

**A Cyber-Consumer Protection Framework for Prevention of
Online Deceptive Advertising**

Mr. Ahmad Aladwan

This thesis is presented for the Degree of
Doctor of Philosophy
of
Curtin University

June 2012

Thesis Abstract

Online deceptive advertisements engender distrust among cyber-consumers, leaving many negative physical and emotional effects and financial losses; we find that such incidents occur in every country in the world. This research addressed issues with online fraud and deceptive advertising related to cyber-consumer transactions (CCT) and consumer protection, whether local or international. The focus of this study was to propose a means of protecting the cyber-consumer from online fraud and deceptive advertising before and after losses through the Cyber Consumer Protection Framework (the framework) developed from this thesis. This framework provides potential solutions and redress methods in order to minimise online fraud and deception as well as protecting the cyber-consumer when making an online transaction whether locally or internationally. The framework offers a set of redress methods and approaches to prevent online fraudulent behaviour to protect cyber-consumers. This framework is developed based on the analysis of cognitive processes and the behavioural studies of advertisers and consumers. These provide a foundation for examining how advertisements provide information that attracts consumers and how consumers interpret advertised messages. We then determine the characteristics of advertisements for products or brands, and then provide guidelines about the advertising qualities and how these exhibit significant differences in their impact on consumer behaviour. The research has provided a tool for consumers to analyse the advertiser's interests and to pin-point fraudulent or embedded hidden agenda. The outcome of this thesis is a proposed cyber-consumer protection framework which incorporates a set of approaches for the protection of cyber-consumers. These approaches include an online federated consumer protection portal with strengthened crime detection features, updated consumer protection policies, law

enforcement methods for the cyber environment to deal with online deceptive advertising and cyber crimes, thereby helping the consumer to prevent losses and possibly recover damages.

This thesis gives a clear explanation of ‘deceptive advertising’ and provides detailed examples to illustrate its impact on consumers. We provide cognitive processes analysis and behavioural studies, and provide a Cyber Consumer Protection Framework to prevent deceptive advertising. Much existing work to date has provided some guidelines for consumers on what not to do. However, deceptive advertising and fraudulent activities continue to intensify due to the fact that there are no strong cyber-based legal frameworks for making vendors accountable for fraudulent and deceptive online activities. In Australia, we found that the legislation for consumer protection is not detailed enough to protect the cyber-consumer. Further, local policies such as those of the Australian Competition and Consumer Commission (ACCC) have no guidelines on how to deal with online fraud that involves fraud from other jurisdictions, because the jurisdiction for policies are only ‘local’, not international or across states. These weaknesses have encouraged more and more fraud and deception in products and services as well as misleading information in the online market. Therefore, this thesis also proposes solutions for cyber-consumers in terms of what they can do after being deceived, how to avoid being deceived, and how to deal with false and misleading advertisements through our Cyber Consumer Protection Framework and approaches to prevent financial losses and psychological harm.

Table of Contents

THESIS ABSTRACT.....	II
TABLE OF CONTENTS	IV
LIST OF TABLES.....	XII
STATEMENT OF AUTHORSHIP	XV
LIST OF ABBREVIATIONS	XVI
ACKNOWLEDGEMENTS	XVIII
CHAPTER ONE THESIS INTRODUCTION.....	1
1.1 INTRODUCTION	1
1.2 DEFINITIONS	2
1.2.1 ONLINE FRAUD.....	2
1.2.2 ONLINE DECEPTIVE ADVERTISING.....	2
1.2.3 CYBER-CONSUMER BEHAVIOUR	2
1.2.4 FOREIGN VENDOR	3
1.2.5 CYBER-CONSUMER TRANSACTION	3
1.2.6 REDRESS	4
1.2.7 EFFECTIVENESS	4
1.3 THE RESEARCH PROBLEM	5
1.4 MOTIVATION OF THE STUDY	9
1.5 THESIS OBJECTIVES	10
1.6 THESIS PLAN.....	11
1.7 CONCLUSION.....	13
CHAPTER TWO THEORETICAL BACKGROUND AND LITERATURE REVIEW.....	15

2.1	INTRODUCTION	15
2.2	HISTORY OF DECEPTIVE ADVERTISING.....	16
2.3	COGNITIVE APPROACH TO DECEPTIVE ADVERTISING	17
2.4	THE APPROACH OF THE FEDERAL TRADE COMMISSION	20
2.5	AUSTRALIAN CONSUMER PROTECTION LAW	22
2.6	REGULATION OF BUSINESS TO BUSINESS AND BUSINESS TO CONSUMER TRANSACTIONS	26
2.7	CONTRACT LAW	28
2.8	PRIVATE INTERNATIONAL LAW	29
2.9	CYBER CRIME LAW	34
2.10	E-COMMERCE AND TECHNOLOGY APPROACH	37
2.11	ONLINE LAWYERS	37
2.12	ONLINE PUBLIC CONSUMER PROTECTION AUTHORITIES	41
2.13	ALTERNATIVE DISPUTE RESOLUTION AND ONLINE DISPUTE RESOLUTION	45
2.14	ARBITRATION	56
2.15	INDUSTRY-BASED CONSUMER DISPUTE RESOLUTION SCHEMES	59
2.16	CODES OF CONDUCT	61
2.17	ESCROW SERVICES	64
2.18	THE UNITED NATIONS GUIDELINES	66
2.19	THE ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT GUIDELINES	70
2.20	THE EUROPEAN MODELS.....	75
2.21	UNITED STATES LAW.....	76

2.22 CONCLUSION.....	79
CHAPTER 3 RESEARCH ISSUES: ADVERTISING DECEPTION	81
3.1 INTRODUCTION	81
3.2 THE EFFECTS OF DECEPTIVE ADVERTISING ON PURCHASING DECISIONS: INTERPRETATION OF THE LEGAL DIMENSION.....	82
3.3 THE EFFECTS OF DECEPTIVE ADVERTISING ON PURCHASING DECISIONS: INTERPRETATION OF THE BEHAVIOURAL DIMENSION.....	85
3.4 THE EFFECTS OF DECEPTIVE ADVERTISING ON PURCHASING DECISIONS	88
3.5 CONCLUSION.....	92
CHAPTER FOUR CONCEPTUAL FRAMEWORK.....	93
4.1 INTRODUCTION	93
4.2 DECEPTIVE ADVERTISING.....	94
4.3 CYBER LEGISLATION AND CYBER-CONSUMER PROTECTION	96
4.4 LAWS FOR FEDERATED CYBER-CONSUMER PROTECTION	96
4.5 CYBER-CONSUMER COGNITIVE PROCESS AND BEHAVIOUR ANALYSIS.....	97
4.6 CYBER SOLUTIONS FOR CYBER-CONSUMER PROTECTION	97
4.7 CONCEPTUAL OVERVIEW OF THE CYBER CONSUMER PROTECTION FRAMEWORK FOR THE PREVENTION OF DECEPTIVE ADVERTISING	99
4.8 CONCLUSION.....	102
CHAPTER 5 CONCEPTUAL DEFINITION OF ONLINE DECEPTIVE ADVERTISING AND CYBER CONSUMER PROTECTION	103
5.1 INTRODUCTION	103
5.2 DEFINING DECEPTIVE ADVERTISING.....	104

5.3 ASPECTS OF DECEPTIVE ADVERTISING	105
5.3.1 FIRST DEFINITION.....	105
5.3.2 SECOND DEFINITION.....	105
5.3.3 THIRD DEFINITION	105
5.3.4 FOURTH DEFINITION.....	106
5.4 AUSTRALIAN COMPETITION AND CONSUMER COMMISSION METHODOLOGY	107
5.5 INDICATIONS OF DECEPTIVE ADVERTISING	108
SIGNIFYING INDICATORS.....	109
5.7 THE EFFECTS OF DECEPTIVE ADVERTISING ON PURCHASING DECISIONS	115
5.8 ONLINE DECEPTIVE ADVERTISING.....	116
5.9 COMMON STRATEGIES FOR ONLINE ADVERTISING.....	117
5.9.1 BANNER ADS.....	117
5.9.2 ONLINE VIDEO ADVERTISEMENTS	118
5.9.3 POP-UP ADS.....	119
5.10 DECEIVING ADVERTISERS	120
5.10.1 BAIT AND SWITCH SCHEMES	121
5.10.2 BLATANT DECEPTIVE ADVERTISING.....	125
5.11 CYBER-CONSUMER	127
5.12 FORMS OF ONLINE FRAUD OR DECEPTION.....	128
5.13 DEFINING DECEPTIVE ADVERTISING.....	130
5.13.1 DEFINING DECEPTIVE ADVERTISING: THE LEGAL DIMENSION	130
5.13.2 THE DEFINITION OF THE FEDERAL TRADE COMMISSION	130
5.14 CONCLUSION.....	132
CHAPTER 6 NEW CYBER LEGISLATION: LIBERTARIANISM VERSUS INTERVENTIONISM	134

6.1	INTRODUCTION	134
6.2	CONSUMERS	136
6.3	CYBER-CONSUMER PROTECTION.....	137
6.4	LIBERTARIANISM AND INTERVENTIONISM	142
6.4.1	LIBERTARIANISM	142
6.4.2	INTERVENTIONISM	142
6.4.3	COMMON GROUND BETWEEN LIBERTARIANISM AND INTERVENTIONISM.....	143
6.5	LIBERTARIANISM VERSUS INTERVENTIONISM IN CYBERSPACE.....	145
6.6	CONCLUSION.....	154
CHAPTER SEVEN EXTENSION OF LAW FOR FEDERATED CYBER-CONSUMER PROTECTION ..		157
7.1	INTRODUCTION	157
7.2	THE EXISTING BODY OF LAW	157
7.2.1	CONSUMER-PROTECTION LAW	157
7.2.2	CONTRACT LAW	157
7.2.3	PRIVATE INTERNATIONAL LAW	157
7.3	POTENTIAL SOLUTIONS AND REDRESS: CURRENT METHODS	158
7.4	DIFFICULTIES WITH CURRENT LEGISLATION.....	161
7.4.1	FEDERATION PROTECTION WITH ENFORCEMENT	161
7.4.2	FEDERATION TO ADDRESS COMPLEXITY.....	162
7.5	CONCLUSION.....	163
CHAPTER EIGHT INTERNATIONAL COOPERATION FOR CYBER CONSUMER PROTECTION....		165
8.1	INTRODUCTION	165
8.2	AUSTRALIAN INTERNATIONAL COOPERATION	169

8.3	UNITED NATIONS COOPERATION	171
8.4	OECD COOPERATION	175
8.5	EUROPEAN COOPERATION	180
8.6	UNITED STATES COOPERATION.....	181
8.7	CONCLUSION.....	184
CHAPTER NINE CYBER-CONSUMER COGNITIVE PROCESS AND BEHAVIOUR ANALYSIS.....		187
9.1	INTRODUCTION.....	187
9.2	THE SUGGESTED FRAMEWORK FOR THE DETERMINANTS OF ONLINE DECEPTIVE ADVERTISING	188
9.2.1	RECOGNISING (EXPOSURE).....	188
9.2.2	ATTENTION	190
9.2.3	COMPREHENSION AND PRIOR KNOWLEDGE	193
9.2.4	INVOLVEMENT	196
9.2.5	BELIEFS	203
9.3	CYBER-CONSUMER PROTECTION INSPIRED COGNITIVE PROCESS	207
9.3.1	ONLINE FOREIGN LAWYERS	207
9.3.2	ONLINE FOREIGN PUBLIC CONSUMER PROTECTION AUTHORITIES.....	208
9.3.3	ARBITRATION	208
9.3.4	ONLINE INDUSTRY-BASED CONSUMER DISPUTE RESOLUTION SCHEMES	208
9.3.5	INDUSTRY CODES OF CONDUCT	208
9.3.6	ESCROW SERVICES	208
9.3.7	ONLINE TRANSACTION INSURANCE.....	209
9.3.8	TRUSTMARK	209
9.3.9	CONSUMER EDUCATION PROGRAMS.....	209
9.3.10	CYBER-CONSUMER COMPLAINTS BULLETIN BOARDS	209
9.3.11	NATIONAL DEREGISTRATION	209

