for correcting input errors, availability of terms and conditions of the contract.

Section 8 of the UK Electronic Communications Act 2000 grants authority to appropriate ministers to modify the provisions of any legislation to remove the

78 Dessent, above n 76, 944–54.
82 Ibid.
barriers related with traditional writing requirements for facilitating electronic commerce. It states:\(^{83}\)

1) Subject to subsection (3), the appropriate Minister may by order made by statutory instrument modify the provisions of—
(a) any enactment or subordinate legislation, or
(b) any scheme, licence, authorisation or approval issued, granted or given by or under any enactment or subordinate legislation,
in such manner as he may think fit for the purpose of authorising or facilitating the use of electronic communications or electronic storage (instead of other forms of communication or storage) for any purpose mentioned in subsection (2).

(2) Those purposes are—
(a) the doing of anything which under any such provisions is required to be or may be done or evidenced in writing or otherwise using a document, notice or instrument;
(b) the doing of anything which under any such provisions is required to be or may be done by post or other specified means of delivery;
(c) the doing of anything which under any such provisions is required to be or may be authorised by a person’s signature or seal, or is required to be delivered as a deed or witnessed;
(d) the making of any statement or declaration which under any such provisions is required to be made under oath or to be contained in a statutory declaration;

Although this section facilitates fulfilment of writing requirement, it does not provide any information about accessibility and storage of electronic documents, as the Model Law on Electronic Commerce does.\(^{84}\) Further, unlike Australian legislation, this requirement neither provides specific guidance nor specifies accessibility and usability requirement.\(^{85}\) Hence, it suffers from limitations.

However, like the European Directive, Regulation 9 (3) Talks about storage of terms and conditions as follows:\(^{86}\)

\(^{83}\) *Electronic Communications Act 2000 (UK)* c 8.
\(^{84}\) Ibid.
\(^{85}\) *Electronic Transactions Act 2000 (Vic)* s 8.
Where the service provider provides terms and conditions applicable to the contract to the recipient, the service provider shall make them available to him in a way that allows him to store and reproduce them.

This provision does not specifically deal with click wrap agreements but vaguely talks about storage of terms like the European directive. However, these provisions do not talk about providing specific notice about the terms and conditions of the website. The electronic transaction legislation of Australia does not have an equivalent provision.  

8.7 Conclusion

Within this analytical framework the interaction of click wrap agreements with the privacy policies of web sites were assessed. Privacy policies are usually presented to users in the form of click warp agreements. Terms are unilaterally imposed upon the users. This approach will make users more vulnerable. Sometimes the users also click the acceptance buttons without being aware about the privacy policies. Web site owners must take measures to more clearly notify the users. Web site users must be given a choice to negotiate the privacy terms. The privacy terms must be provided to users in a more static manner. Users who allow the web site owners to use all their information for commercial purposes must be allowed to use all the services of the websites. Users who only permit to use partial information for commercial purposes must be allowed to use limited services of the websites. In addition web site owners must also protect the private information of users though advanced technical solutions.

Consumer should be given more control over their private data and a better bargaining position. There is also need for more effective legal regulation. Consumers should be given the right to choose what type of information to share with the websites. The information collected about users should be used for the purpose of advertising only after seeking specific permission from the users.

87 Electronic Transactions Act 2000 (Vic).
9.1 Introduction

9.1.1 Primary Question: Has the Electronic Transaction Legislation Resolved Issues that are Left Unresolved under Traditional Law?

9.1.1.1 Invitation to Treat

9.1.1.2 Time of Contract Formation

9.1.1.3 Place of contract formation

9.1.1.4 Signatures

9.1.1.5 Writing Requirements and storage of contractual terms

9.1.1.6 Conclusion of primary research question

9.1.2 Primary Question Two: What issues arise when traditional contract principles are applied to electronic contracts?

9.1.2.1 Click wrap Agreements

9.1.2.2 Mistaken Identity

9.1.2.3 Conclusion of primary research question two

9.1.3 Sub-question One: Have other Jurisdictions Addressed the Issues Differently?

9.1.4 Sub-question Two: What Is the Role of International Developments in Addressing Issues? How Is Australia Responding to the International Developments?

9.2 Concluding Remarks: Summary of Major Findings, Contributions of the Research to the Area of Electronic Contracts and Its Implications

9.3 Recommendations and Suggestions

9.4 Areas for Future Research

9.1 Introduction

This chapter draws together the analysis of the preceding chapters and answers the following research questions identified in Chapter One:

1. Has the Electronic Transaction Legislation of Australia resolved the issues?

2. What issues arise when traditional contract law is applied to electronic contracts?
3. Do other jurisdictions have same issues? Is it an International problem?
4. What is the role of international developments in addressing issues? How is Australia responding to the international developments?

The aim of the thesis was to evaluate the role of electronic transaction legislation of Australia in establishing an appropriate legal framework for electronic contracts. The above research questions were framed to assess this and the objective was achieved by analysing two sets of laws, traditional contract principles and the electronic transaction legislation of Australia. Additional insights on issues related to electronic contracts were obtained by evaluating analogous laws of different countries and international developments on electronic contracts.

9.1.1 Primary Question One: Has the Electronic Transaction Legislation of Australia Resolved the Issues?

The research has found that the electronic transaction legislation of Australia has not resolved all of the issues related to electronic commerce activities in Australia. Gaps found after the analysis of the electronic transaction legislation can be summarised under the following sub-headings.

9.1.1.1 Invitation to Treat

There is body of law regarding invitation to treat yet there is a lack of clarity around invitation to treat in the context of electronic contracts. In brief, neither the traditional contract principles nor the electronic transaction legislation provide specific criteria dealing with invitation to treat with regards to electronic contract. As a result, a lack of clarity around an invitation to treat in the context of electronic contracts still persist.

The interactive and non-interactive nature of a website creates difficulty in differentiating between an offer and an invitation to treat in the online context. This was identified in Chapter Four. Websites cannot be easily classified as an offer or an invitation to treat. They incorporate some of the features of advertisements, vending machines and even display of good in shops. The interactive and non-interactive nature of a website creates difficulty in differentiating between offer and invitation to
treat in the online context.¹ Contract law does not specifically address how to differentiate between offers and invitation to treat in an online context. An online vendor may wish to be certain that the goods offered through online websites are an invitation to treat, because if online websites are regarded as offers, then the online vendor will be exposed to the risk of unanticipated number of acceptances. Internet offers an easy global worldwide platform to businesses hence this risk is exuberated in the online context.

However, in the absence of clear law, the issue of differentiation between offer and invitation to treat in an online context can only be avoided through unambiguous disclaimers and written instructions on the website, which will assure that the advertisements are invitation to treat.² In particular, this approach provides a solution only if the disclaimers are sufficiently clear. Consumers can also get misled if such disclaimers are not sufficiently clear.

The purpose of the electronic transaction legislation, is to clarify the extent to which parties offering goods or services, through accessible communication systems such as websites, are bound by advertisements. Under the legislation a proposal for concluding a contract, other than that addressed to a specific person or persons, must be considered an invitation to make offers, unless the person making the proposal indicates otherwise. Under the electronic transaction legislation the distinction between an offer and an invitation to treat depends on the vendor’s intention, in the absence of a clear indication by the vendor to be bound by an offer. It is to be evaluated based on the circumstances such as automatic systems used for placing order and click wrap icons provided for the formation of contract.³ This criteria is not completely convincing by itself as different technologies used for expressing intent will represent different degrees of intent. This criteria can also confuse and mislead

² Christoph, above n 1; S Graw, above n 1.
consumers regarding vendors’ actual intentions. Intention is very important for the
formation of a contract. It is intention which differentiates an offer from invitation to
treat. In an email, a seller may clearly explain or specify his or her intention to form a
contract, thereby differentiating an offer from invitation to treat. Moreover, in an
email, there is a possibility for further negotiations and clarifications regarding
intention. Such a facility to establish intention through negotiations does not exist in
an online click wrap agreement. Therefore, while the criteria discussed above under
the electronic transaction legislation of Australia, is a good step forward, there may
still be uncertainties about whether the website is an offer or an invitation to treat.

It leaves some of the questions unanswered, such as how the intention of the vendor
is to determined, and which technology for specifying intent will be considered
satisfactory. One of the advantages of the internet is providing cheap global platform
for small businesses by means of low advertisement costs, start up and maintenance
expenditure.\(^4\)

Mostly electronic contracts are commercial in nature and the parties are presumed to
have intention to create legal relations, thereby intending to be legally bound by the
contract.\(^5\) Therefore if the intention of the online vendor is not clear it is likely that
products made available through online web sites will be regarded as offers. The
electronic transaction legislation of Australia provides some guidance to vendors if
they wish to avoid making an online offer but such guidance may not be adequate as
it does not provide concrete criteria.

Further, automatic websites which allow customers to download music and books
appear to be irrevocable as seen in *Thornton v Shoe Lane Parking Ltd*.\(^6\) In addition,
websites which control the actions of a customer significantly by making the

---

\(^4\) Wales Web Design & Web Development, <http://www.thomas-design.co.uk/website-


\(^6\) *Thornton v Shoe Lane Parking Ltd* (1971) 2 QB 163, 174.
transaction time bound do not provide much scope for a customer to negotiate the contract like a vending machine. Automatic websites resemble vending machines strongly but also slightly differ from automatic websites in both content and functionality. Vending machines are usually used only for cheap disposal items unlike websites which are used for expensive products like laptops. Vending machines carry out the transaction by merely making the selected product available to the customer. While, automatic websites carry out more advanced functions by making decisions such as issuing discount coupons, issuing special product vouchers. Further, through vending machines direct physical selection of products is made unlike web based transactions which are carried out remotely. Due to these difference web based transactions provide scope for more errors.

The principles of unilateral mistake will also not be of much help to the vendors for terminating the contract. Traditional contract law does not provide clear-cut principles in relation to electronic contracts. If online websites are always regarded as offers instead of invitation to treat, then the online vendor may be exposed to the risk of an unanticipated number of acceptances. This risk is increased due to the global nature of the internet. Therefore, the traditional principles in relation to invitation to treat may need reconsideration in the online context.

9.1.1.2 Time of Contract Formation

Time of communication is of importance in an electronic contract yet, problems do exist while identifying exact time of communication. The time of communication cannot be easily established in electronic contracts, though electronic transaction legislation and traditional law of contract are extended to cover time of communication in an electronic contract. Despite the existence and extension of traditional law of contract and statutory law to instantaneous communication and electronic contracts there are problems related to inadequacy of emails and inadequacy of electronic contracts. Thus, areas such as recognition of time of contract formation are uncertain under both traditional law and electronic transaction legislation.
In brief, the analysis of traditional principles of contract and the electronic transaction legislation indicate that there is no rule that can automatically establish time of contract formation for electronic contracts. Therefore, the gap in relation to time of contract formation still persists.

Under the general principles of the law of contract, a contract is formed at the time and place an acceptance is communicated to the offeror as explained in Tallerman and Co Pty Ltd v Nathan’s Merchandise (Vic) Pty Ltd. In determining the time of contract formation, the instantaneous and non-instantaneous nature of communication is the main factor of uncertainty. This ambiguity arises due to the resemblance of electronic communication to both face-to-face and distant communication as described in Chapter Five. Neither the receipt rule nor the postal acceptance rule provide an appropriate fit for electronic contracts especially formed through email communication, even if it is accepted that the postal rule is not applicable to email and acceptance occurs when the message is received. There is still an ongoing debate regarding when communication actually occurs. If an acceptance is sent by email, there are several options regarding the communication of the acceptance, such as the time when the recipient reads the email, or the time that the email is downloaded to the recipient’s computer, or the time when the email is received by the recipient’s Internet Service Provider. Thus, electronic contracts formed through computers can give rise to different dilemmas regarding time of contract formation. There is no single rule workable in all the circumstances. There is no rule that can automatically indicate the time of contract formation for electronic contracts. There is a lack of rules addressing specific unique features of electronic contracts such as specific time of contract formation. Inadequacy in relation to time of contract formation can have a deterring effect especially for commodities with high fluctuating prices such as gold, petroleum and currencies. Such an inadequacy is seen in electronic contracts because, the time of formation of contract poses problems. As a result, contracting parties can suffer losses when the prices of gold, petroleum and currencies change every moment, if time of formation of contract is

7 Tallerman and Co Pty Ltd v Nathan’s Merchandise (Vic) Pty Ltd (1957) 98 CLR 93.
not clearly ascertainable. This handicap can discourage transacting parties from using the internet for such products.

It is necessary to determine the time of contract formation because terms and conditions which are included in a contract after the formation of a contract will not be regarded as enforceable. Online web sites can be updated easily. Therefore, if the time of contract formation is not determined, then it can provide scope for a vendor to claim that the users are bound by terms included after the formation of the contract and mislead consumers. For example, in *eBay International AG v Creative Festival Entertainment Pty Ltd*, which involved online sale of tickets highlights this issue. In this case, online purchasers of the tickets were unable to see a new condition 6 until the tickets were received and the process took over six weeks after completion of the transaction online. Rares J concluded that condition 6, as it appeared on the tickets that were sent to the purchasers, did not apply to any tickets purchased through the website prior to 8 November 2006 (when the website was updated to include the new version of condition 6). Rares J also held that condition 6 on the tickets did not have contractual force and it was not relevant to the contracts under which the tickets were purchased. Thus, by sending tickets including condition 6, Creative had made a false representation in trade or commerce. Therefore, the representations of future matters contained in condition 6 of the *Big Day Out* tickets contravened s 52 of the *Trade Practices Act 1974* (Cth).

Further, it is necessary to determine the time of contract formation because the time of contract indicates where a contract was formed. Email communications resemble the postal system as communication takes place through servers and delays can be caused due to delayed access of emails. Conversely, email communications can also facilitate real time communication like telephone or mobiles round the clock if the offeree is present online and accesses the message instantly. Therefore, the conduct of an offeree and the manner in which they are accessed can trigger the application of

---

9 *Olley v Marlborough Court* (1949) 1 KB 332.
10 *eBay International AG v Creative Festival Entertainment Pty Ltd*, FCA 1768, 28 (2006).
postal rule and receipt rule. Consequently, the legal effect of where a contract is formed may not be automatic but conditional on the conduct of the offeree.

In recognition of the difficulties regarding the time of contract formation, criteria dealing with receipt and dispatch of communication were introduced in the electronic transaction legislation of Australia. While addressing these hurdles, the electronic transaction legislation only provides guidance regarding receipt and dispatch of message. It does not go far enough and state when a contract is formed. The shortcomings of the criteria dealing with receipt and dispatch of communication are identified in Chapter Five. In summary, the legislation provides different criteria for a designated information system (when a specific email address is provided for sending communication) and a non-designated information system (when a specific email address is not provided for sending communication) while dealing with receipt of communication. Hence, the time of receipt will vary depending upon whether there is a designated or non-designated information system. Under the non-designated criteria, receipt may occur when the messages either ‘come to the attention’ of the recipient or when the recipient is ‘reasonably’ aware of the message. In case, a message is sent to an email address that is not in frequent use, receipt will occur only when it is actually viewed or when the addressee, reasonably knows about the receipt. Hence, under the non-designated information system criteria, receipt will occur only in limited situations, especially if it is sent to an email address that is not in frequent use.

One of the greatest advantages of electronic commerce is speed. Hence, the approach of non-designated communication rule will lead to delayed receipt undermining this advantage of electronic commerce. Further, the non-designated criteria can provide opportunity for fraudulent businesses to deceive consumers by delaying time of contract formation by claiming that the message was not viewed or the receiver did not have reasonable information about it. Hence, this approach is too weak to be workable for electronic commerce especially from the prospective of consumer confidence and may not build consumer confidence as was intended by the legislation.

13 Christensen, above n 1.
The electronic transaction legislation of Australia has further complicated the issue. For example, in relation to receipt of communication, it states that the time of receipt is the time when the addressee becomes aware about the message. Awareness can amount to both actual receipt by the receiver or just receipt of the message in the inbox. It does not state whether the receiver must actually read the message or just the availability of the message in the inbox is sufficient.

9.1.1.3 Place of Contract Formation

In summary, neither the traditional contract principles nor the electronic transaction legislation provide specific criteria dealing with place of electronic contracts. As a result, a gap in relation to place of electronic contract still exists.

Issues related to the time of contract formation transforms into jurisdictional issues as discussed in Chapter Five. In recognition of difficulties created due to the global nature of the internet in determining the jurisdiction of parties, criteria dealing with the place of business of parties was introduced in the electronic transaction legislation of Australia which prescribes rules regarding place of business. The intention of the legislation was to provide guidance in relation to jurisdiction through these rules. However, it only provides broad guidelines regarding how to determine the place of business. The shortcomings of these criteria were highlighted in Chapter Five. According to the first criteria, where the originator (sender of a message) or addressee (receiver of a message) has more than one place of business, then the place of business is deemed to be the place that has a closer relationship with the underlying transaction, or if this does not apply, then the place of business is deemed to be the originator’s or addressee’s principal place of business. If the originator or addressee does not have a place of business, then the place of business is deemed to be the place where the originator or addressee ordinarily resides. Websites can be accessed from any place; hence, the criteria related to ‘closer relationship with the underlining transaction’ may lead to multiple places.

The second criteria also appears to be unworkable. It uses ‘principle place of businesses’ as a metaphor. It does not state how to define a principle place of business. It defines place of business only in relation to government activities. Hence, under the ‘principle place of business’ criteria, a vendor who has more than one business branch in different jurisdictions can claim jurisdiction in different places. Similarly, under the ‘ordinary place of residence’ criteria, a vendor who has many business branches and more than one residential place can also claim jurisdiction in multiple places. Hence, a fraudulent vendor can file suits for the same breach of contract in different jurisdictions. Further, he or she can also seek jurisdiction in a particular place to avoid strict consumer protection laws which are unfavourable to them. As a result, these criteria may not build consumer and business confidence, as was intended by the legislation.

The electronic transaction legislation of Australia also provides additional factors for determining the place of business of the parties. Under this criteria, a party’s place of business is presumed to be the place indicated by that party. It requires the other party to demonstrate that the party making such a claim does not have a place of business at that place so revoking the presumption. This places an unfair burden on that other party. In cases where there is more than one place of business, then the place of business is the place that has the closest relationship to the transaction. Under these criteria, in circumstances when a business has different branches spread across different locations, ‘the closest relationship’ metaphor can provide jurisdictions in several places. Further, the definition of place of business itself is too broad to provide jurisdictions in several places. Due to all these shortcomings, the new amended criteria is unlikely to solve the difficulties around jurisdiction.

In addition, the new criteria also enables a court to consider domain names for determining jurisdiction. Domain names do not necessarily indicate the location of

16 Ibid Recommendation 8.
a business. Hence fraudulent traders can provide misleading domain names to avoid jurisdiction. Thus, this criterion also suffers from shortcomings.

In sum, determination of place of business of parties is still problematic under the electronic transaction legislation.

9.1.1.4 Signatures

Electronic transaction legislation and traditional law of contract exists and both are extended to cover electronic signatures. Despite the extension of legislation and traditional law of contract, problems such as reliability and security of electronic signatures do exist. Thus, although there is body of law relating to electronic signatures it does not address the all the issues of electronic signatures.

The analysis of signature cases and the electronic transaction legislation demonstrate that a written signature on a contract cannot always be replaced by an electronic signature. In brief, electronic signatures cannot create evidence per se so, electronic signatures cannot protect transacting parties from fraud as traditional handwritten signatures can. In the light of this issue, the approach adopted by the electronic signature cases indicate that an electronic signature can only be provided validity as well as protection from fraud on the basis of surrounding facts and circumstance of a case. Also, the electronic transaction legislation was not intended to deal with the evidential aspects of an electronic signature. Therefore, the approach adopted by both the electronic signature cases and the electronic transaction legislation is inadequate as outlined below.

The analysis of electronic signature cases indicates the approaches adopted by courts to recognise electronic signatures and how these approaches suffer from limitations. In a recent judicial decision of Australia, McGuren v Simpson, an electronic signature was provided validity under contract law. In this case, a signatory was authenticated on the basis of the authentication fiction doctrine. Under this doctrine, ‘where the party to be charged expressly or impliedly acknowledges the writing as an

---

authenticated expression of the contract, typed words will be deemed to be his or her signature". However, this doctrine has limitations, as it can only apply when the party expressly or impliedly acknowledges the writing as an authenticated expression of the contract. It cannot apply in situations where a person denies a signature and makes a claim of fraudulent behaviour.

Another approach that is being used by courts is to authenticate a signature with the help of the facts and circumstances of the case, as seen in *R v Frolchenko*. In *R v Frolchenko*, Williams J recognised that the modern means of communications may not allow for a personal signature and stressed the importance of authenticating such communications based on the facts of the case. However, even this approach has its limitations, as this can only apply if there are adequate offline surrounding circumstances associated with the identity of the signatory. Hence, in the light of recent judicial decisions discussed above and the increased risk of identity theft in an electronic environment, the legal protection available to electronic signatures still has gaps. Thus, if an electronic signature is used, it can only be recognised on the basis of surrounding facts and circumstances. Electronic signatures cannot create evidence *per se* so, electronic signatures cannot protect transacting parties from fraud as traditional handwritten signatures can. The approaches of validating electronic signatures based upon the surrounding facts and circumstances discussed above was also seen in *Dow Chemical Company v G.E.*, *Bazak International Corp v Tarrant Apparel Group*, *Lamle v Mattel Inc*, *Roger Edwards LLC v Fiddes & Sons*, and *Rosenfeld v Zerneck*. It is likely that these approaches will be followed in future and thus may suffer from similar limitations.