9.4 CONCLUSION.....	210
CHAPTER TEN NEW CYBER SOLUTIONS TO PREVENT LOSSES, FINANCIAL DAMAGES AND PSYCHOLOGICAL HARM TO CYBER-CONSUMERS 212	
10.1 INTRODUCTION	212
10.2 POTENTIAL CYBER SOLUTIONS	213
10.2.1 ONLINE TRANSACTION INSURANCE TO SUPPORT LOSS RECOVERY.....	214
10.2.1.1 DESCRIPTION	214
10.2.1.2 ASSESSMENT.....	215
10.2.1.3 CONCLUSION.....	215
10.2.2 TRUSTMARKS TO PREVENT CYBER LOSSES	216
10.2.1.1 DESCRIPTION	216
10.2.1.2 ASSESSMENT.....	218
10.2.1.3 CONCLUSION.....	219
10.2.3 CONSUMER EDUCATION PROGRAMS TO PREVENT DECEPTION	220
10.2.3.1 DESCRIPTION	220
10.2.3.2 ASSESSMENT.....	221
10.2.3.3 CONCLUSION.....	221
10.2.4 CYBER-CONSUMER COMPLAINTS BULLETIN BOARDS	222
10.2.4.1 DESCRIPTION	222
10.2.4.2 ASSESSMENT.....	223
10.2.4.3 CONCLUSION.....	224
10.2.5 NATIONAL DEREGISTRATION FOR FRAUDULENT BEHAVIOUR	225
10.2.5.1 DESCRIPTION	225
10.2.5.2 ASSESSMENT.....	225
10.2.5.3 CONCLUSION.....	226
10.3 CONCLUSION.....	227

CHAPTER ELEVEN EVALUATION OF THE PROPOSED CYBER-CONSUMER PROTECTION FRAMEWORK	231
11.1 INTRODUCTION	231
11.2 IDENTIFYING DECEPTIVE ADVERTISING: A BEHAVIOURAL PERSPECTIVE.....	231
11.3 IDENTIFYING DECEPTIVE ADVERTISING: THE LEGAL PERSPECTIVE	236
11.3.1 AFFIRMATIVE DISCLOSURE	236
11.3.2 CORRECTIVE ADVERTISING.....	237
11.4 MEASURING DECEPTIVE ADVERTISING.....	240
11.4.1 MEASURING DECEPTIVE ADVERTISING: THE LEGAL DIMENSION	240
11.4.2 MEASURING ADVERTISING DECEPTION: THE BEHAVIOURAL DIMENSION	243
11.5 DETERMINING ADVERTISING EFFECTIVENESS AND DECEPTIVE ADVERTISING	245
11.6 THE FRAMEWORK EVALUATION SUMMARY.....	249
11.7 CONCLUSION.....	249
CHAPTER TWELVE ENCAPSULATION AND FUTURE WORK.....	251
12.1 INTRODUCTION	251
12.2 THE IMPACT OF THE RESEARCH	251
12.3 ENCAPSULATION	254
12.4 OVERALL CONCLUSION	259
REFERENCES	263

List of Tables

Table 2.1 Online/foreign lawyers.....	41
Table 2.2 Online foreign public consumer protection authorities.....	45
Table 2.3 Alternative dispute resolution/online dispute resolution.....	56
Table 2.4 Arbitration	59
Table 2.5 Industry-based consumer dispute resolution schemes.....	60
Table 2.6 Industry codes of conduct.....	63
Table 2.7 Escrow services.....	66
Table 7.1 Potential cyber-consumer protection solutions and evaluation of redress methods	160
Table 7.1.1 Litigation: redress under current legal regime	160
Table 7.1.2 Redress methods.....	160
Table 7.1.3 Potential solutions	161
Table 9.1 The affective span of the cognitive process in recognising deceptive advertising	196
Table 9.2 The affective span of the involvement process in recognising deceptive advertising	202
Table 10.1 Online transaction insurance	216

Table 10.2 Trustmarks	220
Table 10.3 Consumer education	222
Table 10.4 Consumer complaints bulletin boards	225
Table 10.5 National deregistration	227
Table 10.6 Evaluation of cyber-consumer protection and CCT redress methods.....	228
Table 11.1 Summary of definitions of deceptive advertising	235
Table 11.2 The relationship between a false advertisement and a deceptive advertisement	242
Table 12.1 Evaluation of cyber-consumer transaction redress methods	260
Table 12.1.1 Current redress methods.....	260
Table 12.1.2 Potential solutions and redresses for cyber-consumer protection	260

List of Figures

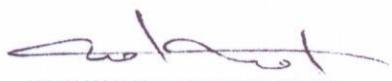
Figure 3.1 Influence of deceptive advertising on consumer purchasing decisions	89
Figure 3.2 Conceptual framework.....	100
Figure 3.3 Overview of the conceptual proposal of Cyber Consumer Protection Framework for preventing deceptive advertising	101
Figure 5.1 Influences of deceptive advertising on consumers' purchasing decisions	116
Figure 9.1 The affective span of the process of exposure to the ad in recognising the deceptive message.....	189
Figure 9.2 The affective span of the attention process in recognising deceptive advertising	193
Figure 9.3 The framework of the consumer's involvement with the product.....	198
Figure 9.4 The affective span of beliefs in recognising deceptive advertising.....	206
Figure 11.1 The steps of assessing advertisement claims using legal trends	239
Figure 11.2 Normative belief technique.....	244
Figure 11.3 The ad's effectiveness and relationship to DA	248

Statement of Authorship

Except where reference is made in the text of the thesis, this thesis contains no material published elsewhere or extracted in whole or in part from a thesis submitted for the award of any other degree or diploma

No other person's work has been used without acknowledgment in the main text of the thesis.

This thesis has not been submitted for the award of any degree or diploma in any other tertiary institution.



Mr Ahmad Aladwan

Date 17/12/2012

List of Abbreviations

CCT	– cyber-consumer transaction
ACCC	– Australian Competition and Consumer Commission
ADR	– alternative dispute resolution
APEC	– Asia-Pacific Economic Cooperation
B2B	– business to business
B2C	– business to consumer
CCT	– cyber-consumer transaction
CISG	– Convention for the International Sale of Goods
DA	– deceptive advertising
EU	– European Union
FTC	– Federal Trade Commission
ICANN	– Internet Corporation for Assigned Names and Numbers
ICPEN	– International Consumer Protection and Enforcement Protection Network
ICT	– international consumer transaction
IS	– Internet Service Provider
ODR	– Online Dispute Resolution
OECD	– Organization for Economic Cooperation and Development
OEEC	– Organization for European Economic Cooperation

UDRP – Uniform Dispute Resolution Policy

UK – United Kingdom

UN – United Nations

US – United States of America

Acknowledgements

This thesis is the end of my PhD journey, and I have not travelled alone. This thesis has been kept on track and been seen through to completion with the love, support and encouragement of special people including my advisors and my family.

It is a pleasure and honour to express my gratitude to all who contributed in their different ways to the success of this study and helped make it an unforgettable and memorable experience for me.

First and foremost I am gratefully honoured to acknowledge my supervisors: Deputy Vice-Chancellor Professor David Wood, Professor Elizabeth Chang and Professor Dora Marinova, for their guidance and support from the beginning of my Candidacy Proposal and Presentation to the day I happily submitted my research. I am grateful for their suggestions and guidance which kept me focused and motivated to overcome all the struggles and challenges during the writing of my thesis. Without their courage and inspiration, I would have not reached the end of my journey successfully.

I also take this opportunity to sincerely thank Dr Farookh Hussain and Dr Omar Hussain for their great support, kindness and help when needed. Both had their doors open for me in times of need and offered an enormous amount of genuine advice and help.

I am also extremely indebted to my dearest loving and caring brother Dr Khalid Aladwan, for the loving, caring and tender support he provided my family and me during his stay with us. Despite the complications and struggles he had during his own PhD studies, he still managed to be there and lend his helping hand in times of hardship and give all he had with warm love and

care to my family and with his sense of humour he turned dull grey days into days full of brightness and joy. I would also like to take this opportunity to proudly congratulate him on his success and completion of his PhD degree with Charles Sturt University.

Last, but not least, and most importantly, this thesis would not have been successfully accomplished without the prayers and the good wishes and heart-warming support of the dearest and most precious people God has gifted and blessed me with.

I am forever indebted and from the bottom of my heart deeply appreciative to my family, firstly my hard working and honourable father Mr Mahmoud Aladwan for his never ending support and encouragement. His strong belief in me filled my heart, body and soul with immeasurable strength to stay positive and persist. I also owe all my thanks to the sunshine of my life, my priceless jewel, my dearest mother Mrs Aladwan for her boundless love and care. She put all her belief and trust in me and along with her warm touching words she gave me strength and guided me with her eyes throughout this long journey. I can't thank both my father and mother enough for all they have sacrificed to smooth my pathway.

I am forever grateful to my loving and caring brothers, Dr Yasser Aladwan, Dr Khalid Aladwan, Sergeant Omar Aladwan and Mr Raed Aladwan for their support and encouragement. I am also very much appreciative for the love and tenderness my beautiful sisters provided me with during my journey.

My thanks don't end here. My acknowledgements would not be complete without my warmest and explicit thanks to my loving and caring wife Carolyn Aladwan, my two lovely boys Omar and Mohammed Aladwan and of course my beautiful baby daughter Shahed Aladwan. I am very

grateful for their trust and belief in me. Their patience, support and encouragement are what truly kept me motivated towards completing this thesis.

*Finally I dedicate this thesis and all my hard work to
my family, my lovely wife Carolyn and my beloved children
for their constant support and unconditional love.*

I love you all dearly

CHAPTER ONE

THESIS INTRODUCTION

1.1 Introduction

This thesis is concerned with online fraud deceptive advertising (DA) and cyber-consumer transactions (CCT) with a foreign vendor via the Internet or otherwise, and whether the consumer has any effective means of redress in the event of deceptive/fraudulent behaviour by the vendor in relation to standard CCT contracts. ‘Standard’ contracts here are those concluded directly between vendor and consumer (i.e. not involving third party intermediaries such as eBay) and not involving exceptional circumstances. The focus is on the vendor performing online fraudulent or deceptive behaviour in order to attract the cyber-consumer. Thus, this thesis relates to unsatisfied deceived customers and CCT issues.

Although this thesis focuses on international law to an extent, specifically consumer international law, most of the resources utilised are from an Australian perspective. That is, while the thesis is not preoccupied solely with Australian consumer parties to CCTs, Australian law is the starting point for most of the research approach. This limits the scope of the thesis to illustrating, by comparison, the problem facing consumer parties to CCTs in other jurisdictions, and avoids the need to look at the details of consumer laws of multiple jurisdictions. The only exceptions to this limitation are brief considerations of the positions of United States of America (US) and European Union (EU) consumers. This is done where the laws and practices of comparable non-Australian jurisdictions appear to offer significant advantages to Australian cyber-consumers. Therefore, in this chapter we briefly define the

major themes and explain the problem of the research. Also, in this chapter we explain the objectives and the plan of the research.

1.2 Definitions

1.2.1 Online fraud

‘Online fraud’ in this thesis is defined as a deliberate misrepresentation that causes an online consumer to suffer monetary losses. Both deliberateness and consumer suffering are usually required for an act to be considered fraud; for example, it would not be fraud unless in doing so, the scammer caused someone else to sustain financial losses or damages. Online fraud occurs when the scammer acts as a legitimate vendor or organisation in order to obtain personal information (identity theft) and make illegal transactions using the consumer’s account. This type of fraud may also be referred to as phishing scams.

1.2.2 Online deceptive advertising

‘Online DA’ in this thesis is defined as a form of online advertising practised by online vendors or advertisers using deceptive tactics to lead to a larger mailing list or purchases for the advertiser. Online DA, also referred to as online false advertising, is the practice of making untrue claims or statements about a product or service. Though not always illegal, DA often goes beyond the boundaries of moral and ethical behaviour.

1.2.3 Cyber-consumer behaviour

‘Cyber-consumer behaviour’ in this thesis refers to an online purchase, whether international or local. Cyber-consumer behaviour is the process of online shopping from a consumer’s perspective. The field of cyber-consumer behaviour can be broad. In many respects, the study

of cyber-consumer behaviour is the study of the interaction between the cyber-consumer and the online vendor. Cyber-consumer behaviour theories tend to concentrate on how consumers make decisions to reach the highest level of satisfaction, how consumers consider the utilities and features of different products, or what and how much consumers know about particular products. Therefore, different types of cyber-consumer behaviour theories tend to focus on the choices consumers make based on prior knowledge and level of understanding of the advertisement message.

1.2.4 Foreign vendor

A ‘foreign vendor’, in this thesis, is one not in the same country as the consumer; neither party is necessarily in any particular country.