19 Ibid.
22 The Queen v Stefanie Frolchenko (Unreported, Supreme Court of Queensland Court of Appeal P Fitzgerald, J A McPherson and J Williams, 3 March 1998, 20 March 1998).
25 Lamle v Mattel Inc 2005 USAppLEXIS217 (Fed.Cir.2005).
Moreover, electronic signatures are insecure and can raise concerns regarding the impersonation of signatures, as seen in *CSX Transportation, Inc. v Recovery Express, Inc.*\(^{28}\) and *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson.*\(^{29}\)

While, electronic signatures are only provided basic general validity under Australian electronic transaction legislation, as affirmed in *Faulks v Cameron*\(^{30}\) and *Getup Ltd v Electoral Commissioner.*\(^{31}\) However, this legislation was not intended to deal with the evidentiary aspects of signatures such as the important functions of traditional signatures, which include the cautionary, protective, challenging and record keeping functions that were identified in Chapter Seven. Further, the electronic transactions legislation also lacks specific identification requirements. The proposed new amendments to the legislation examined in Chapter Seven also suffer from the same fate. Thus, lack of appropriate consideration of the evidentiary aspects of signatures under the electronic transaction legislation coupled with the enhanced possibility of impersonation of signatures expose contracting parties to considerable risk. In sum, there is lack of concrete signature criteria under the electronic transaction legislation of Australia.

9.1.1.5 Writing Requirements and Storage of Contractual Terms

Electronic transaction legislation requires parties consent for the applicability of the legislation to a contract but does not provide concrete criteria for determining consent. Therefore determination of consent of the parties is problematic. Similarly, the electronic transaction legislation does not specifically deal with storage of terms of an electronic contracts. Hence, gap in relation to this aspect of electronic contracts also still exist.

---

\(^{28}\) *CSX Transportation Inc v Recovery Express Inc* 415 F Supp 2d 6 (Mass, 2006).

\(^{29}\) *Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Martenson*, Case No 1: 2008cv07833 (NYSD, 2008).


\(^{31}\) *Getup Ltd v Electoral Commissioner* [2010] 268 ALR 797.
In order to extend the application of electronic transaction legislation to a contract, it is necessary to prove that the other party to a transaction has consented to the information that is provided electronically. Under the electronic transaction legislation consent may be express or implied as seen from the conduct of the parties. However, it is not certain as to when conduct could be construed as giving of consent. Even though consent is unlikely to be implied because parties have used electronic communications previously, consent may be inferred where parties have conducted similar electronic transactions in the past. The requirement of consent has led to uncertainties in an electronic contract because it is difficult to establish implied consent and the electronic transaction legislation have not defined ‘implied consent’. In order to avoid such situations, the parties to an electronic contract must ensure that the electronic communications are legally certain and identify consent of the parties clearly.32

Analysis of case law indicate that determination of consent for the applicability of the electronic transaction legislation is problematic. Under electronic transactions legislation, transactions can be conducted electronically only if the parties consent to transact through electronic means. In Terumo Corporation v B Braun Melsungen33 it was held for the application of Electronic Transactions Act, if the parties do not specifically object to the mode of communication then implied conduct can be inferred from their conduct. Similarly, in Aristocrat Technologies Inc v IGT34 it was established that implied consent can be inferred from the conduct of the parties if there is long history of communication through electronic means. On similar lines, in Tugum Cobaki Alliance Inc v Minister for planning and RTA35 It was held that making a document available through electronic link also satisfies the requirement of writing under the electronic transactions Act. While, Department of Health and Human Services v H36 appears to indicate that consent can be determined only if there is evidence to prove it. Likewise. KM Ravich v King Island Council and BH Hassing37 it was held that the writing requirements were not satisfied as there was

32 Christensen, above n 8.
34 Aristocrat Technologies Inc v IGT (2008) 80 IPR 413.
35 Tugum Cobaki Alliance Inc v Minister for Planning and RTA [2006] NSWLEC 396.
lack of clear consent. Similar view was also expressed in *Illich & Anor and Baystar Corporation Pty Ltd.* On the other hand, *Kim v Minister for immigration* on 23 August 2005 indicate that the Electronic Transactions Act does not apply to the practice and procedures of the court. Similarly, in *Re Ryan and Secretary, Department of Employment and Workplace Relations* it was held that *Electronic Transactions Regulation 2000*(Cth) Specifically Exempts applicability of *Administrative Appeals Tribunal Act 1975*. Thus, there is lack of concrete consent criteria under the legislation.

Further, the writing requirement prescribed under the Electronic Transaction Legislation of Australia was only intended to provide a basic standard in relation to the electronic form of writing. It provides the minimum standard to be met by an electronic document for retention of documents. Traditional paper-based writing provides a permanent record of terms and conditions agreed between the contracting parties. The permanent retention of record is not considered by the legislation. It merely requires ‘accessibility’ and ‘usability’ of the electronic document falling short of ‘permanent retention’. The criteria is broad enough to encompass any storage device that is capable of retaining the information and permits usability of information. These broad requirements provide less certainty than the traditional paper based contracts and leave more scope for disagreement regarding, terms and conditions that were agreed between the parties. In a traditional contract, terms and conditions are clearly written by the parties, who are physically present and such writing takes permanent form which cannot be changed or altered without the parties detecting any alteration. However, in an electronic contract, alterations of terms and conditions can be easily made, without the knowledge of the parties, due to the lack of permanent form of electronic media and also the absence of paper based contract. In addition, factors such as technological developments or alterations also have an impact on agreed terms and conditions leading to disagreement because, the old version of terms may not be readable in the new version of terms and conditions. Non-assurance of agreed terms and conditions of a contract can discourage contracting parties from effectively using electronic media for contract formation.

---

38 *Illich & Anor and Baystar Corporation Pty Ltd* [2004] WASTR 25.
39 *Kim v Minister for Immigration*—BC200608625.
40 *Re Ryan and Secretary, Department of Employment and Workplace Relations* (2005) 90 ADL 800.
All these shortcomings do not assure enforceability of contracts in the same way as paper-based contracts do. Although the legislation was intended to facilitate effective formation of electronic contracts, it cannot be regarded as an adequate facilitator. Thus, gaps in relation to agreed terms of contract still exist.

Further, analysis of the issue in the context of electronic contracts formed through mobile phones illustrate additional difficulties. Data stored in a mobile phone in the form of a text SMS or in the memory of a SIM card (subscriber Identity Module) can also amount to writing under the broad criteria provided under the electronic transactions legislation of Australia. Mobile phones can be stolen easily thereby making data tampering relatively easy and also leading to easy data loss. Mobile phones can be easily stolen as seen in *Hayek v R*, 41 *Johnson v R*, 42 *Director of Public Prosecutions (DPP) v Malikovski*, 43 *Joyce v Gee*, 44 *Nanai v R*, 45 *Dolan v R*, 46 *Devine v R*, 47 *Director of Public Prosecutions (DPP) v Kuru*, 48 *R v Mann*, 49 and *R v Harris*. 50 Thus, data can be more easily tampered, destroyed and lost in case of mobile phones. Therefore, all the above shortcomings do not assure enforceability of electronic contracts in the same way as paper-based contracts do. Thus, broad writing requirements do not appear to be appropriate for electronic contracts.

Further, in the case of electronic contracts formed through mobile phones, evidence of text message from a mobile phone and memory of a SIM card appears to be acceptable as evidence only if the data is accurate as seen in *Bevan v The State of western*. 51 This can further add another layer of complexity in the context of electronic writing by creating evidentiary issues.

9.1.1.6 Conclusion of Primary Research Question

41 *Hayek v R* [2010] NSWCCA 139.
43 *Director of Public Prosecutions (DPP) v Malikovski* [2010] VSCA 130.
44 *Joyce v Gee* [2010] WASC 76.
48 *Director of Public Prosecutions (DPP) v Kuru* [2009] VSCA 206.
49 *R v Mann* [2009] VSC 536.
50 *R v Harris* [2009] VSCA 189.
51 *Australia Bevan v The State of Western Australia* [2010] WASCA 101 para 15–16.
Overall, the electronic transaction legislation indicated its shortcomings. In conclusion, the electronic transaction legislation of Australia did not address all issues related to electronic commerce. Issues relating to electronic signatures, time of contract formation, jurisdiction, and invitation to treat and writing requirements still exist.

Table below summarises the gaps of electronic transaction legislation identified in the previous section:

<table>
<thead>
<tr>
<th>Electronic Transactions Act (vic)</th>
<th>Gaps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time of receipt s 13 A</td>
<td>Lack of concrete criteria in relation to ‘designated’ and ‘non designated’ information system</td>
</tr>
<tr>
<td>Time of dispatch s 13</td>
<td>In relation to s13 the Act does not explain what amounts to entry into the first information system as seen in SZSKX v Minister for Immigration and Anor.52 and Liu and Ors v Minister for Immigration and Anor53</td>
</tr>
<tr>
<td>Place of business s 13 B</td>
<td>Does not provide concrete criteria</td>
</tr>
<tr>
<td>Click wrap agreements and mistaken identity issues</td>
<td>Lack of concrete criteria in relation to closest business</td>
</tr>
<tr>
<td>Writing s 8</td>
<td>Does not deal with these issues</td>
</tr>
<tr>
<td>Signature s 9</td>
<td>Electronic signatures are provided validity only if evidentiary issues are not raised as seen in Faulks v Cameron59, Getup Ltd v Electoral Commissioner60, and Lang v the Leasing Centre (Aust) Pty Limited and Anor61</td>
</tr>
</tbody>
</table>

52 SZSKX v Minister for Immigration and Anor [2014] FCCA 157 (4 April 2014).
53 Liu and Ors v Minister for Immigration and Anor [2013] FCCA 2208 (9 December 2013).
55 Aristocrat Technologies Inc v IGT.55 Tugum Cobaki Alliance Inc v Minister for planning and RTA56, Department of Health and Human Services v H57, KM Ravich v King Island Council and BH Hassing58.
56 Tugum Cobaki Alliance Inc v Minister for Planning and RTA [2006] NSWLEC 396.
60 Getup Ltd v Electoral Commissioner [2010] 268 ALR 797.
There is lack of concrete signature criteria as seen in *Corneloup v Adelaide City Council*\(^62\) Points North \(^63\) and *Lang v the Leasing Centre (Aust) Pty Limited and Anor*\(^64\)!

9.1.2 What Issues Arise When Traditional Contract Principles are Applied to Electronic Contracts?

Gaps found after the analysis of traditional law can be summarised under the following sub-headings.

9.1.2.1 Click Wrap Agreements

Although there is a vast body of law relating to click wrap agreements there are still uncertainties in the online context.

The use of click wrap agreements is complicated, as they do not provide scope for a user to negotiate the terms of a contract.\(^65\) Favourable online terms can be unilaterally imposed by the vendor, and the users cannot proceed with the transaction unless they accept them. As a result, click wrap agreements can make consumers vulnerable.\(^66\) Click wrap agreements incorporate terms through hyperlinks. Terms which are incorporated through hyperlinks in turn incorporate documents creating a branching tree of several click wrap agreements. Therefore, use of hyperlinks make online scenario more complex and complicated. Some online web sites such as the Australian ticket agency\(^67\) time bound the transaction by allotting specific time for the completion of the transaction. The amount of time allotted to complete the transaction may not permit a consumer to view all the terms of the online transaction prior to agreeing to the terms. Click wrap agreements also pose some novel problems. For example, if consumer purchases online software, downloads the software and later wishes to return the product there will be no physical product or

---

\(^{62}\) *Corneloup v Adelaide City Council* [2010] SADC 144.

\(^{63}\) *Points North* [2006] QBCCM 212.

\(^{64}\) *Lang v the Leasing Centre (Aust) Pty Limited and Anor* [2014] VCC 910 (20 June 2014).


commodity to obtain a refund. In addition, online websites can also be easily upgraded, including new terms which further complicates the online context.\textsuperscript{68}

The federal government has introduced the new \textit{Competition and Consumer Act} 2010. The aim of the new law is to harmonise the consumer laws of Australia as well as update consumer laws of Australia. It also proposes reform to provisions dealing with unfair terms.\textsuperscript{69} It focuses more on balance of fairness. In addition, under the Act an action can only be taken only after the consumer suffers loss.\textsuperscript{70} The Act appears to be unsatisfactory as it does not \textit{per se} prevent the use of unfair terms.

Additionally, click wrap cases analysed in the thesis indicate that validity is easily provided to these agreements even if they are made casually as part of the registration process.\textsuperscript{71} Hence, this approach must be adopted with caution, because if followed, users will be easily bound when unfair terms are included in such agreements. \textit{Peter Smythe v Vincent Thomas},\textsuperscript{72} involved the sale of an aircraft. The binding nature of the click wrap agreement was recognised in this case as the parties had accepted the terms and conditions of the website by clicking on an acceptance icon as part of the registration process.\textsuperscript{73} An aircraft was listed on the ebay web site by the defendant. Plaintiff made a bid for the aircraft. Both the plaintiff and the defendant received notification by ebay stating that the plaintiff had won the aircraft. The defendant refused to sell the aircraft to the plaintiff and claimed that a valid contract was not formed. The defendant argued that the contracts were only formed between ebay and the plaintiff and, ebay and the defendant therefore no contract was entered into between the plaintiff and the defendant.\textsuperscript{74} The court held that the terms and conditions of ebay web site created a framework within which both the plaintiff and the defendant were participants. It was found that when parties register with ebay.

\textsuperscript{68} Ibid; Clapperton and Corones, above n 65,156–175.
\textsuperscript{70} Gray, above n 69; Nottage, above n 69.
\textsuperscript{71} \textit{Peter Smythe v Vincent Thomas} (2007) NSWSC 844.
\textsuperscript{72} Ibid.
\textsuperscript{73} Ibid.
web site by clicking on the acceptance icon, they agree to follow the terms of ebay which also includes parties to complete the transaction when the auction is carried out.\textsuperscript{75} Thus, in \textit{Peter Smythe v Vincent Thomas},\textsuperscript{76} the click wrap agreement was easily recognised without evaluating whether the users intended to adopt the underlying terms presented to them, which were generally presented as part of the registration process.\textsuperscript{77} This appears to indicate that in an online context click wrap agreements can be easily regarded as enforceable. If this approach is followed, users will be easily bound when unfair terms are included in such agreements.

In \textit{eBay International AG v Creative Festival Entertainment Pty Ltd},\textsuperscript{78} the scope of s 52 of the \textit{Trade Practices Act} 1974 (Cth) was discussed. In \textit{eBay International AG v Creative Festival Entertainment Pty Ltd},\textsuperscript{79} the issues was whether the click wrap agreement had contravened s 52 of the \textit{Trade Practices Act} 1974 (Cth). As seen in this case, click wrap agreement will be enforced only if a clear notice of the terms is provided to the contracting party at the time when the product is purchased. Further, click wrap agreements do not have scope to negotiate the terms of the contract as seen in these cases. In addition, as seen in this case, click wrap agreements can turn out to be misleading and deceptive if all the terms and conditions are not brought to the attention of the parties at the time when the transaction is conducted. Online websites can be easily upgraded to include new terms which complicates the online context. Further this novel feature can also more easily mislead consumers. Although s 52 prevents misleading and deceptive conduct, it could go further to protect consumers by specifically addressing complexities involved in an online context.

Overall, the protection available to consumers in an online context appears inadequate, and may not facilitate the development of global electronic commerce.

\textsuperscript{75} \textit{Peter Smythe v Vincent Thomas} (2007) NSWSC 844, paras 37–40; E-commerce Update, above n 74.
\textsuperscript{76} \textit{Peter Smythe v Vincent Thomas} (2007) NSWSC 844.
\textsuperscript{77} \textit{Le Mans Grant Prix circuits Pty Ltd v Lliadis} (1998) 4 VR 649.
\textsuperscript{78} \textit{eBay International AG v Creative Festival Entertainment Pty Ltd} [2006] FCA 1768 at 28.
\textsuperscript{79} \textit{eBay International AG v Creative Festival Entertainment Pty Ltd} FCA 1768, 28 (2006).
9.1.2.2 Mistaken Identity

the article leads to the consideration of deficiencies in relation to mistaken identity. Traditional common law principles cannot accommodate mistaken identity issues in relation to mobile commerce. Unlike offline transactions identities cannot be adequately identified and attributed to a specific person in the online scenario. Digital identities are growing rapidly and are distinct from our physical offline existence.\textsuperscript{80} These digital identities are blending into the digital enterprise. Users create personal credentials for baking, consumer products, electronic commerce retailing, government services, home insurance policies and even for remote internet access. Organizations are realizing the power of digital identities. However, a logical single and trustworthy universal secure digital identity which can be used with confidence across different sectors is still lacking.\textsuperscript{81}

Traditional common law principles appear to be displaced with regards to mobile commerce. Liberal interpretation of traditional contract principles can easily prejudice the innocent parties involved in the transaction. The insecure nature of internet and easy means of tampering identity of another party warrants judicial intervention. Appropriate legislative measures must be taken to prescribe specific security standards which could protect the innocent parties to a considerable extent. In the light of easy means of tampering the identity of a person in an online scenario adequate measures must be taken to protect the rights of the innocent third party. A standard based on a technical neutral and media neutral approach must be adopted to protect both the person first deceived and the innocent third party.

Due to the inherent insecure nature of internet a person cannot be made specifically accountable for an act in the online medium. As a result, there is need for specific guidelines which can be used to assess the adequacy of the authentication measure used by the parties in relation to mistaken identity cases. There is a need for law


reform in these three areas. Firstly, the distinction between face to face dealings and paper based transactions should be removed. Secondly, there is need for specifying what measures contracting parties should take to secure their transactions. In this regard, there is also a need to prescribe guidelines regarding who should bear the loss if the authentication method is compromised. Arguably, internet is an inherently insecure medium and if the party first deceived takes the risk of entering into a contract over the internet then the party first deceived should be made to bear greater part of the loss in mistaken identity scenarios. Innocent third party should be made to bear lesser part of the loss. Thirdly, it is necessary to provide guidelines regarding how the importance of identity should be proved and against whom the contract should be enforced. Equally important is the need to state what should be the basis to assess whether a person is who he claims to be. In particular, legislative response should specify what minimum measures should a party take to determine the authenticity of the transaction and who should be made accountable.

9.1.2.3 Conclusion of Primary Research Question Two

Overall, analysis of traditional contract principles indicated their shortcomings. In conclusion, although there is law relating to click wrap agreements and mistaken identity uncertainties still persist in the context of electronic contracts. Traditional contract principles are inadequate and may not facilitating the development of electronic commerce. Hence, new laws need to be drafted.

9.1.3 Sub-Question One: Do Other Jurisdictions Have the Same Issues? Is it an International Problem?

Similar to Australia, the UK and the USA have introduced new legislation to deal with impediments arising in electronic commerce due to traditional laws. The legislation goes beyond the Australian legislation as they either favour consumers or better acknowledge the technical features of electronic contracts. Australian legislation is more minimalist than any of these legislations. While it is commendable to note that different countries have adopted different approaches for facilitating electronic contracts, none of them provide an appropriate solution.
The shortcomings of the laws of these jurisdictions and their differences from the Australian legislation have been evaluated are elaborated below under various sub-headings (please see below for details).

The table below summarises the different approaches adopted by the electronic transaction legislation of different countries analysed in the thesis.

<table>
<thead>
<tr>
<th>ISSUES</th>
<th>AUSTRALIA</th>
<th>USA</th>
<th>U.K</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage of terms of electronic contracts</td>
<td>The permanent retention of record is not the aim of the legislation. It merely requires ‘accessibility’ and ‘usability’ of the electronic document falling short of ‘permanent retention’</td>
<td>Provide supplementary criteria in relation to writing requirement which specifically talk about storage of electronic documents ‘retrievable in a perceivable form’</td>
<td>Precisely deal with storage of terms and conditions of electronic contract</td>
</tr>
<tr>
<td>Reliability of electronic signature</td>
<td>None</td>
<td>E-signs of USA provides detailed consumer protection laws favouring consumers specifically in relation to electronic documents</td>
<td>None</td>
</tr>
<tr>
<td>Determination of time of contract formation</td>
<td>Provides general basic criteria regarding dispatch and receipt of message</td>
<td>UETA and E-sign of USA specifically emphasise on intention of the signatory and its association with the electronic record and electronic contract. UETA also provides supplementary provisions regarding verification of electronic signatures.</td>
<td>Provides technical requirements which are inclined towards digital signatures. It guarantees reliability only on the basis of digital signatures. Electronic transaction legislation of UK also specifically talks about admissibility of electronic signatures as evidences</td>
</tr>
<tr>
<td>Determination of place of contract formation</td>
<td>Provides general basic criteria regarding place of business</td>
<td>Provides vague criteria regarding place of business</td>
<td>Provides supplementary requirements regarding center of business activities in relation to place of contract formation</td>
</tr>
</tbody>
</table>
Addressing complexities of click wrap agreements

| None | None | Deal with incorporation of terms |

9.1.3.1 Writing and Storage of Contractual Terms

Paper-based documents posed obstacles to electronic contracts, as identified in Chapter Three. In recognition of these shortcomings, the *Uniform Electronic Transactions Act 1999*[^82] (UETA) of the USA prescribes criteria similar to that of the electronic transaction legislation of Australia. Further, UETA goes beyond the Australian legislation and requires documents to be specifically stored in relation to the writing requirement. Although it prescribes additional criteria, it is not completely satisfactory, and suffers from the limitation by using controversial terms for example in relation to writing, the Act requires the electronic record to be ‘retrievable in a perceivable form’. This phrase raises serious unanswered questions. Documents that are corrupt can be reproduced in a perceivable but unreadable form. Hence, the requirement raises unanswered questions regarding what amounts to ‘retrievable in a perceivable form’.[^83] The definition of the term electronic record places additional requirements.