1.2.5 Cyber-consumer transaction

A “consumer transaction” is a transaction involving the purchase of goods for a price of up to AUD\$50,000—this thesis is concerned only with redress available to consumers engaging in transactions for less than this amount. This amount is similar to the upper limit found in Australian consumer protection legislation (AUD\$40,000—higher if the goods are acquired for non-commercial purposes) introduced in 1986 (the *Trade Practices Act 1974* (Cwlth)). The figure of AUD\$50,000 provides a practical upper monetary limit with which to compare potential expenses to be incurred when seeking a remedy for a disputed or failed CCT. It also acknowledges that quite substantial sums of money can be lost in connection with disputed or failed CCTs. The failure by a consumer to take precautions before entering into higher value CCTs (assuming that is at all possible; see the section on online transaction insurance in Chapter Nine) for example, does not preclude him/her from seeking post-transaction remedies, through the courts or by other means since it is not an offence at law to fail to protect oneself.

1.2.6 Redress

‘Redress’ means any reasonable method by which a consumer who is an aggrieved party to a CCT could justifiably seek a remedy from an uncooperative vendor for any online fraudulent behaviour or online deception. Redress is specifically of concern in this thesis, as opposed to the wider but related issue of cyber-consumer protection. ‘Cyber consumer protection’ is a broader concept and covers issues of regulation of the bargaining phase and of contract terms as well as access to justice issues. Thus, although redress and protection are related, they are not the same. For example, if there is greater ‘protection’ through the legislative imposition of uniform and implied terms, then arguably there will be fewer disputes and dispute resolution will be less costly because there will be no need for arguments over private international law rules regarding applicable law.

Therefore there is a strong argument that issues of effective redress for CCTs should not be considered in isolation from the broader issues of cyber-consumer protection law for CCTs. This link between redress and protection is the context for later discussion of issues (especially in Chapter Ten) concerning cyber-consumer protection law for CCTs.

1.2.7 Effectiveness

‘Effectiveness’ is the ultimate criterion used for the assessment of the redress methods, actual and potential, examined in this thesis: can a genuinely aggrieved consumer obtain effective redress in connection with a failed or disputed CCT using the method contemplated? In this thesis, effectiveness is evaluated in terms of ‘difficulty of enforcement’ and ‘complexity’. The basis of and justification for this choice of criteria is discussed in Chapter Ten.

1.3 The research problem

The Internet has contributed to the emergence of a world market far larger than any single national market. Consumers generally stand to directly benefit from this global market because they now have access to a wider variety of goods, perhaps more competitive prices through increased competition, a greater choice of suppliers, the ability to shop from home (particularly beneficial for those in geographically-remote areas), the ability to shop at any time, and the ability to conclude transactions at greater speed.

Consumers also benefit indirectly from the ability of vendors to reduce the cost of finding customers and suppliers, expand their trading areas from local to global, reduce the time it takes to purchase and receive goods, pay for and receive goods as they are needed without having to rely on large inventories, and reduce or even eliminate the cost of creating documents and other printed materials. Such reductions in costs are frequently passed on to the consumer by way of cheaper prices, and customer service is enhanced with faster response times (Alexander, 1997).

While there are benefits for consumers undertaking online shopping, whether local or international, consumers are facing a greater problem causing them financial losses and other damages of all kinds due to their exposure to online fraudulent behaviour and online deception, specifically ‘advertising’.

Surprisingly then, use of the Internet to purchase goods is increasing. According to Australian Government data, ‘on average, approximately one million Australians aged 14 years and over made a purchase online in any given week of 2002–03. This represented an increase of 85 per cent since 2000–01’ (Australian Government Treasury, 2005). It was predicted that business to consumer e-commerce would add 2.7 per cent to Australia’s GDP by 2007

(Smith, 2004) on the basis of an Australian Competition and Consumer Commission (ACCC) report of May 2000 (ACCC, 2003).

This is consistent with international trends. According to the Organization for Economic Cooperation and Development (OECD) data, e-commerce sales in the US, as a share of total retail sales, increased to 1.2 per cent in late 2001, being valued in excess of US\$10 billion in 2001. The same data also shows that an average of 10 per cent of all e-commerce transactions in nine EU countries plus Canada involve purchases from sources outside the EU and Canada (oecd.org 2002). It is worth mentioning here that there is no Australian perspective in this thesis. Data on the growth of e-commerce in the US is used simply because it is available from a reliable source. All data presented here is indicative of international trends regarding an international phenomenon (international consumerism), as indicated in the US and elsewhere.

According to the OECD's (2002) survey of cyber-consumers, one of the most significant impediments to engagement in a CCT is consumer concern about the lack of consumer protection, specifically "fraud and deceptiveness, trust concerns/concerned about receiving and returning goods" (oecd.org 2002). The above data shows that the proportion of e-commerce sales to total retail sales have increased *without* alleviation of consumer concerns about Internet purchasing. This suggests that a solution to the problem of untrustworthiness (for consumers) will lead to a further, possibly exponential, acceleration of e-commerce sales.

However, currently there is little effective government control in respect of CCTs; this means that vendors, in the apparent absence of effective redress methods for online fraud and deception including CCTs, can generally breach CCTs with impunity. National consumer protection laws such as the Trade Practices Act and the Sale of Goods Acts of the various Australian states, whilst applicable to consumer transactions, may not be applicable in

practice to international CCTs due to their limited jurisdictional reach, or face resistance by foreign vendors.

The use of national consumer protection laws in CCTs, through the inclusion of law clauses within contracts between vendors and consumers, can involve complex private international law issues concerning jurisdiction, recognition and enforcement. If CCTs continue to increase as the present trend indicates, it will be despite such problems. The more such problems can be solved, the more popular CCTs will become. Conversely, unless a remedy is soon found, unsatisfactory experiences with Internet consumer transactions will eventually result in critical loss of consumer confidence in the Internet and electronic commerce.

A minimal solution to the CCT redress problem would be to make the enforcement provisions of national consumer-protection laws globally enforceable through an international treaty. A more comprehensive solution would be to amalgamate the various national laws into a single set of internationally-applicable laws to ensure global cyber-consumer protection. Both solutions could only be achieved through the negotiation and implementation of a comprehensive international convention, and only governments working in concert can achieve that, since only they have the coercive powers of states, individually as sovereign nations and collectively through treaties.

A third possible solution is a libertarian one: leave those who choose to conduct transactions in cyberspace alone to regulate themselves. ‘Cyberspace’ may be considered as the global but generally borderless space created by the Internet (as opposed to the actual physical world, referred to in this thesis as ‘realspace’), and within which some perhaps legally novel phenomena occur; for example, multiple cyberspace identities representing a single real-world identity, or vice versa, or a person ‘existing’ in cyberspace whose identity does not correspond with any physical or artificial identity in the real world (Johnson & Post, 1996).

However, such a ‘self-regulated cyberspace’, a concept considered in detail in Chapters Seven and Eight, would have no ultimate authority to enforce its own laws, at least where breach of consumer contract occurs offline. Non-litigation-based remedies, such as alternative/online dispute resolution, are usually ineffective remedies for CCTs, a point explored in Chapter Nine.

It might be argued that the ‘minimal solution’ just described is already available through the international scheme underlying the *Foreign Judgments Act 1991* (Cwth). This scheme facilitates the enforcement of the rulings of a plaintiff’s local court against foreign defendants in the country of the defendant. Such enforcements, however, are limited to the rulings of superior courts and thus are well beyond the monetary jurisdiction for matters involving CCTs. They also involve agreements between only a limited numbers of countries and are applicable only to the assets of the defendant in the country of the defendant. The US, for example, is not a party to the scheme behind the *Foreign Judgements Act 1991*.

As this thesis will demonstrate, none of the existing or currently proposed solutions to the CCT redress problem are satisfactory. The pursuit of foreign vendors from within their own country through use of national consumer redress laws is not economically viable in respect of the vast majority of CCTs which are too small in value compared to the cost of litigation. Other potential consumer redress schemes such as ‘industry codes of conduct’ (where vendors are members of an industry sector which regulates itself), alternative/online dispute resolution, web-site ‘Trustmarks’ or the like, credit card-holder maximum liability limits on fraudulent transactions, ‘chargeback’, or transaction insurance, are either legally unenforceable, too narrowly-based, or impractical.

Before the governments of the world can proceed to develop and implement either a minimal or comprehensive international consumer redress/protection law, it must be completely and

authoritatively demonstrated that none of the existing or currently proposed solutions to the CCT redress problem are adequate. Such a complete and authoritative demonstration has not yet been conducted, and this thesis fills that gap.

1.4 Motivation of the study

The motivation of the research is the following:

- There is an urgent need to redress the legal framework that governs the CCT and cyber-consumer protection, as it occurs in realspace.
- There is a need to tackle the jurisdiction limitation to some certainty—Australian Consumer Law (ACCC), Commonwealth Law, and state law. Cyber-consumer protection and CCT are needed not only for a single national law, but also for a single international consumer law: an international enforcement scheme with strong powers for all nations, states and territories, to be used to manage online fraud and online criminal offences, and regulate cyber-consumer protection.
- There is a need to point out the weaknesses in consumer protection laws ('ignorance of law'), and suggest redresses to strengthen consumer protection law as well as cyber-consumer protection laws. There is also a need for an international task force to provide international assurance on cyberspace and safe transactions.
- There is a need to provide guidelines not only to counteract cyberspace fraud and deception, but also to deal with losses and psychological harm after being deserted by the vendor, and to provide a safe online environment that will help strengthen and encourage global online trading and activities.

- There is a need to propose an international system for the regulation of international online sales methods, and redress for cyber-consumer protection involving approaches to prevent DA.

1.5 Thesis objectives

This thesis seeks to achieve three specific objectives.

To provide a detailed cognitive process analysis and behaviour study of cyber consumers and CCT in order to provide alerts that help protect consumers engaging in consumer transactions, including CCTs from online fraudulent behaviour and deception, through legal and theoretical perspectives on protection for consumer protection and CCTs as a phenomena of cyberspace.

To provide a Cyber Consumer Protection Framework for the prevention of DA, and to validate its adequacy and effectiveness based on the extended existing legislation of redress for not only national cyber-consumer protection but also internationally as well as CCTs.

To seek a range of potential solutions within a Cyber Consumer Protection Framework on how to prevent DA and how to recover the losses before and after a fraudulent event occurs, including relevant models of laws enacted or proposed by the UN, the EU, the OECD, the US and others with a focus on uniting such law models to address the currently ineffective means of tackling CCT redress problems, and to assess the likely effectiveness of the various initiatives/solutions (if any) to unite or unify such laws.

1.6 Thesis plan

The following chapters support the development of the Cyber Consumer Protection Framework:

Chapter Two - *Theoretical background, The Literature of the Study of Deceptive Advertising* - raises the common issues related to DA and the laws related to consumer protection and CCT. There are several areas in the law that need to be covered for the purposes of this thesis. These laws involve Australian consumer protection law, private international law, cyber law, and e-commerce law.

This chapter briefly describes the above-mentioned laws; Chapter Five discusses them in depth including their relationship to cyber-consumer protection and CCTs.

Chapter Three, - *Advertising Deception and research Issues* - examines the recognition of the effects of deceptiveness. The chapter suggests a framework for the determinants of DA process, defining the determinants of consumer recognition of deception when exposed to it through the consumers' level of recognition (exposure), attention, comprehension and prior knowledge, involvement and beliefs; all help to alert the consumer to deception and fraud.

Chapter Four - *Conceptual framework* - raises the main issues of DA and consumer protection. This chapter also discusses the weaknesses of current consumer protection approaches, and explains the benefits of introducing cyber law and cyber-consumer protection.

Chapter Five - *Conceptual Definition of Deceptive Advertising and Consumer Protection* - defines the concepts of DA from the legal perspective as it involves consumer protection and redresses and the behavioural dimension as it determines the consumers' cognitive process, to

what level the consumer is aware of noticing the deceptive advertising message when exposed to it. As the main concern of this thesis is online-related fraud and deception related to CCT, this chapter's focus is mainly on online fraud-related issues and online deceptive advertising and online strategies. Also, it is worth mentioning that various types of online fraud are discussed which, although different, are all somewhat related to online deception.

Chapter Six - *New Cyber Legislation, Libertarianism versus Interventionism* - concerns consumer protection and the regulation of cyberspace and, to some extent, realspace, in terms of 'libertarianism' and 'interventionism' — terms which will be defined there. It considers whether cyberspace should be regulated at all, who should regulate cyberspace, and how it should be regulated; and concludes that interventionism is the best approach to take to solve problems with effective redress for CCTs. The purpose of this chapter is to establish and examine the wide context in which problems associated with redress for CCTs exist, since most CCTs will be transacted, at least to some extent, within cyberspace. Within this context, the link between the availability or otherwise of effective redress for online fraud and deceptiveness related to CCTs and the existing regulation regime, is considered.

Chapter Seven - *Extension of Law for Federated Cyber Consumer Protection* - assesses the effectiveness of existing methods and guidelines for federated consumer protection. The assessment is based on the current laws and legislations; this provides the foundation for discussing and addressing potential solutions.

Chapter Eight - *International Cooperation for Cyber Consumer Protection* - examines and evaluates the opinions of academic, judicial and other commentators regarding the specific redress and enforcement provisions of the model consumer redress-related laws proposed by Australia, the United Nations, the Organisation for Economic Cooperation and Development, the European Union and the United States – and whether such provisions translate, or could

translate, into mechanisms for cost-effective CCT redress. It is also concerned with the assessment of potential redress for CCTs.

Chapter Nine - *Cyber Consumer Cognitive Process and Behaviour* - assesses in depth, through previous studies, the consumers' cognitive processes and characteristics. This chapter discusses DA from the legal perspective in order to identify where laws and legislation fail to protect cyber-consumers and CCTs.

Chapter Ten - *New Cyber Solutions for cyber consumers* - assesses the effectiveness of existing methods and the potential solutions and CCT redress mechanisms. The assessment is based on the various empirical data available, including data on contractual solutions such as credit card terms and transaction insurance, technological solutions such as trust marks, consumer complaint bulletin boards, and national deregistration, alternative dispute resolution (ADR) and arbitration, consumer education programs, industry codes of conduct, and the appointment of foreign lawyers.

Chapter Eleven - *Identifying and Measuring Deceptive Advertising* - assesses through previous studies, consumers' level of awareness and recognition of deceptive advertising.

Chapter Twelve encapsulates the thesis and provides recommendations for redress methods and future research.

1.7 Conclusion

This chapter included brief definitions of the major themes of this research and presented the objectives, motivation and structure of the thesis. The conclusions reached in this thesis apply to all consumer transactions whether or not they are conducted online. For reasons of simple practicality (see below), it seems that the Internet is, and will for the immediate future,

continue to be the most common means by which consumers will engage in consumer transactions for the purchase of consumer goods. However, CCTs are not a special case, and the problems faced by consumers contracting internationally via the Internet are not substantively new. The only differences the Internet appears to make are: (1) the global volume of CCTs has increased exponentially because the Internet makes consumer transactions vastly easier to engage in; and (2) the complexity of consumer transactions conducted via the Internet, and thus the potential complexity of the associated legal issues, is potentially much higher in some cases.

Consumers do not normally prefer to conduct transactions by telephone; hence, the consistent focus on CCTs in this thesis. Further, the Internet itself could provide a new forum for redress possibly via an automated cyberscourt, a prospect considered in Chapter Ten.

There is, on the other hand, an important distinction between CCTs and consumer transactions involving parties in the same country: the international dimension of CCTs makes them more-expensive in the case of having to obtain a remedy. Adding jurisdictions typically adds greater expense. Such additional expense for an effective remedy, in the present circumstances, is virtually impossible. Obtaining an effective remedy for a domestic consumer transaction may not be easy, but getting one for a CCT is virtually impossible precisely because it is a CCT. This is the rationale for the focus on international CCTs in this thesis.

CHAPTER TWO

THEORETICAL BACKGROUND AND LITERATURE REVIEW

2.1 Introduction

Deceptive advertising is a harmful marketing activity for both the consumer and the marketer. If it is possible to identify the harms inflicted on the consumer, then, in the long run, the advertiser would also be harmed as a result of using deception in an advertisement targeting potential consumers. After trying the product, if a consumer is dissatisfied, then it is likely that a repeat purchase will be made from a competitor, which in turn exposes the first vendor to losses resulting from the loss of some of his marketing share (Methenitis, 2007).

Some countries have tried to eliminate the practices of DA by issuing legislation or establishing bodies which have the power to fight DA and to reform vendors. An Act issued in the US by the Federal Trade Commission (FTC) and False Trading highlighted the prevalence of the concept of DA in the period between 1914 and 1969 (Millstein, 1969).

The legal concept of DA relies on making decisions about the application of a set of standards which, when evident in an advertisement, deems it as deceptive. Those standards were determined in light of advertisements which consumers thought were deceptive, through rulings issued by courts, and the efforts of scholars in this field. This led to the extension of the powers of the FTC to monitor DA (Millstein, 1969; William, 1998).

2.2 History of deceptive advertising

To establish the history of DA, the ad's history must be examined from its initiation through to the various stages of its development, taking into consideration that the ad reflects the needs and values of society; hence, the ad is a reflection of the scientific, social, economic and technological characteristics of society at a particular time. Therefore an ad can give an insight into the targeted audience, whether it is society in general or a particular sector (Moore, Farrar, Ronald, Collins & Erik, 1998).

Therefore, it is often not possible to determine the exact point at which DA began, since the ad is representative of a social stage in its development and therefore cannot be judged by recently-established standards. Moreover, the courts in 1911 asked consumers to test the goods which they intended to purchase, to see if they were suitable. The courts also expressed the view that the ad is a mere expression — a matter of opinion — which should be dealt with accordingly (Gellhom, 1969).

The establishment of the FTC in 1914 in the US can be considered, , as signalling the beginning of interest in A.D. This was accompanied by scholars' interest in DA as a concept that affects the consumer's purchasing behaviour (Gellhom, 1969).

The period from 1970 to 1990 witnessed an increased interest by scholars in DA, unlike the decline of interest shown from 1990 to 2000 (Dann, Dann, Belch & Belch, 2004; Ross, 1996).

Due to the harm caused by advertisers' practice of DA, most countries passed legislation in an attempt to put an end to those practices which inflicted harm on both the consumer and the advertiser (Ross, 1996).

2.3 Cognitive approach to deceptive advertising

Cohen (1975) was the first to discuss advertising deception. In previous studies, Cohen did not determine any of the cognitive variables which mediate the process of recognising the effects of DA; rather, he brought attention to the necessity of studying those variables. However, Cohen did establish some standards that are still used by the FTC to determine or identify DA.

Nevertheless, Cohen (1975) acknowledged that these standards were not enough to identify DA, and that the consumer's cognitive variables need further studies to determine the process of recognising the deception.

On the other hand, Gardner (1985) focused on the beliefs that the consumer forms as a result of being exposed to DA as a basic element mediating the process of recognising advertising deception. Gardner also concludes that DA can be recognised when the consumer has some beliefs about the attributes of the advertised product which differ from the normative attributes of the product's functional attributes. This is what Gardner calls the 'normative belief' method.

Kuehl & Dyer (1986) followed Gardner's method by considering the beliefs as the cognitive variable which affect, mediate and determine the process of recognizing the advertising deception.

Hulbert and Howard (1973) conclude that DA is recognised when the consumer interprets the set of symbols contained in the advertised message through comprehension of the advertised message. Accordingly, the researchers determined the process of recognising (comprehending) the advertising message as a behavioural variable determining the process of recognising the DA.

Aaker (1974), tried to direct attention towards the cognitive processes which occur within the consumer's cognitive structure. He concludes that the cognitive processes are a major determinant of recognising the advertising deception through which the consumer reaches conclusions contradicting the reality of the advertising message. Aaker did not determine any of the components of the cognitive framework as being a fundamental behavioural variable mediating the process of recognising advertising deception. Rather, he considers the sum of cognitive processes as a mediating variable in determining advertising deception.

Armstrong and Russ (1975) state that the cognitive variables mediating DA process awareness are the consumer's perception and beliefs in the availability of certain traits in the advertised product as a result of exposure to the DA message.

Jacoby and Small (1975) reached the same conclusions as those mentioned in the previous studies. They determined that the cognitive variables which mediate DA process awareness are those which form impressions or beliefs.

In a similar vein, Olson and Dover (1978) concluded that cognitive variables which mediate the consumer's recognition of the DA message are the process of forming false beliefs. Therefore, beliefs are considered to be the basic determinant of the processing of the DA message.

Gaeth and Heath (1987) claimed that the cognitive variables which mediate the advertising deception awareness process are the processes of forming beliefs. Accordingly, the researchers consider beliefs as a basic determinant of advertising deception.

Wright (1973) concludes that trends of advertising and trends of production lead to the acceptance of the advertising message and to the failure to recognise the advertising deception.

Shimp and Preston (1984) conclude that the extent of attention paid to the advertising message and the implicit and explicit claims it makes, are considered the cognitive determinant of recognising DA and that the greaterer the extent of the consumer's attention when receiving the advertising message, the more probable becomes the recognition of the advertising deception.

In another study, Shimp (1978) determined that the ads which contain claims based on a comparison of advertised products with rival products, are deceptive. This is because this biased comparison misleads the consumer and might be deceptive since the consumer is taking the ad at face value without question.

Bonnie and Robert (1987) conclude that the consumer's failure to understand the meaning of the brand name leads to failure to recognise the deception in the advertisement. Accordingly, the researchers use the comprehension process as a cognitive variable which mediates the process of recognising advertising deception. Those results concur with the results published by the FTC concerning the purposely deceptive markings on some products.

Johar (1995), as well as Lord and Kim (1995), conclude that the consumer's level of involvement is considered a cognitive determinant in recognising the deception in an ad, and that the process of protecting the consumer against DA requires studying the involvement framework of the consumer in order to eschew the effects of advertising deception on the consumer. In light of the research:

- There is a consensus of opinion among researchers that cognitive processes mediate the process of recognising advertising deception by the consumer, so are cognitive determinants of advertising deception.

- In the above-mentioned study, in light of the methodology of each respective study, the cognitive process was studied as a cognitive determinant mediating the process of awareness of advertising deception.
- The researcher can, in light of previous studies, suggest a framework of the determinants of advertising deception enabling this to be recognised, and an affective framework for each cognitive process variable involved in recognising DA.

2.4 The approach of the Federal Trade Commission

In 1914, the American Trade Law was amended. The first paragraph of Article Five mentioned the establishment of the FTC, which had the authority to monitor and prohibit the practices which harm competition. Those practices were labelled ‘Unfair’. Since then, the FTC has been interested in monitoring ads which harm competition. The commission focused its efforts on monitoring advertising practices which allow one of the competitors to establish profiles through untruthful advertising claims (Carney, 1972).

In 1914, The FTC started dealing with cases of DA on the basis that they imply unfair practices. It passed a significant amount of legislation to control the advertising of false prices or fraudulent claims (Craswell, 1985).

In 1938, the first paragraph of Article Five of the American Trade Law was amended to give the FTC more authority to control deceptive practices or untruthful practices in trade. The amendment introduced the term ‘Trade’ which was intended to mean both sides of offer and demand, or the producer and the consumer. This amendment meant that the FTC could deal with DA directly, by virtue of law, not just in the framework of unfairness of the ad and the practices which cause harm to competition, as was the case according to the first legislation issued in 1914 (Cohen, 1980).

It is worth mentioning here that the FTC, according to its constitution, comprises a group of experts in the area of products subject to advertisement. Horton (1984) believes that this type of organisation (i.e. the group of experts) led to concentrated efforts by the FTC to monitor ads that had the potential or capacity to deceive, in light of the opinions of experts taking the perspective of the producer and not the consumer.

But, with the rise and diversification of cases of deception, in early 1971, the FTC declared the ‘Advertising Substantiation Program’ (Cohen, 1980; Wilkies & Wilcox, 1974). The aims of this program were: that the ad shall imply the full statement of information required for the consumer to take the right purchasing decision; identifying the ads not supported by proof to be announced by the FTC as being un-supported advertising claims; and the ads should be stopped until they become supported (Brandt & Preston, 1977; Wilkes & Wilcox, 1974).

It is worth mentioning that the program faced some difficulties, represented by the tests which indicated an advertised product’s performance, or the certificates which supported the ‘truthful’ ad claims, making the consumer believe in their authenticity whereas they are just one commercial aspect of the advertised product, without any real test results or certificates from experts (Brandt, M., Preston, I., 1977; Wilkes & Wilcox, 1974).

In 1977, the FTC started to use consumer-based evidence in order to identify DA claims, considering that evidence as supplementary and not as an alternative. This did not change the concept and the FTC’s approach to dealing with DA. Hence, no consideration was given to the behavioural effects of DA, and its influence on decisions and actions taken by the consumer (Brandt, & Preston, 1977; Preston, 1987).

2.5 Australian consumer protection law

Consumer protection laws serve to protect individuals from fraudulent corporations or business practices. These laws may also assist consumers to rebuild credit or recover from bankruptcy. Some countries such as Germany, the United Kingdom (UK) and Australia, have agencies that operate to protect consumers to a certain level, whereas the US Congress has passed several Acts to regulate fraudulent business practices and protect consumers (ftc.com 1977).

Furthermore, in Australia, consumer complaints are addressed by the ACCC, which enforces the *Trade Practice Act 1974* and serves to protect consumers from fraud. Warranties of the Act are specifically aimed at regulating product safety and identifying unfair trade practices (law.justanswer.com, 2010; Vaughan, 2000).