Conversely, the *Electronic Signatures in Global and National Commerce Act*[^84] (E-SIGN) which validates the use of electronic contracts and electronic writing, provides detailed consumer protection provisions and favours consumers by limiting the ability of sellers to effectively conduct transactions. E-SIGN provides many consumer protection provisions that protect consumers from unintentionally entering into electronic contracts. It requires consumers to provide their consent and requires the vendor to fulfil a number of requirements.[^85] It prescribes several requirements such as informing the consumer about the options of obtaining information in an non-

[^83]: Ibid § 2(13).
electronic form, informing consumers about their right to withdraw consent, informing the consumer whether the consent is sought for a particular transaction or for a particular category of notices, informing the consumer regarding how a paper-based copy can be obtained, notifying the consumer regarding the hardware and software that will be required for accessing it, ensuring that the consumer can access the information in a particular format.\(^{86}\) It can be argued that these requirements place unreasonable burden on businesses to take consent from consumers and jeopardise the enforceability of electronic contracts.

Although the purpose of the E-sign is to facilitate electronic commerce, the Act could be seen to discourage online vendors because, it favours consumers, tilting the balance towards the buyer and consumers. Strict consumer protection provisions can create obstacles for the continued development of electronic commerce due to improper balance in favour of consumers against sellers ability to progress in electronic business. It can adversely affect the incentive of businesses to conduct transactions through electronic means. Hence, a more balanced approach would better serve the purpose of facilitating electronic commerce.

Along similar lines, the aim of the electronic transaction law of the UK was to remove obstacles to the use of electronic contracts. In relation to the writing requirement, it validates the electronic form of writing to facilitate electronic commerce. Further, it also provides criteria that specifically refers to the storage of terms of a contract. In an electronic contract, alterations of terms and conditions can be easily made, without the knowledge of the parties, due to lack of permanent form of electronic media. By making reference to storage of contract terms, the criteria make an attempt to resolve this aspect. Hence, this criterion goes beyond the Australian electronic transaction legislation. However, it suffers from limitations as sufficient consideration has not be given in prescribing clear guidelines regarding how these requirements needs be to fulfilled. Article 10(3) of the Electronic Commerce Directive only says ‘contract terms and general conditions provided to the

recipient must be made available in a way that allows him to store and reproduce them.\footnote{Directive 2000/31/EC on Electronic Commerce [2000] OJ L 178/1.}

9.1.4.2 Time

Electronic communications such as email incorporate features of instantaneous and non-instantaneous communication as described in Chapter Five. Hence, neither the receipt rule nor postal rule can be specifically applied, as discussed in Chapter Five.

In recognition of these difficulties, UETA prescribes rules dealing with the time of electronic communication. Unlike the Australian legislation, UETA provides guidance regarding the technical aspects of sending messages, taking account of some technical aspects of electronic communication. It requires the electronic communication to be addressed properly. Further, it requires the communication to be sent to a system from which it can be processed appropriately, it also requires it to be sent to a system from which it can be viewed appropriately.\footnote{Amelia H Boss, ‘The Uniform Electronic Transactions Act in a Global Environment’ (2001) Idaho Law Review 275, 327.} However, this provision only applies if the message is ‘addressed properly or otherwise directed properly to an information processing system that the recipient has designated’ or if it is sent to a system which the recipient ‘uses for the purpose of receiving electronic records or information of the type sent’.\footnote{Uniform Electronic Transactions Act 1999, § 15(a)(1).} Hence, it is not necessarily well suited for electronic contracts as it does not provide rule workable in all the circumstances. It works only in the situations discussed above.

Impediments associated with time of receipt of electronic communication have also been addressed under the law of the UK. However, it contains detailed consumer protection provisions regarding the acknowledgement of receipt and favours consumers. This can discourage businesses hence is not necessarily well suited. Australia does not have similar consumer protection provisions dealing specifically with electronic contracts and addressing complexities of electronic communication hence Australian legislation is more minimalist.
9.1.4.3 Place of Business

A contract is formed at the time and place where acceptance is received. This creates difficulties in determining place of contract formation, as discussed in Chapter Five. In recognition of difficulties created due to place of contract formation, UETA prescribes place of business criteria, and these criteria are similar to the Australian approach.

The Electronic transaction law of the UK prescribes similar criteria to that of Australia to deal with hurdles in relation to place of business. However, it goes beyond the Australian legislation, by providing additional detailed requirements regarding center of business activities.

9.1.4.4 Signature

The electronic form of signatures poses impediments for the development of electronic commerce, as identified in Chapter Seven. In order to address this difficulty, UETA and Electronic transaction law of the UK have prescribed signature criteria that provide further detail requirements compared to Australian law.

Unlike traditional signatures, electronic signatures do not create evidence, which is a considerable shortcoming. UETA and E-SIGN do not address this issue, resulting in gaps in relation to this issue. However, UETA places greater emphasis on intention of the signatory and its association with the electronic record and electronic contract. Further, s 9(a) of UETA does not prescribe a particular signature technology it provides supplementary provisions regarding verification of electronic signatures. The Electronic transaction law of the UK only talks about admissibility of electronic signatures as evidences.

Conversely, electronic transaction law of the UK addressed this shortcoming, but it is highly technical. It guarantees reliability only on the basis of digital signatures. It
recognises the digital signature certificates of other countries if the requirements prescribed under Electronic transaction law of the UK are met.

Interestingly, an analysis of the cases also indicates that different approaches are being taken to recognise electronic signatures. In *Cloud Corporation v Hasbro, Inc*[^90^] and *Lamle v Mattel, Inc.*[^91^] and *Shattuck v Klotzbach,*[^92^] the issue in each case involved the recognition of a name in an email as a signature for the purpose of the statute of fraud. Names in an email were accepted as a valid signature by drawing analogies between electronic signatures and traditional signatures in these cases without evaluating the protective functions of paper-based signatures such as protection against fraud. The cases appear to have ignored the protective function of traditional signatures. Traditional signatures protect parties from fraud by specifically identifying the signatory and by maintaining integrity of the document.[^93^] These functions were not emphasised in these cases. While it can be generally accepted that electronic signatures are provided legal validity, uncertainty can still arise in situations when an electronic signature is tampered with. Therefore, the legal validity of electronic signatures is still problematic. The effect of a person’s name in an email was also considered in *Brantley v Wilson.*[^94^] In this case,[^95^] buyers of real estate argued that one of the seller’s names in an email constituted the required signature of the seller. The name in the email was not recognised as a valid signature under UETA due to lack of clear intention to adapt it as a signature.

The analysis of the cases in UK indicate that a name in an email will be recognised as a valid signature only if a person’s intent to sign the electronic document is clearly ascertainable, as seen in *Nilesh Mehta v J Periera Fernandes S.A.*[^96^] The issue in this case was whether automatic insertion of an email address amounts to a signature for the purpose of the statute of fraud. The automatic insertion of an email address was

[^90^]: Cloud Corporation v Hasbro, Inc 314 F 3d 289 (7th Cir, 2002).
[^91^]: Lamle v Mattel Inc 394 F 3d 1355 (Fed Cir, 2005).
[^95^]: Ibid.
not accepted as a signature due to lack of intention of the party to adapt it as a signature. A more restrictive and stricter approach was adopted in *Hall v Cognos Limited*,97 where it was held that only a printed name of an email can be considered signed writing, for the reason that it provides stronger evidence. It appears that courts are still reluctant to readily provide validity to electronic signatures.

9.1.4.5 Click Wrap Agreements

An analysis of cases in the US indicates that the requirement of reasonable notice in an electronic environment seems to be adequate only when the electronic agreements provide more obvious notice. Courts are reluctant to enforce the agreement if the notice is not obvious enough. Agreements where a user specifically clicks ‘I agree’ button after being notified clearly about the terms are being enforced by the courts.

In the context of electronic contracts, concerns of courts for not enforcing click wrap agreements have been lack of obvious notice. For example, in *Ticket Master Corp. v Ticket Masters.Com Inc*,98 the court found that simply listing of terms on the main page of the website did not amount to sufficient notice and refused to enforce the agreement. A similar view was expressed in *Pollstar v Gigmania Ltd*.99 In *Specht v Netscape Communications Corp*,100 the court held that simply because a user might have known that additional information did exist below the icon, does not mean that the user must have reasonably concluded that a license agreement appeared at such a location.101 The decision in *Feldman v United Parcel Service, Inc*102 was also based on similar reasoning, where a pop up window that provided notice about the terms was not enforced, as it did not provide specific link to the terms page.

Ambiguous ways of including terms through hyperlinks have only been enforced if the contracting party is a long time user of the website, as seen in *Druyan v*

---

97 *Hall v Cognos Limited*, Industrial Tribunal Case No.1803325/97.
100 *Specht v Netscape Communications Corp*, 306 F 3d 17, 31–32 (2nd Cir, 2002).
101 Ibid.
However, continuous use of a website is used as a basis of enforceability only if a user is provided with notice of the changed terms beforehand, as seen in *Douglas v United States District Court for the Central District of California*. In relation to the notice requirement, the obviousness of the notice is becoming paramount in the online context. If this path is followed, in most situations, click wrap agreements will be regarded as unenforceable due to lack of obvious notice or enhanced notice. This approach can have negative implications on online vendors and may not provide enough incentive to conduct online transactions.

Electronic transaction law of the UK only vaguely deals with incorporation of terms, Australia has no similar provision.

To sum up, the legislation of Australia is more minimalist than that of the US and the UK. Unlike these jurisdictions, Australia has no consumer protection provisions or provisions addressing technical features of internet. However, the approaches adopted by these jurisdictions are also not completely satisfactory. They have inclined more towards either technology or consumer protection, which can affect the incentive of business to function online and hinder technological development. Hence, a more balanced approach can effectively regulate electronic commerce.

Various factors such as different traditional backgrounds, the impact of international developments, the influence of rapidly changing signature technologies and the influence of the laws of other countries have led to different approaches adopted by different countries to regulate electronic contracts.