Circumstances confronting courts include whether they have the inherent power to practice any jurisdiction in any particular case, the laws of which jurisdiction should be applied to resolve the dispute, and trans-border recognition and enforcement of judgments.

The most important consumer protection law in Australia is the Trade Practices Act. The Act is considered in two significant passages in this thesis—once here, to assist with the establishment of the legal context for this thesis, and later, in Chapter Ten, as one of several model laws whose redress provisions are analysed and compared.

The Act came into force on October 1, 1974, and it was introduced to provide uniformity of business rules for fair trade in relation to both business-to-business (B2B) trade and business-to-consumer (B2C) trade. The Act thus regulates both anti-competitive trade practices, and misleading or deceptive trade practices throughout Australia.

The general purpose of the legislature in enacting the Act was stated in the Australian Federal Parliament's Second Reading Speech, vol 57:

The purpose of the Bill is to control restrictive trade practices and to protect consumers from unfair commercial practices. The principle known as caveat emptor which may have been appropriate for village markets has ceased to be appropriate as a general rule, because now the marketing of goods or services is conducted on an organised basis and by trained executives with whom the untrained consumer is no match. Thus, now the consumer needs protection by the law.

Whereas, in 'village markets', the seller and the buyer had roughly equal knowledge about the subject of their negotiations, the widespread availability and complexity of goods, such as motor cars, computers, television sets, etc. means there is indeed now an inequality of bargaining power (through an information/knowledge imbalance) in the market, thus prompting governments to try to achieve a level playing field on behalf of the entire community.

Thus, the Trade Practices Act is two Acts rolled into one: it contains laws concerning B2B transactions, such as laws about restrictive trade and anti-competitive practices; and it contains laws safeguarding consumers engaged in B2C transactions. The two types of regulation are bundled together, presumably, because they are both concerned with consumer protection; for example, prevention of anti-competitive practices protects consumers.

It is this second type of law which is of direct relevance to CCTs; specifically, certain provisions contained in Part V, Consumer Protection, which eliminates unfair trade practices (such as misleading and deceptive conduct, and false representations). Also of relevance are provisions in Part IVA, Unconscionable Conduct, dealing with situations where unfair advantage is taken of a person under a 'special disability' by another party, where that other party was aware, or ought to have been aware, of that special disability, and Part VI, Enforcement and Remedies, concerning fines, injunctions and damages to allow public and private enforcement of the Act indirectly in connection with CCTs involving the fraud,

wrong-delivery or non-delivery of goods to consumers. It is envisaged that such provisions would become part of the substantive content of a comprehensive harmonised CCT solution.

The most important specific provisions which should be considered here are Section 71, from Part V, and Section 80, from Part VI. Section 71 relates to the problem of fraud, as defined in this thesis, by prohibiting the supply of goods, deception, misleading information by a vendor to a consumer, or when goods are unfit for their intended purpose or not of merchantable quality. Section 80 allows an aggrieved consumer to apply for a mandatory injunction to compel the honouring of a contract to remedy such breaches.

In terms of the justification for state intervention in the form of consumer protection law, the specific ground for intervention in contractual performance is undoubtedly inequality of bargaining power: society will not tolerate deception or non/wrong delivery by a corporation merely because a corporation is better able to absorb the response of individual consumers to deception or non/wrong deliveries than consumers are able to absorb deception or non/wrong deliveries.

In other words, just because a corporation has greater bargaining power, a corporation should not be permitted to breach contracts with consumers by deception or non/wrong delivery. As for *non-delivery*, further examples of statutory intervention are Section 52 *Sale of Goods Act 1896* (Queensland), which allows a consumer to sue for damages for non-delivery of goods, and Section 53 of the same Act, which allows a consumer to sue for specific performance of a contract for supply of goods.

The principal consumer protection law in Australia is the Trade Practices Act, a Commonwealth law. While internationally/online the Trade Practices Act has little status, it is useful to consider here as it provides an example of how a law can be successfully created

and enacted over the divergent laws of separate geographical areas (Windeyer & Young, 1964). Therefore, here it is discussed as a useful principle, not in terms of its status.

The Act applies to the activities of corporations and the commercial activities of non-corporations who engage in online interstate or overseas trade or online commerce in Australia. Section 109 of Australia's Constitution provides that "when a law of a State is inconsistent with a law of the Commonwealth, though not applicable to the cyber-consumer, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid."

The Act therefore applies to matters involving more than one state, and it overrides prior inconsistent state consumer protection-related laws. The Act was introduced to deal with the divergence of consumer protection laws between the states, such as the *Misrepresentation Act 1972* (South Australia) and the *Contracts Review Act 1980* (New South Wales) which had no close equivalents in the laws of other states. The Act is therefore a successful attempt at ensuring the universal recognition and enforcement of judgments within a multi-state environment, and at uniting substantive content—but not including the cyber-consumer.

In addition to concerning itself with Australian cross-jurisdictional matters, the Act also applies to overseas trade or commerce, and thus purports to reserve for itself an extra-territorial application. For example, Section 4(1) refers to trade and commerce "between Australia and places outside Australia", Section 6(2) refers to the Act having effect in respect of contracts relating to trade or commerce "between Australia and places outside Australia", and Section 67(b) provides that where a contract for the supply of goods to a consumer purports to substitute the law of some other country for the provisions of the Act, the Act applies regardless. Once again, this may be effective if enforcement is sought against assets of a foreign vendor *within* the jurisdiction, if there are any.

This is the basic problem with domestic consumer protection laws which purport to exercise full extra-territoriality: such claims are necessarily hypothetical when it comes to the enforcement of judgments (based on such law) regarding assets outside the geographical scope of that law.

In respect of CCTs where the foreign vendor has no assets within the Australian consumer's jurisdiction, the Act provides a remedy no better than the litigation redress method described in Chapter Nine. So, domestic consumer protection laws such as the Act considered here are ineffectual in dealing with failed CCTs because they cannot be effectively applied against the foreign assets of uncooperative non-performing foreign vendors. This is true even if the foreign vendor in question resorts to the domestic consumer protection law by invoking a particular clause in the law.

2.6 Regulation of business to business and business to consumer transactions

There are three main issues which need to be considered here.

The first is whether there is an essential difference between B2B and B2C transaction types, in which case there should be a regulatory system for B2C transactions, which is completely separate from that for B2B transactions.

According to Vaughan (2000) "the main difference between B2B and B2C is the buyer, whose expectations, choice of suppliers and product, payment method and purchasing requirements vary dramatically from one customer to another". While this is not a juridical approach to the issue, Vaughan's perspective is a reminder that consumers are indeed

different or at least can be different from corporations and lead back to the basic discussion regarding whether consumers should be protected by law at all.

Martin (2002), however, says that B2B contracts justify the adherence to traditional freedom of contract principles in a way that B2C contracts do not. Businesses may be presumed to possess a measure of sophistication in commercial bargaining which individual consumers do not.

To argue that the existence of two different types of law, trade practices law to regulate B2B and consumer protection law to regulate B2C, is evidence that there is a difference between them that justifies having separate laws, is a global argument, and thus the discussion must fall back on whether or not consumers should be protected by law at all. As the issue has already been canvassed, however, it is not necessary to go any further with that here.

The second issue is whether an interventionist approach should be taken to regulate online B2C transactions just because this is the approach taken for the regulation of online B2B transactions. The interventionist arguments given above for the protection of consumers would, as a matter of common sense, strongly suggest that interventionism for protection of B2C transactions should be stronger than for B2B transactions, given the weaker position of consumers in B2C transactions.

Further, the fact that CCTs occur in cyberspace does not, in any way, appear to weaken the arguments for consumer protection through interventionism. On the contrary, the greater the distance of the vendor from the consumer, the more the consumer needs protection, since foreign vendors could more easily avoid national regulators or enforcement agents.

The third issue is whether B2B laws can simply be modified to regulate B2C transactions. The existence of distinct laws for the independent regulation of trade practices and of

consumer protection suggests not, but perhaps more telling is the fact that the Hague (2003) Convention on Private International Law, which alleges in some way to regulate international B2B transactions, expressly excludes provisions regulating CCTs.

2.7 Contract law

An issue of fundamental importance to redress for CCTs and the wider issue of international consumer protection is whether an enforceable contract even exists—a contract cannot be breached if it does not exist, so the question of whether a contract can be validly formed internationally and electronically, in cyberspace, is fundamental. Once that threshold is crossed, the law regarding enforceability of contracts for each is out of the picture, at least as far as it is separate from consumer protection law. As a result, contract law, for the purpose of this thesis, can be dispensed with quickly.

Whilst the basic principles of offer and acceptance are not affected by technology, and legal requirements that contracts be constituted in writing or signed can pose difficulties for paperless transactions, consideration has therefore been given to statutory developments relating to digital signatures.

The challenge for the law is to assure the recipient that the sender of the electronic message is who he or she purports to be, that the text of the message has not been altered thus eliminating the risk of repudiation, and that the recipient wishes to do business with the sender within the terms of a potentially binding electronic communication (Horning, 1997).

In other words, there is an issue as to whether electronic contracts can be valid and binding.

Many common business practices have accepted ‘signatures’ deemed adequate under the Statute of Frauds. In *Brown v The Butchers and Drovers’ Bank*, a bill of exchange endorsed

in lead pencil, was considered sufficient to amount to a signature according to the Statute of Frauds. Moreover, code words adopted by pre-arrangement, bank account numbers written on the back of cheques, stationery containing a business letterhead, and purchase order forms with the firm's name at the top have all been held to satisfy the 'signed' requirement of the Statute (Horning, 1997).

Section 8(1) *Electronic Transactions Act 1999* (Cwlth), provides that "for the purposes of the Commonwealth, a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications."

Section 10 *Electronic Transactions Act 1999* (Cwlth) provides that an electronic signature, such as a consumer's electronic signature in a CCT, can be valid if certain requirements are satisfied. Other countries have passed similar legislation.

2.8 Private international law

Private international law refers to a collection of laws that determine which jurisdiction will apply in a specific legal case. In this definition, jurisdiction usually refers to a location, such as a state in which certain laws are upheld although they may not be necessarily imposed on other areas. Consequently, these laws can determine where a hearing is to be held, if one is needed. Private international law is usually consulted if a party involved in the case has a stake in an unrelated jurisdiction (Nyhg & Davies, 2002).

On an international level, private international law can be complex, as its purpose is to reach a middle ground in recognising and implementing national laws, while at the same time acknowledging other countries' own sets of laws. In some cases, these laws, sometimes called 'conflict of laws', also have to acknowledge the laws related to business

establishments, while still implementing national or foreign laws. Some cases can be more complicated when countries have multiple jurisdictions, such as in the US, where each state is an individual jurisdiction.

In general, there are three elements of private international law (Sykes & Pyles, 1991).

- The first, determines what cases the court system can handle if given authority by judges.
- The second is the choice of law — the process that decides which set of laws will be used in resolving the case and reaching the final verdict.
- The third is foreign judgment or the agreement to impose the laws coming from one jurisdiction to another.

This topic is examined briefly here to assist in establishing the legal context of CCTs and to construct a basis for a proposed solution, presented in the final chapter. It is examined more closely in Chapter Nine, for a different reason.

Private international law is part of the municipal domestic law of each country and subject to unilateral change by each country's own legislature. As such, private international law rules vary between countries. Private international law deals with relationships between private persons in different countries and is concerned with resolving 'conflicts', wherever they arise, due to interaction between independent legal systems. Conflicts can occur, from the viewpoint of a particular local court, when a dispute has foreign elements in it, such as where one of the parties is a resident of a foreign state, the cause of action has arisen in a foreign state, or a foreign legal system or foreign litigation are somehow relevant (Nygh & Davies, 2002; Sykes, & Pyles, 1991).

Nygh and Davies (2002) conclude that *private* international law must be distinguished from *public* international law which is a supranational legal system that exists independently of the

legal systems and legislatures of each nation, and which can be altered only by international convention, and is concerned mainly with relations between sovereign nations.

A basic issue in this area, for this thesis, is whether consumer protection principles found in private international law are effective for transactions mediated by the Internet.

A representative view on this issue seems to be that private international law on consumer contracts is not very well developed and is unlikely to be able to cope with the new problems caused by Internet consumer trade—current private international law does not always provide adequate solutions for consumer contracts made over the Internet (Nygh, 2002; Schu, 1997).

Schu (1997) also mentions that the place and form of marketing activity in the cyber world is not appropriate as far as connecting factors are concerned. To determine the applicable law, relevant connecting factors are the places of business or residence of the parties in addition to substantial content of any online marketing. On the basis of these connecting factors, a set of basic rules for consumer contracts made in the cyber word can be established.