9.1.4.6 Mistaken Identity

Comparative analysis of the laws the UK, The USA and Australia indicate that the laws are deficient from the prospective of mistaken identity. Different approaches have been adopted by these two jurisdictions. Influence of technology and

---

103 *Druyan v Jagger*, 508 F Supp 2d 228 (SDNY, 2007).
104 *Douglas v United States District Court for the Central District of California*, 495 F 3d 1062 (9th Cir, 2007), cert. denied sub nom; *Talk Am Inc v Douglas* 128 S Ct 1472 (2008).
international developments has led to the adoption of different approaches. However, the Australian law appears to be more technology neutral in approach and appears to be a better model. In addition, reform of Australian contract law appears to be the first step in the right direction.

An analysis of laws of the US and the UK show similar gaps and uncertainties. As in Australia, a lack of a predictable and certain legal framework provided the impetus for legal change in these jurisdictions and also led to the development of global norms. Other jurisdictions also have problems like the Australian legislation it is an international problem.

9.1.4 Sub-Question Two: What Is the Role of International Developments in Addressing Issues? How Is Australia Responding to the International Developments?

The analysis of international developments indicates how international developments are trying hard to materialise and appropriately regulate electronic commerce from the 1980s. The Model Law on Electronic Commerce was developed in 1996, and then the Model Law on Electronic Signatures was developed in 2001. The Convention on the Use of Electronic Communications was developed in 2005. Rapidly changing technologies are posing difficulties for the international developments to shape up and materialise appropriately.

In essence, international organisations such as ICC, OECD and UNCITRAL are playing a significant role in resolving issues dealing with electronic contracts. Various organisations have been working in close cooperation and in a coordinated manner since the 1980s to resolve the issue, as illustrated in Chapter Two. Chapter Two also sought to explain that apart from national and international developments, regulation of electronic contracts in the form of trading partner agreements also took place at the national level, which played a significant role in the entire norm generation process. Trading partners agreements consisted of terms and conditions which were drafted by the traders to overcome the obstacles associated with electronic commerce, which were These international developments played a major role in shaping the national developments. This also indicates that the international developments are still in the process of materialization.
Like the national laws discussed above, international developments also suffer from similar gaps in relation to electronic contracts. Due to rapid technical development as well as inadequate consideration of all the aspects of electronic contracts, international developments have not materialized completely. New features of internet have been creating impetus and the need to acknowledge that traditional principles alone are unworkable from 1970s as identified in Chapter Two. Outdated traditional laws have been threatening the growth of effective development of electronic commerce from 1970s as illustrated in Chapter Two. Inadequate laws can similarly threaten its effective development in future also.

Additionally, inadequate traditional laws provided the impetus for the development of global norms as identified in Chapter Two. Inadequate legal framework of electronic contracts can likely provide similar impetus for regulation in future also.

International developments that are technologically neutral in approach are having a direct influence on the Australian electronic transaction legislation, which was based upon the *Model Law on Electronic Commerce 1996*. To keep pace with international developments related to electronic contracts, the Australian government is currently considering accession to the Convention on the Use of Electronic Communications 2005. OECD’s declaration on authentication also had an influence on Australia. However, the *Model Law on Electronic Signatures 2001* was not adopted as it was more inclined towards digital signatures.

More specifically, Chapter Two showed that both the *Model Law on Electronic Commerce 1996* and *Model Law on Electronic Signatures 2001* acted as guiding principles for the development of the UN Convention on the Use of Electronic Communications 2005. Although the *Model Law on Electronic Signatures 2001* did not have a direct influence on Australia, it still had an indirect influence as it was part of the norm generation process of the convention that Australia is planning to adopt.

The developments leading to the introduction of Australian electronic transaction legislation that have occurred from 1980s represent two main concerns. The first is
that the failure to follow international trends such as the development of electronic transaction legislation would adversely affect Australian businesses in their international transactions. Second, there was a growing concern regarding how the electronic transactions, which are relatively new, are to be conducted effectively in the absence of predictable legal environment. In addition to all the these factors, non-binding obligations created by the Model Law on Electronic Commerce in 1996 and the OECD Declaration on Authentication for Electronic Commerce also provided the impetus for the development of electronic commerce legislation in Australia. Thus, fear of uncertain law coupled with the influence of international developments such as the UNCITRAL Model Law on Electronic Commerce 1996 and the OECD Declaration on Authentication provided the main impetus for the introduction of electronic transaction legislation, as identified in Chapter Three. It is likely that international instruments if undertaken will likely have a similar influence on Australia in future. Similarly, the laws of the US, the UK were influenced by international developments.

9.2 Concluding Remarks: Summary of Major Findings, Contributions of the Research to the Area of Electronic Contracts and Recommendations

Regulation of electronic contracts is at a cross-roads. The effectiveness of the Australian electronic transaction legislation remains unclear. In the absence of scholarly research in this area, this thesis provides a new conceptual framework of gaps and international developments. Within this framework, further considerations regarding suitable legislation can be made in Australia. This thesis draws parameters within which solutions can be found, but does not attempt to provide solutions. Providing solutions is an area for future research.

This thesis has identified current gaps in Australia in relation to electronic contracts, and how these gaps can cripple the effective development of electronic contracts.

The analysis of the laws of other countries provides additional insights into these issues by indicating how different approaches are being adopted by various other countries.
By analysing international developments, this thesis demonstrates how international instruments have influenced Australian legislation in the past, and what likely impact they can have in the future. This aspect of the thesis also offers contribution in terms of theoretical application of international law.

9.2.1 Recommendations and Suggestions

The analysis conducted in the thesis can be boiled down to make the following suggestions and recommendations:

1.) The thesis identified gaps dealing with electronic signatures, time of contract formation, jurisdiction, invitation to treat and writing requirements. The common key deficiency which emerged from the analysis is that the electronic transaction legislation has fallen short of its intended aim of building business and consumer confidence in electronic commerce. Comparative analysis of electronic transaction legislation with other jurisdictions such as USA and UK, also indicated that the electronic transaction legislation is more minimalist than the other jurisdictions. Although the approaches adopted by other jurisdictions are more comprehensive, none of them provide an appropriate solution. Therefore, more legislative action dealing with these gaps can better facilitate electronic commerce.

2.) New criteria dealing with electronic signatures, time of contract formation, jurisdiction, invitation to treat and writing requirement must be introduced in the existing electronic transaction legislation.

3.) Analysis of international developments indicate that the international developments are still trying hard to materialise and appropriately regulate electronic commerce. Australia must closely monitor these developments.

4.) The thesis also identified gaps dealing with click wrap agreements. The key deficiency that has emerged is that the traditional principles dealing with these issues are displaced in an online context. Displaced traditional principles are affecting the interests of the contracting parties and also the development of electronic commerce. These issues were never considered as
being covered by the electronic transaction legislation or the international developments. Consideration of these issues by the electronic transaction legislation can better regulate electronic commerce.

5.) New criteria dealing with click wrap agreements must be introduced in the existing electronic transaction legislation through amendment.

9.3 Areas for Future Research

As identified in the thesis, international developments are playing a significant role in resolving issues related to electronic contracts. However, both traditional law and the electronic transaction legislation have been inadequate in resolving these issues. A new signature guideline titled ‘Promoting Confidence in Electronic Commerce: Legal Issues on International use of Electronic Authentication and Signature Methods’ was released by UNCITRAL in 2007.\(^\text{105}\) Hence, one area that justifies future research would be the influence, if any, those guidelines will have on Australia and other countries.

BIBLIOGRAPHY

JOURNAL ARTICLES, CONFERENCE PAPERS AND NEWS PAPER ARTICLES


Arasaratnam N and Barber S, ‘Electronic Transactions Update’ (2001) 2(1) Communications Law Bulletin 1


Avellan Hancock J A, in Borderless Cyberspace: The Cross Jurisdictional Validity of Electronic Signatures and Certificates in Recent Legislative Texts’ (1998) 38 Jurimetrics 301


Chen-Chi L and Chi-Sung L ‘The GPKI developing Status of Taiwan and Some Major Asian Countries’ (2003) 26 Computer Communications 1884


Clark D, ‘Cisro Connect Online’ (1997) 1 (6) IEEE Internet Computing 55


<http://www.infoworld.com/articles/tc/xml/00/10/16/001016tcdigcerts.html> at 11 August 2008


338


Das K M, ‘Forum Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the “Reasonably Communicated” Test’ (2002) 77 Wash. L.Rev. 481


Davidson S J and Bergs S J, ’Open, Click or Download: What Have You Agreed To? The Possibilities Seem Endless’ (1999) 6(4) The Computer Lawyer 1


340


Friedman L M, ‘A Quick Ride on the Internet(part1)’ (1997) CBA REC 42


Fuller L, ‘Consideration and Form’ (1941) 41 Columbia Law Review 799


Giles D, ‘You have got mail..or have you?’ (2002) 3(1) *Internet Law Bulletin* 12


Gray A, ‘Unfair Contracts and the Consumer Law Bill’ (2009) 9(2) *QUTLJJ* 155


Hill S W B, 'Flogging a Dead Horse-The Postal Acceptance Rule and E-mail' (2001) 17 (2), Journal of Contract Law 151


Hoye, J C, ‘Click- Do We Have a Deal?’ (2001) 6 Suffolk J. Trial and App. Advoc 163


Koger J L, ‘You Sign, E-Sign, We All Fall Down: Why the United States Should Not Crown the Market Place as Primary Legislator of Electronic Signatures’ (2001) 11 *Transnational Law and Contemporary Problems* 491


Lloyd I, ‘Shopping in Cyberspace’ (1993-1994) (3) 1 International Journal of Law and Information Technology 335


Mekeiver P, ‘Contracting on the Internet’ (2001) 4 (8) Inhouse Counsel 90

McNamara J and O’Shea K, ‘Minimising Legal Risks in Electronic Contracting’


MiK E K, From Clay Tables to AJAX Replicating Writing and Documents in internet Transactions 15(8) Journal of Internet Law2, 2-4


Moriarty C, ‘The Internet: Removing the Mystery Does it have any Real Application?’ (1994) National Accountant 40


Moriarty C, ‘The Internet: Removing the Mystery Does it have any Real Application?’ (1994) National Accountant 40


Murry D R and Chorvat T J, ‘Stepping up to the Next Level: From The UETA to the URE and Beyond’ (2000-2001) 37 Idaho Law Review 415


Noeding T and Bumberger K, ‘Electronic Signatures in German Civil Law’ (2001) 6 (3) Communications Law 8


Perritt H H, ‘Cyberspace and State Sovereignty’ (1997) 3 Journal of International Legal Studies, 155


Rosas R, ‘Comparative study of the formation of electronic contracts in American law with references to international and Mexican law’ (2003) 26 Houston Journal of International Law 63


Ryrie T, ‘Connecting to the Net’ (1997) Charter 42

Ryrie T, ‘Enter the Web’ (1997) Charter 42

Ryrie T, ‘Messaging the Media’ (1997) Charter 50


Shipman A, ‘Managing E-mail and E-Commerce Records’ Records Management Journal 98


Smart Phones and Tablets for Measurements and Controls <http://zone.ni.com/devzone/cda/pub/p/id/1387 at 20 April 2013


Smedinghoff T J, ‘Seven Key Legal Requirements for Creating Enforceable Electronic Transactions’ (2005) 9 (4) Journal on Internet Law 3


Smith L, ‘Online Shopping Experience’ (2005) 8(3) Internet Law Bulletin 44


Surdo A L, ‘Fraud and the Internet- the more things Change the more They Stay the Same’ (1999) 2(4) Internet Law Bulletin 51

Surveillance Self-defense https://ssd.eff.org/tech/mobile at 8 November 2013


Annual Conference, Academy of Legal Studies in Business National Proceedings, St Petersburg, Fla, 2006)


Wong E and Lawrence A, from Shrink to lick and Browse- Ensuring enforceability of Web terms’, (2004) 7(5) Internet Law Bulletin 61


TEXT BOOKS


Brown R A; *Documentary Evidence in Australia* (2nd ed, 1996)


Christou R, Drafting Commercial Agreements (3rd ed, 2005)

Christensen S. et al., ‘Land Contracts in Queensland’ (2nd ed, 2007)


Gemignani M, Law and the Computer (1981)


Nagamalai D, Advances in Parallel, Distributed Computing (2011) 514


Keller H, The codes of conduct and their Implementation: The Quest for Legitimacy in Rüdiger Wolfrum and Volker Röben, Legitimacy in International Law (2008)


Reed C, Computer Law (2nd ed, 1993)


Webster’s Dictionary (1988)


WEB SITES

Amazon.co.uk<http://www.amazon.co.uk/gp/help/customer/display.html/ref=footer_cou?ie=UTF8&nodeId=1040616> at 17 July 2012.

Australian Competition and Consumer Commission, ‘ACCC alleges VIPtel Mobile misled customers and acted unconscionably’<http://www.accc.gov.au/content/index.phtml/itemId/943152> (19 August 2010) at 1 November 2010


Business Services, 50% of teenagers buying age sensitive products online http://www.192business.com/news/50-percent-of-teenagers-buying-age-sensitive-goods-online at 12 July 2010


Contract and Consumer Law<http://austcontractlaw.wordpress.com> at 7 June 2010


Department for Business Innovations and Skills  


Ticket Master <www.ticketmaster.com.au> at 8 September 2007,


Senseng \(<\text{http://senseg.com/experience/senseg-experience}>\) at 22 March 2013

Shanghai Administrative Measure on Digital Certificates
<http://www.infosec.org/c/fanv/o2_03.htm> at 4 December 2007

Signature Initiatives \(<\text{http://www.ilpf.org/groups/survey.htm}>\) at 19 November 200

Slatterymedia\(<\text{http://www.slatterymedia.com/termsofuse/}>\) at 17 July 2012

Skype\(<\text{skype.com}>\) at 18 June 2013

States Legislation Table \(<\text{http://www.mbc.com/ecommerce/legislative.asp}>\) at 19 November 2006.

Swati, *Poor Age Verification Systems Allow kids to buy Knives, Alcohol, Adult DvDs Online!* http://devilsworkshop.org/poor-age-verification-system-allow-kids-to-buy-knives-alcohol-adult-dvds-online/ at 12 July 2010


The Internet Society (ISOC) <http://www.isoc.org/internet/history> at 20 July 2006


United Nations Conference on Trade and Development (UNCTAD), http://r0.unctad.org/ecommerce/ecommerce_en/faq_en.htm at 1 August 2006


United States Department of Justice, Identity Theft and Identity Fraud <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html> at 8 September 2007


Wales web design & Web Development Web Site and E commerce Maintenance <http://www.thomas-design.co.uk/website-maintenance.aspx> at 8 September 2009

Yahoo<www.yahoo.com> at 18 June 2013

Zhi Z, Online Sales to Minors Invalid Without Consent of Parents http://english.cri.cn/6909/2010/05/23/2321s571586.htm at 12 July 2010, 192

OFFICIAL REPORTS AND STATEMENTS


Asia Pacific Economic Cooperation (APEC), *Electronic Authentication: Issues related to its Section and Use*, 2002 p 34


EDI Association Standard Electronic Data Interchange Agreement, EDI Association of the United Kingdom (1990)


OECD, *Dismantling The Barriers to Global Electronic Commerce* DSTI/ICCP(98)13/FINAL (1997)


*Model Electronic Data Interchange Agreement and Commentary*, EDI Council of Australia (1990)

*Model Electronic Data Interchange Trading Partner Agreement and Commentary*, EDI Council of Canada (1990)

*Model Electronic Data Interchange Trading Partner Agreement and Commentary*, American Bar Association (1990)


Reed C, *Digital Information Law: Electronic Documents And Requirements of Form* Centre for Commercial Law Studies, Queen Mary and Westfield College, London (1996)


*Standard EDI Agreement*, New Zealand Electronic Data Interchange Association (1990),


INTERNATIONAL INSTRUMENTS


Draft Model Law on Electronic Data Interchange (EDI) and related means of communication, Compilation of Comments by Governments and International organizations, UNCITRAL (1995)


LEGISLATION

AUSTRALIA

*Competition and Consumer Act 2010 (Cth)*

*Conveyancing Act 1919 (NSW)*

*Conveyancing Law of Property Act 1884 (Tas)*

*Competition and Consumer Act 2010 (Cth)*

*De Facto Relationships Act 1991 (NT)*.

*Electronic Transactions Act (2001) (ACT)*

*Electronic Transactions Amendment Act (ACT) 2012*

*Electronic Transactions Act 1999 (Cth)*

*Electronic Transactions Amendment Act (Cth) 2011*

*Electronic Transactions Amendment Bill 2011*

*Electronic Transactions Act 2000 (NSW)*

*Electronic Transactions Amendment Act 2010 (NSW)*

*Electronic Transactions Act 2000 (NT)*

*Electronic Transactions Amendment Act (NT) 2011*

*Electronic Transactions Act 2001 (Qld)*

*Electronic Transactions Act 2000 (SA)*

*Electronic Transactions Amendment Act (SA) 2011*

*Electronic Transactions Act 2000 (Tas)*

*Electronic Transactions Amendment Act 2010 (Tas)*
Electronic Transactions Act 2000 (Vic)

Electronic Transactions (Victoria) Amendment Act 2011

Electronic Transactions Act 2003 (WA)

Electronic Transactions Amendment Act (WA) 2011,

Electronic Transactions Bill 1999 (Cth)

Electronic Transactions Bill 2000 (Vic)

Fair Trading Act 1999 (Vic)

Interpretation Act 1901 (Cth)

Interpretation Act 1915 (SA)

Interpretation Act 1931 (Tas)

Instruments Act 1958 (Vic)

Interpretation Act 1984 (WA)

Imperial Acts (Substituted Provisions) Act 1986 (ACT)

Law of property Act 1936 (SA)

Law of Property Act 2000 (NT).

Law Reforms (Miscellaneous Provisions) Act 1955 (ACT)

Law Reforms (Statute of Frauds) Act 1962 (WA)

Mercantile Law Act 1935 (Tas)

Model Transactions Amendment Bill 2010

Property law Act 1974 (Qld)

Statute of Frauds 1677 (Imp) (WA)

Trade Practices Act 1974 (Cth)

Trade Practices Amendment (Australian Consumer Bill) 2009 (Cth)

Trade Practices Amendment (Australian Consumer Bill) 2009 (Cth),

UNITED KINGDOM
Bills of Exchange Act 1882 (U.K)
Electronic Communications Act 2000 (U.K)
Electronic Communications Act 2000 (ECA)
Electronic Signatures Regulations 2002 (ESR)
Interpretation Act 1978 (U.K)
Law of Property Act 1925 (U.K)
Statute of frauds 1677 (UK)
Solicitors Act 1974 (U.K)

UNITED STATES OF AMERICA

California Government Code 1995
Electronic Signatures Global and National Commerce Act 2000 (US)
Electronic Commerce Security Act 1998
Massachusetts Electronic Records and Signature Act 1998
Uniform Commercial Code
Uniform Electronic Transactions Act 1999 (US)
Utah Digital Signature Act 1995

SINGAPORE

Electronic Transactions (Certification Authority) Regulations (Sing.), Revised Edition, 2001
Electronic Transactions Act (Sing.)1998
Electronic Transactions Act (Sing) 2010
Electronic Transactions Act (Sing.) Revised Edition 1999
Evidence Act (Sing.) Revised Edition 1997

Evidence (Computer Output) Regulations Evidence (Computer Output) Regulations (Sing.), Revised Ed.1997

GERMANY

German Civil Code (BGB)

German Code of Civil Procedure

German Digital Signature Act (DSA) 1997


OTHER COUNTRIES

Argentina Digital Signature Law, Presidential Decree No 427/98

Accounting Act 1977 of Norway

Belgian Civil Code

Malaysia Digital Signature Act 1997

Italian Law No 59, (enacted March 15 1997)

EUROPEAN COMMUNITY


TABLE OF CASES


American Express Australia Ltd v Michaels [2010] FMCA 103.

Australian Competition and Consumer Commission v Allphones Retail Pty Ltd [2009] FCA 17.

Australian Competition and Consumer Commission (ACCC) v Boost Tel Pty Ltd [2010] FCA 829; BC201005896

Australian Competition and Consumer v Clarion Marketing Pty Ltd [2009] FCA 1441; BC200911007.


ACCC v Jetplace Pty Ltd BC [2010] FCA,201005035

Australian Communication and Media Authority v Mobiligated Ltd a company Incorporated in Hong Kong and Others (2009) 256 ALR 85


Australian Competition and consumer commission v Teracomm Ltd [2009] FCA 903; BC200907523.

Adam v Lindsell (1818) 106 ER 250 at 251.


Asher v Seabrook [2008] FMCA 140.

Aristocrat Technologies Inc v IGT (2008) 80 IPR 413.


Australian Woollen Mills Pty Ltd v Commonwealth (1954) 92 CLR 424.

Aviet v Smith & Searls Pty Ltd (1956) 73 WN (NSW) 274.


Bajwa v Minister for Immigration and Anor [2008] FMCA 915.


Beswick v Beswick [1968] AC 58 at 72, 83.

Bhyat and Minister for Immigration and Multicultural and Indigenous Affairs [2003] AATA 1051.

Blackwell v Clark, Johnson (Tenancy) [2013] NSWCTTT 438 (26 August 2013)

Body Corporate and Community Management (Standard Module) Regulation 1997 Points North [2006] QBCCM 212.

Bowman v Durham Holdings Pty Ltd (1973) 131 CLR 8.


Brinkibon Ltd v Stahag Staht und Stahlwarenhandelsgesellschaft mbH [1983] 2 AC 34 at 41.

Brogden v Metropolitan Railway Co (1877) 2 App Cas 666 at 691.

Bundesverband v deutsche interent ECJ 08D266Oct.