Unfortunately, while rules for jurisdiction clauses in CCTs for the sale and purchase of goods have been proposed, some do not seem to amount to radical departures from the ordinary private international law rules which present so many problems in this area. For example, where the contract is for the supply of goods to a delivery address coincident with the consumer's residence, a strong connection of the contract to that place exists; however, the connection is strong enough to place the applicable law in the country of the consumer's residence *in the absence* of a choice-of-law clause (Schu, 1997).

The basic private international law problems for CCTs, whether mediated by the Internet or not, are uncertainty, complexity and expense:

uncertainty due to the unpredicted outcome of potentially involved foreign laws;

complexity because of the inherent complexity of litigations involving multiple legal systems; and

expense because of the need to comply with the practical demands of complexity. While, strictly speaking, these problems are not unique to CCTs mediated through cyberspace, they may be greatly aggravated by it.

If both parties were located within the same geographic jurisdiction of the court, then the local law would most likely apply. However, where the controversy involves parties in more than one state, the court must determine which jurisdiction's laws it will apply, although activities conducted via the Internet may give rise to particularly thorny choice-of-law questions.

Online transactions may routinely involve several jurisdictions. For example, a person in state A may make a communication through a computer located in state B, received by a person in state C through a server located in state D, owned and operated by a company headquartered in state E, that results in shipment of physical goods from a source located in state F (Rothchild, 1999).

While not new in terms of their intrinsic legal nature, the potentially extreme increase in uncertainty, complexity and expense is new; hence the demand for appropriate and effective legislation. A court may potentially be faced with a matrix of facts far more complex than those found in 'normal' or 'traditional' trans-border transactions in realspace, which can make extremely difficult the job of deciding who has jurisdiction and what law will apply.

There are some libertarians in this area with unconventional views regarding seller and consumer relations. The Internet, according to Rice (2000) who cites an example concerning

securities traders “alters the balance of power between buyer and seller because it arms buyers with masses of information and new analytical tools”. While this assertion has to be seen in the context of the fact that securities traders are undoubtedly more sophisticated than the usual Internet consumer, this is an original notion and may in fact become a general development to watch for in the future.

Furthermore, the basic principles of jurisdiction are essentially geography-based. As a result, jurisdictional principles are difficult to apply to the Internet, which is a largely boundless medium. A website may be viewed from anywhere in the world; the actual location of computers is irrelevant to either the providers or recipients of the information; and there is no necessary connection between the Internet address and a physical location (Rice, 2000).

The conclusion drawn from this observation is that “the rules of jurisdiction pre-date the personal computer age courts and regulators. The Internet is a serious issue because the Internet of today is a glimmer of what lies ahead” (Rice, 2000).

In other words, legislation has not kept pace with the new technology and its consequences. The controlling minds behind these events, however, necessarily remain at specific points in realspace, a fact no doubt behind the EU’s position that “the Convention focuses on the substance of transactions, as opposed to their form” (Dickie, 1999).

Nygh (2002) also argues that the Internet defies traditional rules based on national sovereignty and locality; national legislatures cannot impose their will on it, courts cannot call the actors in the Internet before them or seek to regulate their actions, cyberspace is an area beyond the reach of municipal law that is either anarchic or must be made subject to its own rule and institutions.

Nygh (2002) re-asserted recently that the problem of locating relevant cyberspace events geographically, the problem of identifying cyberspace parties, and the fact that the global reach of the Internet potentially brings multiple legal systems into play in any CCT done there, all challenge existing private international law rules (Nygh, P., 2002).

Furthermore, the researcher points out that “these issues have not as yet been addressed specifically by the revisions of private international law and jurisdiction which have taken place at national and international level. Nothing has been stated; of any rule that addresses specifically jurisdiction and choice of law in online transactions” (Nygh, P., 2002).

In light of the above, a warning has been issued by Nygh (2002) against an automatic reflex against adopting libertarian views because “those who act through the Internet can be found within legislative and judicial jurisdiction of nation states. Cyberspace is not a no-man’s land where anarchy reigns.” Cyberspace is not beyond the reach of conventional state intervention, according to this view.

Balanced against this is the observation made earlier that recent libertarian views have departed from their earlier position that Cyber law/cyber law and realspace law are forever separate, by asserting that the old libertarian assertion that cyberspace is immune from territorial regulation is susceptible to an empirical rebuttal: realist commentators who disagree with them need only refer to examples of successful Internet regulations in China and Singapore to refute their argument (Harvard Law Review 1574).

2.9 Cyber Crime Law

In previous chapters, “cyberspace” has been defined as the global but generally borderless notional virtual “space” created by the Internet, as opposed to the actual physical world

which is referred to as “realspace”. Cyberspace is also been defined as “a computer network consisting of a worldwide network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange (Dictionary.com),” and as “the online world of computer networks” (Merriam-Webster Online Dictionary).

Within cyberspace, novel phenomena occur in terms of legality . For example, multiple cyberspace identities may be used to represent a single real-world identity, or vice versa; and the identity of a person “existing” in cyberspace may not correspond with any physical or artificial identity in the real world (Johnson, D., & Post, D., 1996).

Further, cyberspace lends itself to the increased probability that a vendor’s true identity or location is legally unknowable, and that the law governing any particular transaction is indeterminate.

Cyber law has been defined in this thesis as the body of law used to regulate cyberspace. It has also been defined as “an embryonic collection of laws and principles which, through design or necessity, have been applied to the Internet” (Lim, 2002), whereas Fitzgerald (2002) sees it as a “law relating to the internet, digital intellectual property and electronic commerce” All three definitions emphasise that ‘cyber law’ is new, is a synthesis of older laws, is very broad in scope, and is as yet undefined as an exact jurisdiction.

A major theme within the cyber law literature is whether governments should be involved in cyber-consumer protection in cyberspace through a sub-set of cyber laws. Specifically, the issue is whether consumers who shop online, nationally or internationally, can be protected by ‘market forces’ or other non-government means, or whether there is a need for cyber-consumer redress/protection laws specifically adapted or created for CCTs.

Thus, this issue is concerned with arguments about the extent of government involvement in cyber-consumer redress/protection in cyberspace, and informs considerations given to the nature and extent of regulation proposed by any relevant model law, whether national or international: whether governments are to be involved in protecting CCTs, and how this should or might be done. Consideration of how to protect CCTs is thus an issue at the core of any consumer redress/protection sub-set of cyber laws. Solutions to CCT problems will thereby emerge, apart from other sources, and will affect the development of cyber law.

Cyber crime is generally defined as any type of illegal activity that makes use of the Internet, whether through a public or private network, or a private home computer system. While many forms of cyber crime concern the appropriation of proprietary information for unauthorised use, other examples involve the invasion of privacy. As this is a growing problem around the world, many countries are beginning to implement laws and other regulatory mechanisms in an attempt to minimise the incidence of cyber crime (Johnson & Post, 1996).

Furthermore, common examples of cyber crimes that may also be classified as Internet crimes, or that may have a cyber-component to them, include fraud, phishing, and identity theft, as well as terrorist activities and child pornography. Crimes such as fraud and identity theft are often committed through phishing. Cyber crime is normally attempted by hacking into personal files, or deceives people into divulging personal data and/or banking account information over the Internet, which the cyber-criminal later uses to make illegal purchases or transfer funds from one account to another (Lim, 2002).

Computer crime encompasses a wide variety, and ever growing, array of crimes. As a result of the many different types of computer crimes, the techniques and procedures used in cyber crime investigation are varied as well. Often, cyber crime investigation involves law

enforcement agencies in multiple jurisdictions. Traditional law enforcement detectives, forensic accountants, and experts in information technologies are all frequently involved in investigating cyber crimes (Fitzgerald & Fitzgerald, 2002).

2.10 E-commerce and technology approach

Electronic commerce or e-commerce refers to economic activity that occurs online. E-commerce includes all sorts and types of business activity such as online shopping, online banking, investing and rentals. The popularity of online commerce is understandable, considering the time and hassle otherwise involved in running from one location to another (Sykes & Pyles, 1991).

Global Internet use is continuing to increase at a rapid rate – faster than any governing law. As the Internet and its technical capabilities outpace the judicial systems of the world, regional, and international courts continue to try cases with no legal precedence. Until laws are passed to address every possible internet-related crime, it is most likely that internet crime jurisdiction will be largely determined by case history.

2.11 Online lawyers

Seeking out foreign lawyers for matters related to online transactions (i.e. those who reside in the vendor's country) is one means by which a consumer might respond to some sort of fraud, a non-delivery or wrong-delivery in an CCT where such response covers (mostly) all manner of negotiations with the vendor, but extending to litigation in the vendor's country, should that be required.

With respect to foreign lawyers, a lawyer in one country who wishes to acquire the assistance of a lawyer in a foreign country, would most likely start by enquiring through their local Law Society (or equivalent) to see if they had the contact details of the equivalent body in the relevant country, who would then be contacted for a recommendation based on various suitability criteria. Alternately, the lawyer could conduct a search for such contact details online.

The first method would probably not even occur to the average consumer and, while the second method would necessarily be technically available to the Internet-using consumer, it would probably not even occur to them to look for such a body. Average consumers are unlikely to know about the existence of various foreign law firms. A third method and perhaps the most common would be for the consumer or their local lawyer to approach a local law firm with foreign agents or affiliates.

Such appointments apart from cost, language and private international law issues, potentially provide an excellent solution to problems associated with CCTs. Furthermore, such appointments will not alter the fact that the CCT itself has trans-border-related difficulties, but it may make the subsequent handling of the matter easier because of the lawyer's local knowledge and skill. For example, it may be more worthwhile for a lawyer in the vendor's country to negotiate with the vendor rather than for the consumer's local lawyer to attempt the same. The possibility of appointing lawyers in the country of the offending supplier might potentially reduce the complexity of such situations down to the level found in the situation facing a consumer involved in a dispute with their local supplier pursuing the usual methods of redress.

Unfortunately, foreign lawyers, being 'foreign', will not always speak the language generally spoken by the consumer or in the consumer's country. Therefore, at the very least, there may

be communication problems between the foreign lawyer and the consumer. Such problems may involve misunderstandings, delays, and increased expenses as direct and indirect results of the language barrier. Thus, cost, language and private international law issues are potentially inherent in situations involving foreign lawyers, and such issues may create serious difficulties for the average consumer.

Furthermore, the common procedure of finding appropriate foreign legal counsel may present another difficulty for the average consumer in its own right, as is the issue of not just finding *a* lawyer in a foreign country but finding the *right* lawyer. The associated problems do not necessarily stop there.

Black (1997) considers the obstacles faced by a consumer considering litigation in a distant location. The prospect entails considerable expenses for travel, both for the consumer and for any witnesses, and communication expenses that are unlikely to be recouped by the awarded costs. The already formidable step of retaining a lawyer is doubly daunting if the lawyer resides in a distant jurisdiction. Foreign counsel will not infrequently be retained on the consumer's behalf by the local lawyer initially contacted by the consumer, which means that the consumer is faced with bills from two lawyers, one of whom is an unknown quantity.

Since the lawyers may have different incentives when it comes to the question of whether to settle or sue, a proceeding may be dragged out in an inefficient manner. In addition, there will be emotional interference since a consumer who litigates in a faraway location will feel psychologically vulnerable and exposed, while the local corporate party will feel correspondingly grounded and assured.

Furthermore, attempts to retain foreign lawyers could see costs escalate. In any event, there remains the potential problem of cost, language and private international law issues.

In the best-case scenario, though very unlikely, the cost problems would be no worse than those in connection with the appointment of lawyers in the consumer's own country of residence in a straightforward consumer redress action against a local supplier—probably expensive enough as it is.

The more likely scenario is that because costs would probably be increased by distance and language issues and possibly also by private international law issues, they are likely to be higher for the plaintiff consumer as compared with costs generated in a purely domestic action. Should it come to litigation, the preliminary process of adjudicating choice of court and choice of law issues can add a whole extra set of expensive problems that must be dealt with before the substantive issues of the original dispute are addressed, especially if the private international law issues are themselves disputed.

Apart from such difficulties, there may also be problems inherent within a foreign jurisdiction because of local cultural peculiarities. For example, in a country like Indonesia, it would be very unusual for an individual consumer to even contemplate an action in the courts, due to the expense and uncertainty of the process and a perceived bias in favour of government or large corporations.

In any event, even with no problems with foreign lawyers, such foreign lawyers guarantee nothing either with or without litigation. That is, expense is the only thing that one can be certain of when retaining a foreign lawyer; it cannot be assumed that a desirable result will be the outcome of the litigation (Black, 1997).

The foreign lawyer redress method may be no better than litigation, and possibly even marginally worse. In other words, if the use of this method is taken to include legal costs, the cost would clearly be comparable with the cost of litigation. Furthermore, if litigation involved any extra costs for foreign lawyers, this method could be worse than straightforward

litigation. If the foreign lawyer method is used without resort to actual legal proceedings, the relative cost would be better than the cost of litigation, since it excludes the costs of litigation.

In terms of enforceability, and continuing to assume that the foreign lawyer method is being used without resort to actual litigation, the method is not especially effective as it is basically concerned with negotiation and the threat of litigation, and as such, it has very little actual coercive force, although it has some degree of psychological coercive power through the involvement of court officers.

In terms of complexity, and continuing to assume that the foreign lawyer method is being used without resort to actual litigation, the method is simple compared with actual litigation. It would be fairly straightforward, once the initial step of retaining the foreign lawyer was taken and assuming potential language difficulties could be avoided, for the cyber-consumer to supply the foreign lawyers with whatever statement and evidence were required.

Based on the above theory, this method without litigation does not involve actual coercive power but may have some persuasive power; its difficulty of enforcement is therefore ‘high’. Finally, the online foreign lawyer’s method of redress in terms of complexity is ‘acceptable’. It is likely then that the appointment of online foreign lawyers might not be effective as a means of solving problems with fraud and CCTs. Tabulated, the overall result for online/foreign lawyers is as follows: Table 2.1: Online/foreign lawyers

Method	Difficulty of enforcement	Complexity
1. Online/Foreign Lawyers	High	Acceptable

2.12 Online public consumer protection authorities

If choosing to obtain help from ‘online foreign public consumer protection authorities’ for cyber-consumers, the deceived cyber-consumer approaches the cyber-consumer protection

authorities in the country of the foreign vendor (if any) either directly or through a local consumer protection authority, hoping that the local authority has a cooperation agreement with an equivalent institution in the vendor's country.

While this is a promising development, enforcement agencies do not typically co-operate in support of consumers bringing actions for civil remedies, and domestic law may pose barriers to enforcement agencies entering into cooperation agreements. For instance, the wording of domestic laws may explicitly link enforcement powers to a specific law. Depending on how narrowly these powers are specified, this may preclude enforcement agencies from providing assistance in respect of matters which do not come within their jurisdiction (APEC, 2002).

In 2002, Asia-Pacific Economic Cooperation (APEC) countries with cooperation agreements were Australia, China, Japan, Korea, Mexico, New Zealand, Russia and the US. The possibility is that regardless of how proceedings are initiated, the authority in the vendor's country may act to seek redress from the vendor on behalf of the consumer.

Depending on the exact nature of the powers invested in such bodies, they are likely to be in no better position to resolve the problem than is the consumer's local authority. The Australian authority, the ACCC, may act against a local offender at the request of a foreign consumer in relation to serious offences, albeit not for low-value CCTs, usually referring problems with CCTs to econsumer.gov.

The econsumer.gov website (launched in April 2001) has amalgamated a number of information resources into a single location. A consumer facing an unfair/fraudulent vendor in a foreign jurisdiction, however, would be hard-pressed to find anything there which would lead to an effective enforceable remedy.

The remedy options offered on the site are neither practical nor helpful. For example, the site allows consumers to “report your complaint” but advises that “you should not necessarily expect any country to pursue your complaint on your behalf” and suggests “ways to resolve your complaint”, but these are limited to “links that may offer a quick and inexpensive way for you to resolve your complaint without having to initiate a formal legal action”. The relevant text, in full, states:

Government agencies may use this information referring to the consumer's complaint report to investigate suspect companies and individuals, uncover new scams, and spot trends in fraud.

However, you should not necessarily expect any country to pursue your complaint on your behalf. Although your complaint may be accessible to government agencies, it may or may not be accessed by them. (econsumer.gov)

Many government agencies bring law enforcement actions to protect the public-at-large, but do not intervene on behalf of individual consumers. Other agencies have an obligation to investigate each complaint. An example is a link to information about ADR/Online Dispute Resolution (ADR/ODR), an ultimately unenforceable option in the vast majority of cases, and depending for success on the benevolence (or otherwise) of the vendor.

The website, while better than nothing, amounts to little of real use; it is merely a complaints registry which guarantees nothing at all (although, as indicated by Michael Donohue, OECD's consumer policy analyst then responsible for the 2003 OECD Guidelines, it may be too early to criticise such efforts, as no trend data is available yet). As of late 2005, such trend data was still unavailable although it was being collected.

The ACCC is also a member of the International Consumer Protection and Enforcement Protection Network (ICPEN), which is a membership organisation consisting of the trade practices law enforcement authorities from more than two dozen countries. The mandate of the network is to share information about cross-border commercial activities that may affect

consumer interests, and to encourage international cooperation among law enforcement agencies (ACCC, 2005).

Bodies like the ACCC and its equivalent in other countries, econsumer.gov and ICPEN, appear to have a long way to go to provide dependable and cost-effective remedies for unsatisfactory low-value Internet transactions.

The redress methods of Foreign public online-consumer protection authorities are normally completely free of charge; all costs of pursuing a resolution are carried out by the public authority which investigates and handles complaints at no cost to members of the public. The only cost incurred by the deceived online consumer would be the incidental costs of submitting complaints with copies or originals of relevant evidence.

In terms of enforceability, the ACCC, for example, may act against a local offender at the request of a foreign consumer in relation to offences other than low-value CCTs, usually referring problems with CCTs to econsumer.gov which, itself, is likely to refer such matters on to ODR providers.

However, where the public authority decides, for example, to take on an offender in order to set an example, it could conceivably litigate. In that case, costs would be low, being restricted by the authority and the enforceability would be high since the foreign enforcement powers would be as effective as possible, given the amount of assets if the vendor remains in the jurisdiction. ‘Taking on an offender in order to set an example’ would, however, occur only in exceptional circumstances and would not be available to consumers as a right.

In terms of complexity, the method would be comparatively simple. It would be fairly straightforward, once the initial step of locating the foreign authority was achieved and

assuming that language issues, if present, were not insurmountable for the consumer to supply that authority with whatever statement and evidence was required.

This method of redress sought through a foreign public consumer protection authority is quite financially reasonable but still not without some expense. This method does not normally involve actual coercive power but may have a little persuasive power; its difficulty of enforcement is ‘very high’. Finally, in terms of complexity, this method is ‘acceptable’. Hence, this method of redress may not be effective as a means of solving problems involving low-value CCTs. Tabulated, the overall result for foreign lawyers is as follows.

Table 2.2 Online foreign public consumer protection authorities

Method	Difficulty of enforcement	Complexity
2. Online Foreign Public Consumer Protection Authorities	Very high	Acceptable

2.13 Alternative dispute resolution and online dispute resolution

ADR is a broad term for a range of methods by which dispute resolution is attempted without resort to litigation and thus without direct appeal to judicial enforcement powers. ‘ADR’, for these purposes, will be taken to incorporate the term ‘ODR’—or online ADR—except where ODR is treated separately.

As a preliminary point, it should be noted here that ODR is not substantially different from ADR; it is merely a technological means of facilitating ADR by allowing some/all efforts by parties to ADR to be made online instead of face-to-face. Also, CCTs, being international in nature, will necessarily require the ODR variant of ADR rather than traditional ADR: rational disputants to low value international consumer transactions (ICTs), being in separate

countries, will not usually physically travel across international boundaries to attempt to settle.

ADR may or may not entail the involvement of a neutral third party, but usually will do so.

ADR has also been defined as the decision-making process by which matters are resolved outside the usual court-based litigation model.

The aim of ADR is to encourage parties in conflict to arrive at compromise solutions with the assistance of a neutral person. ADR includes processes such as assisted negotiation, expert appraisal, mediation, conciliation, evaluation, and arbitration (Butterworths, 2002). It should be noted though, for the purpose of this research, ‘arbitration’ and ‘ADR’ are treated differently. Arbitration here is capable of being judicial, whereas ADR is provided by commercial providers. This thesis thus treats arbitration and ADR separately for clarity and because they are capable of being treated differently.

When a third party is involved in ADR, varying degrees of expertise can be brought to the process, they can have varying degrees of involvement in the process, and their final opinion may be more or less binding on the parties, depending on the rules and standards applicable in each case. Other terms such as ‘mediation’, ‘conciliation’, ‘negotiation’, etc. are understood here as forms of ADR, although it can be noted that the array of third-party involvement, from lesser to greater, arguably runs: negotiation, mediation, conciliation, arbitration.

The term ‘binding’ is understood here as follows: the consumer contract contains a provision that says that in the event of dispute concerning the contract, the parties agree that any subsequent decision resulting from ADR, would be contractually binding on the parties. The problem, however, is that enforcement could involve resort to litigation, which could have been used in the first place.

The OECD's paper on ADR commences with a useful summary of the topic, starting with ways of avoiding the need to resort to ADR in the first place: complain to the vendor, get your credit card issuer to help, contact your local consumer protection agency (OECD, 2002). Specifically, the paper says that "usually, the best first step is to contact the business directly. Businesses often have excellent complaint handling systems that will help solve your problem quickly and efficiently" This is reasonable advice but it will not help the deceived online consumer who wishes or needs to pursue a matter with an uncooperative foreign vendor.

The paper then suggests that "if you paid for goods or services using a credit or debit card ... read your payment card statements for information on contesting charges", and further recommends that the consumer could "check with local consumer protection agency to see whether any special protections apply in your country" (OECD, 2002). Local consumer protection agencies, however, will almost certainly have very limited leverage against foreign/fraudulent vendors.

There are some potential advantages and disadvantages of ADR. ADR can offer cost advantages: it is currently expensive to litigate internationally or for online purposes, especially since there are no guaranteed outcomes, and a means of achieving the same result at relatively low cost could be extremely beneficial. A potential problem with ADR, however, is that there can be ongoing 'service' vendor unresponsiveness to calls to attend ADR and subsequent enforcement problems.

While this criticism can also apply to international litigation, enforcement is potentially a far more serious problem with ADR as it all depends upon the cooperation of the parties involved, even where binding ADR clauses are present in a CCT. If a potential 'defendant' in a transnational ADR matter simply chooses to ignore the ADR equivalent of 'service of

process' or 'judgment', there is little the ADR provider can do about it, even if mandatory or binding ADR clauses are legal in the country of whichever party has the decision against them, apart from recommending litigation to the plaintiff should they succeed.

In respect of judgement, the OECD paper states that where mediation is used "it's up to you and the other party to reach an agreement" (OECD, 2002). This advice will be of little help to a consumer with a legitimate grievance in the face of an intransigent vendor beyond the reach of a body with real enforcement power.

The OECD (2002) concludes that "if you have tried ADR unsuccessfully your last resort may be legal action". Thus, the OECD recommends that the consumer avoids ADR if they can, but if the deceived cyber-consumer must resort to ADR, that ADR does not guarantee a resolution and aggrieved consumers may eventually still have to resort to litigation to pursue their claims.

This raises the following argument: if a deceived cyber-consumer believes there is any chance at all of wasting their energy, time and money by ineffectively pursuing their claim through ADR either because no satisfactory decision will be reached, or because a good decision can be reached but the merchant will not comply with it, thereby requiring litigation anyway to obtain enforcement, then by-passing ADR and going straight to court must be a better alternative. This requires a consideration of two further issues. First, when is there a chance of a deceived cyber-consumer wasting their energy, time and money by ineffectively pursuing their claim through ADR? Second, are there any further advantages of ADR (other than the cost advantage already noted above) which will more strongly justify a cyber-consumer taking a chance and risking it?

Regarding the first question, there could be many indications that the character of the foreign online merchant is such that ADR may be at risk. The merchant could in fact have a good

consumer relations reputation. The merchant could have a convincing consumer disputes policy that suggests they wish to maintain a good public reputation and therefore they will take ADR seriously in a manner sympathetic to the reasonable claims of consumers. They could represent a well-known brand name and wish to avoid adverse publicity even if it costs them something to buy good public relations. The amount at issue could be either trivial or significant and ADR is therefore simply worthwhile depending on the subjective perceptions of the deceived cyber-consumer. The cyber-consumer may therefore decide that they would be wasting their time on ADR if any or all of these factors are either objectively absent, or absent because the consumer may feel the merchant will not co-operate in ADR. For example, in Australia to date there are no reported cases where a court has enforced a pre-existing agreement to mediate, will not take it seriously or will not abide by the decisions made there and thus, the courts will not help anyway (ADR agreements, 1999). This imputes non-rational motives to cyber-consumers. Regarding the second question, Rule (2000) has suggested twelve advantages other than potential cost-saving, which will more-strongly encourage a cyber-consumer to take a chance and attempt ADR before resorting to international litigation. These other (albeit overlapping) advantages of the ODR variant of ADR for consumers (over international litigation) are summarised by Rule (2002):

Speed: scheduling meetings and planning for travel and finding space are not necessary to convening and beginning an online process. A virtual meeting room can be opened instantaneously and a neutral person can be engaged from anywhere around the world.