Byrne & Co v Leon Van Teinhoven and Co (1880) 5 CPD 344.

Canton v Canton (1867) LR 2 HL, 127.

Carlill v Carbolic Smoke Ball Co. [1893] 1QB 256.

City Council Corneloup v Adelaide City Council [2010] SADC 144.

Caspi v Microsoft (1991) 323 NJ Super 118.


Chris Kobas v Electromagnetic Spectrum Pty Limited and Anor [2007] ACTSC 59


Cohen v Roche [1927] 1 KB 169.

Clohesy v Maher (1880) 6 VLR 357.

Cloud Corporation v Hasbro Inc., 314 F. 3d 289 (7th Cir. III 2002).


Corneloup v Adelaide City Council [2010] SADC 144.

Coulls v Bagot’s Executor and Trustee Co Ltd (1967) 119 CLR 460 (High Court).


Cundy v Lindsay (1878) 3 App Cas 459

Curtis v Singtel Optus Pty Ltd and Anor [2014] FCCA1286 (19 June 2014)


Dewhurst (WA) & Co Pty Ltd v Cawrse [1960] VR 278.


Dingle v Hare (1859) 7 CBNS 145; 141 ER 770.

Director of Public Prosecutions (DPP) v Malikovski [2010] VSCA 130.

Director of Public Prosecutions (DPP) v Kuru [2009] VSCA 206.


Douglas v United States District Court for the Central District of California 495 F.3d 1062 (9th Cir.2007).

Doughaiilli v Barua Pty Ltd [2006] NSWSC 1374.


Dunlop Pneumatic Tyre Co Ltd v Selfridge & Co Ltd [1915] AC 847.


Earl of Buckinghamshire v Drury (1762) 2 Eden 60; 28 ER 818.

eBay International AG v Creative Festival Entertainment Pty Ltd [2006] FCA 1768.

Electronic Rentals Pty Ltd v Anderson (1971) 124 CLR 27.

Elpis Maritime Co. Ltd v Marti Chartering Co. Inc., [1992] 1 AC 21, HL.

Entores Ltd v. Miles Far East Corporation (1955) 2 QB 327.

Eng and Org and Minister for Immigration and Multicultural and Indigenous Affairs [2004] AATA 76.

EPCO Carbon Dioxide Prods, Inc v JP Morgan Chase Bank, NA, 467 F.3d 466.

Esso Petroleum Ltd v Commissioners of Customs & Excise [1976] 1 All ER 117.

Evans v Hoare [1892] 1 QB 593; (1892) 66 LTRrep. NS, 345.

Express Airways v Port Augusta Air Services (1980) Qd R 543.

Farrelly v Hircock (No 1) [1971] Qd R 341 (not reported for 13 years) at 356.


Ford v La Forrest [2001] QSC 261.

Ford v La Forrest [2001] QCA 455.


George Hudson Holdings Ltd v Rudder (1973) 128 CLR 387.


Great Britain v Boots Cash Chemists (Southern) Ltd [1953] 1 QB 401.


Hall v Cognos Ltd (Industrial Tribunal Case No. 1803325/97).


Harding v Brisbane City Council & Ors [2009] QPELR 207.


Hayek v R [2010] NSWCCA 139.


Hill and Anor v W and F Lechner Pty Ltd [2006] NSWSC 440.

Hill v Gateway 2000 Inc., 105 F 3d 1147, 1150 (7th Cir.1997).

Hood v Anchor Line (Henderson Bros) Ltd [1918] AC 837 at 846.


Hucklesby v Hook (1900) 82LT 117.

Hyde v Wrench (1840) 3 Beav 334; 49 ER 132.

Hlich & Anor and Baystar Corporation Pty Ltd [2004] WASTR 25.


Imperial Brothers Pty Ltd v Ronim Pty Ltd [1999] 2Qd R 172


Ingam v Little [ 1961] 1 QB 31


Joyce v Gee [2010] WASC 76.

Ker-Optika bt v ANTSZ Del-dunantuli Regionalis Intezete Court of Justice of the European Union (Third Chamber) [2011] All ER (D) 14 Jan; C-108/09.


Kings Norton Metal Co Ltd v Edridge, Merrett and Co Ltd (1897) 14 TLR 98


Koompahtoo Local Aboriginal Land Council v Klalc Property and Investment Pty Ltd and Anor (No2) [2006] NSWSC 169.


Latec Finance Pty Ltd v Knight [1969] 2 NSW 79.


Lazarus Estates Ltd v Beasley [1956] 1 All ER 341.

Lake v Simmons [ 1927] AC 487

Lewis v Averay [1972] 1 QB 198

Lickbarrow v Mason (1787) 2 Temp.rep.63 at 70
Leach Nominees Pty Ltd v Walter Wright Pty Ltd [1986] WAR 244.


Le Mans Grant Prix circuits Pty Ltd v LLiadis (1998) 4 VR 649.

Leeman v Stocks [1951] 1 Ch 941 at 947-948.

Lobb v. Stanley (1844) 5 Q.B. 574; 114 ER 1366.


Liu and Ors v Minister for Immigration and Anor [2013] FCCA 2208 (9 December 2013)


MacRobertson Miller Airline Services v Commissioner of State Taxation (WA) (9175) 133 CLR 125 at 136.


Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson Case No.1:2008cv07833, September 8, 2008, New York Southern District Court.

Macquarie Group Ltd, Macquarie Bank Ltd and Macquarie Holdings (USA) Inc v Peter Martenson, Case No.3: 2009cv00093.


Menzies v Williams (1893) 10 WN (NSW) 13.


NM Superannation Pty Ltd v Baker [1927] ACSR 105 at 114-115.


Nunin Holdings Pty Ltd v Tullamarine Estates Pty Ltd [1994] 1 VR 74.


Olley v Marlborough Court (1949) 1 KB 532.

Optika bt v ANTSZ Del-dunantuli Regionalis Intezete Court of Justice of the European Union (Third Chamber) [2011] All ER (D) 14 Jan; C-108/09.

Partridge v Crittenden [1968] 2 All ER 421.

Patterson v Dolman [1908] VLR 354.

Panavision International LP v Toeppen 97/55467.

Payne v Cave (1789) 3 TR 148;100ER 502.


Pharmaceutical Society (GB) v Boots Cash Chemists (Southern) Ltd [1953] 1 QB 401.

Phillips v Brooks [1919] 2 KB 243


Powell v City of Newton, 703 S.E. 2d 723, 2010 N.C. LEXIS 1078.

Price v Easton (1833) 4 B & Ad 433.


Porter v Lactec Finance (Qld) Pty Ltd (1964) 111 CLR 177.

Quenerduaine v Cole (1883) 32 WR 185.


R v Frolchenko (1998) QCA 34.

R v Harris [2009] VSCA 189.


R Leslie Ltd v Sheill (1914) 3 KB 607 at 618.

R v Mann [2009] VSC 536.

R v Moore: Ex Parte Myers (1884) 10 VLR 322.

R (on the application of Software Solutions Partners Ltd) v Revenue and Customs Commissioners [2007] EWHC 971.


Register.com, Inc. v Verio, Inc.356 F.3d 393 (2d Cir.2004).

Re a Debtor (No 2021 of 1995) [1996] 2 All ER 345.

Re David Scott Ellis; Ex Parte Triple M Mechanical Services Pty Ltd [ No 2] [ 2013] WASC 161 ( 2 May 2013)

Re Imperial Land Co of Marseilles (Townsend’s case) (1871) LR 13 Eq 148.


Re Mount Tomah Blue Metals Ltd (in liquidation) [1963] ALR 436.
Re RealNetworks, Inc Privacy Litigation 2000 US Dist LEXIS 6584.

Re Ryan and Secretary, Department of Employment and Workplace Relations (2005) 90 ADL 800.

Re Ross Frank Finlayson and Migration Agents Registration Authority [2005] AATA 1127.

Reese Bros Plastics Ltd v Hamon-Sobelco (Australia) Pty Ltd (1988) 5 BPR 97325 (Court of Appeal, New South Wales).

Reed Constructions Pty Ltd v Eire Constructions Pty Ltd [2009] NSWSC 678.


Rock Solid Surfaces Pty Ltd v Biesse Group (Australia) Pty Ltd [2011] FCA 42.


Saunderson v Jackson (1800) 2 Bos & Pul 238; 126 ER 1257.

Schneider v Norris (1814) 2 M & S 237; 105 ER 388.


Stocks v Wilson (1913) 2 KB 235.


Shah v Minister for Immigration & Anor [2011] FMCA 18

Southdown Publication Pty Ltd v ACP Magazine PTY Ltd (2003) 60 IPR 367

Shogum Finance Ltd v Hudson [2003] UKHL 62


Smilie Pty Ltd v Bruce (‘Smilie’) [1998] 8 BPR

Spencer v Harding (1870) LR 5 CP 561.

Specht v Netscape Communications Corp. 306 F.3d at 17 (2d Cir.2002).


South Australian Railways Commissioner v Egan (1973) 130 CLR 506.


Sutton v Tatham (1839) 10 Ad and El 27 at 30; 113 ER 11 at 12.


SZSKX v Minister for Immigration and Anor [ 2014] FCCA 157 (4 April 2014)

SZAEG & ORS v Minister For immigration [2003] FMCA 258.


Tallerman and Co Pty Ltd v Nathan’s Merchandise (Vic) Pty Ltd (1957) 98 CLR 93.


Taylor v Johnson (1983) 151 CLR 422B

Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes) [1974] 3 All ER 88.


Tenas Steamship Co Ltd v Owners of the Motor Vessel ‘Brimnes’ (The Brimnes) [1975] QB 928

Thornton v Shoe Lane Parking Ltd [1971] 2 QB 163.

Thorn Airfield Lighting Pty Ltd v W (2012) TASWRC 11 (5 April 2012)


Tinn v Hoffman & Co (1873) 29 LT 271.


Toys ‘r’ Us inc. v Akhaouni (1996) 40 USPQ 2d 1836.


Tugum Cobaki Alliance Inc v Minister for planning and RTA [2006] NSWLEC 396.

Tweddle v Atkinson (1861) 121 ER 762.


Vassallo v Haddad Impor and Export Pty Ltd (2004) 2 DCLR (NSW) 123


Viditz v O’Hagan [1900] 2 Ch 87.

Vincent B Blake v Murphy Oil USA, INC 2010 U.S. Dist. LEXIS 95847.

WGOC and GH and Anor [2006] FamCA 539.

White Trucks Pty Ltd v Riley (1948) 66 WN (NSW) 101.


Wilkie v London Passenger Transport Board [1947] 1 All ER 258 at 259.

William Close Pty Ltd v City of Salisbury & Anor (No 2) [2012] SAERDC 26 (3 May 2012)


Zouchd Abbot & Hallet v Parsons (1765) 3 Burr 1794; 97 ER 1103.