Asynchronous interaction: online participants have the possibility of asynchronous (non-simultaneous) interaction where their response is not expected immediately. Disputants can defer their response until after they have had time to consult or consider the situation.

Power differentials: people in relationships based on past/present power differentials (e.g. expert trader and consumer) can communicate on a more level playing field when online communication options are engaged.

Research: in an ODR process, it is a simple matter for participants to conduct research in the middle of the process.

Cooling distance: compared to face-to-face communications, ODR is less likely to escalate to accusations, name-calling and violence.

More-reflective communication: in written communications, people have a tendency to explain why they are saying what they are saying; whereas in face-to-face communications, people often just state their position and cross their arms, refusing to elaborate further.

Self-disclosure—race, sex, and age: different people are biased against different things. Some people are biased against race, others age or gender, but the Internet provides some anonymity.

Anonymous communication: applicable to CCTs if the deceived consumer had not already disclosed their identity when the contract was first established.

Convenience: in face-to-face communications, there is usually a ‘convening penalty’ consisting of the time, money and energy required to merely get the parties to sit down at the table. With ODR, this is almost entirely eliminated.

Access to better neutral third parties with more subject-area expertise: an advantage of ODR is that geography, schedule, and expertise are no longer major concerns. The parties can choose any neutral party they like to help them resolve their dispute, regardless of where that neutral party is in the world, their time zone, or even their other commitments.

Text-based communication: has the advantage that people are forced to translate their preferences into text from the beginning of the process. When the time comes to draft an agreement, the mediator can lift actual language from past postings to ensure that the parties will approve of the phrasing.

Efficient automated negotiation processes: when online, an automated tool such as blind-bidding software can be used, when the parties reach that particular stage, in order to more efficiently find the amount in question, without the time-consuming back and forth negotiation that characterises most procedures where one side and then the other make monetary bids in an attempt to agree on an acceptable amount.

For example, such software evaluates bids from each party and if the two bids are within a prescribed range (for example, 30 per cent) then the case settles for the median. If the cases are not within the prescribed amount, then the bids are destroyed and neither side knows what the other proposed. Both parties are fully informed about the way the process works before it begins, and they agree to abide by the outcome if one is reached. According to Smith, (1993) no actual law need be involved: in ODR, the legal location of the dispute is irrelevant because the resolution is crafted based on either the preferences of the parties, for example, an industry code of conduct, or some other standard administered by an arbitrator. It is not necessary to obtain legal counsel in the other country, because the decision is not going to be based on the law.

The question arises now as to whether any of these ‘extra advantages’ guarantee (or at least more strongly justify) an acceptable outcome for an average consumer involved with a CCT, such that ODR should be used instead of international litigation and, making the cost of ODR worthwhile.

‘Asynchronous interaction’, ‘research’ and ‘more-reflective communication’ are arguably a single advantage type as they are related. That is, it is asynchronous interaction which makes research and more-reflective communication possible. Of the 13 items listed above (apart from ‘anonymous communication’ which may be inapplicable to CCTs, and where access to better neutrals may be improbable due to the implication that any neutral they like will always be willing and available), all are probably highly attractive to a cyber-consumer, in theory, especially where the alternative is international litigation. The final advantage noted by Rule (2002) (‘no actual law need be involved’), would appear quite attractive because it means that any problems with national legal systems would not be an issue.

The law surrounding these trans-boundary transactions is complex. Just the process of determining which law applies to an online transaction can be costly. Obtaining legal representation or merely advice from another country can be frustrating and expensive. Legal systems are ill-equipped to handle effectively the disputes that straddle borders. Paying lawyers to put the time into figuring it all out does not make that much sense, especially if the transaction is less than a couple of thousand dollars (Rule, 2002).

At this point, ODR sounds like an appealing alternative means of redress for consumers involved in CCTs, more so if the cost of ODR were cheap relative to any particular amount in dispute. Rule (2002) also says that online dispute resolution is still a very new phenomenon, so there is a lot of confusion about how ODR services should be priced. While pricing models vary between ODR providers, there are some common trends. In auction or e-commerce disputes, there is usually a one-off filing fee paid by the initiator of the case.

There is a question about the success rates of ODR-type schemes, that is, about whether they are more effective than international litigation for CCTs. Unsurprisingly, there appears to be

no data on the success rates of international litigation for CCTs, but there is some data suggestive of how successful ODR-type schemes for CCTs might be.

For example, in 1989/1990, the Queensland Consumer Affairs Bureau reported results for ADR as follows: 38.1 per cent full redress; 15.4 per cent partial redress and 22.3 per cent incapable of resolution. For 1990/1991, the same bureau reported that less than 17 per cent of complaints were not satisfactorily resolved, and a further proportion of those achieved satisfactory results in Small Claims Tribunal hearings. Other states report similar high success rates (Harris, 1993).

It is up to the consumer, however, as to whether such data shows ODR-type schemes for CCTs would be worth the risk in terms of time, effort and monetary cost. Likewise with the following data: the US Postal Service, which has one of the most sophisticated and widely used employment ADR programs in the US federal government, found that 81 per cent of mediated cases are eventually closed without a formal complaint being filed. Satisfaction was also extremely high, with exit surveys completed anonymously by 26,000 participants indicating that 88 per cent of employees are highly satisfied or satisfied with the amount of control, respect, and fairness in the ADR process. The Air Force also found ADR very effective in the government contracts area, where it used ADR in more than 100 cases, of which more than 93 per cent settled (Rule, 2002).

Such results are encouraging but a fundamental problem remains. Effective redress for an individual average cyber-consumer or CCT is not available from ADR/ODR. ODR is conducted without the possibility of appeal to judicial enforcement powers: unfair merchants can simply ignore the ‘binding’ decisions of ODR providers.

Harris (1993) says of “private mediation services” that “in relation to consumer disputes, the service is of limited value as it is dependent upon the amenability of the respondent to the

process”; in respect of “community justice centres” Harris also states that “one weakness of this service as an effective dispute mechanism is its inability to ensure compliance, because any agreement reached in mediation is not enforceable in any court”; and in respect of “consumer affairs bureaux” “the agencies do not have power to enforce an agreement reached through intervention”.

At best then, ADR/ODR can be seen as making a valuable contribution to the range of options available to cyber-consumers, with some probability of providing a successful outcome for the cyber-consumer in the event of a favourable decision, noting that consumers seek more than just the one decision, which ever favourable.

There is also an issue about ‘cyberspace authorities’ like the Internet Corporation for Assigned Names and Numbers (ICANN).

One of the biggest challenges of ODR is its enforceability. Sometimes, enforceability in ODR is readily achievable. ICANN is an excellent example of this. When a panellist in a Uniform Dispute Resolution Policy (UDRP) process transfers a domain name, ICANN can easily enforce that decision because it has absolute control over the database that assigns domain names to their owners. In B2C e-commerce disputes, this type of absolute enforceability is not possible. If, for example, a product is shipped to a purchaser and the wrong amount of money is charged, the shipper or the ODR-provider cannot compel the purchaser to return the item or to pay more money.

Furthermore, ODR is “not compatible with disputes in which one side is not participating in a good-faith effort to reach a resolution. This includes all fraud and criminal cases, actually this would be true even without fraudulent intent: ODR may not help even where a merchant disputes a consumer’s complaint concerning mere non/wrong delivery of goods” (Rule, 2002).

This is an example of the self-regulatory regime of so-called ‘code’ (software controls) as the libertarian regulator of cyberspace proposed by Lessig (1996). Unlike realspace where the state tries to convince citizens to adopt norms of behaviour in order to obey the law, in cyberspace because of the unavoidability of ‘code’, the state does not need to ‘convince’ anyone of anything: it is a matter of either obey or stay out; there is simply no opportunity to do otherwise (Lessig, 1996). Such code may seem to regulate Internet presence, existence and activity within cyberspace, but simply will not regulate subsequent offline contractual performance of Internet retailers in realspace. Furthermore, stand-alone retail websites cannot be regulated by network code in the same way that Internet Service Providers (ISPs) can regulate their ‘chat room’ subscribers, for example.

Thus it would appear that none of those ‘extra advantages’ of ADR would guarantee an acceptable outcome for an average cyber-consumer involved with an CCT, such that ODR should be used instead of international litigation. At this point then, the two alternatives are the problems of decisions made through ODR potentially being truly enforceable only through subsequent litigation, or the problems of international litigation as they currently stand.

In terms of enforceability, the method is not especially effective as it is basically concerned with mediation and the potential threat of litigation and therefore has no actual coercive force, whereas in terms of complexity, the method is simpler than litigation. It would be relatively straightforward, in many cases, for the cyber-consumer to supply the ODR service provider with whatever statements and evidence were required but to adequately prepare for ODR as indicated by Rule (2002) could involve almost as much time and effort as preparation for litigation.

The question arises now as to whether effective redress for CCTs is available from ADR/ODR. ADR/ODR can be a valuable contribution to the range of options available to cyber-consumers, but with only some probability of providing a successful outcome for them in the event of a favourable decision concerning a disputed CCT. That would not be good enough. That is, for an average consumer who had fallen victim to some sort of fraudulent behaviour from a vendor, or paid for goods from a foreign source that were delivered but were not what was actually ordered, and who had evidence to prove their case and whose only option was ODR, ODR would not be good enough.

The effectiveness of ADR/ODR in the future depends, to some extent, on increased cost advantages but, primarily, upon strengthening enforcement powers. However, the prospect of this occurring seems unlikely.

Hence, it can be concluded that the ADR/ODR redress method does not involve actual coercive power but has some persuasive power; therefore, its difficulty of enforcement is ‘high’. Finally, its complexity is ‘high’: adequate preparation for ODR, as indicated by Rule (2002), could involve almost as much time and effort as preparation for litigation. Tabulated, the overall result for the ADR/ODR redress method is as follows.

Table 2.3: Alternative dispute resolution/online dispute resolution

Method	Difficulty of enforcement	Complexity
2 ADR/ODR	High	High

2.14 Arbitration

The term ‘arbitration’ can have at least two distinct meanings: “the system of determining disputes by a private tribunal constituted for that purpose by the agreement of the disputants”

(Butterworths, 2002) with non-binding decisions because tribunals do not exercise judicial power; or “the system of permanent *public* arbitral tribunals constituted not by the choice of the parties but by public authority”, not empowered to make binding decisions and not bound to administer the rules of evidence strictly. It is the first meaning which is of interest here as the public variety cannot be applied to CCTs.

Noting that the dictionary definition of arbitration alludes to the idea of a difference between public and private tribunals, ‘tribunal’ has been defined as: a person or body of persons, other than a court, who is required by law to act in a judicial manner to the extent of observing one or more of the rules of procedural fairness in arriving at decisions, for example, *Administrative Law Act 1978* s2 (Victoria) an executive/quasi-judicial body which usually reviews ‘administrative’ action—a tribunal may not exercise the judicial power of the Commonwealth, that is, make enforceable determinations of legal rights and obligations due to the doctrine of the separation of powers.

A private tribunal might thus be defined as a person or body of persons, usually with a commercial interest, empowered by an agreement between private disputants to act on an *ad hoc* basis for the purpose of dispute resolution, and which is required to act in a judicial manner to the extent of observing one or more rules of procedural fairness in arriving at decisions, but without judicial power to make enforceable determinations of legal rights and obligations.

The major distinction then between the two types of tribunal is that in the former (public) case, the body is permanently established by a government mostly to review the decisions of the Executive branch of that government; while the latter is either established by request of the parties to a private contractual dispute, or is resorted to by them, to resolve a private contractual dispute.

Thus, there are some fundamental similarities (aims, methods and absence of enforcement powers) and some fundamental differences (motivation, identity of the clients and permanency) between public and private tribunals. Further, the activities of the former are governed by administrative law, while the latter may be governed by the rules of procedural fairness and the law of contract.

In considering the relationship between ADR and private tribunals, a private tribunal could correspond to a process by which ADR could be achieved, a private tribunal could correspond to a type of ADR (e.g. mediation, conciliation); and both ADR and private tribunals can exist for the same purpose (dispute resolution). ‘Private tribunal’ may also be understood as a name for one type of commercial ADR-provider. Consequently, there is much overlap between the two terms (and thus between the terms ‘ADR’ and ‘arbitration’ as used here), but they are not interchangeable terms and therefore each must be used deliberately and precisely.

In terms of ‘enforceability’, the method is not especially effective as it is basically concerned with negotiation and, in some cases, the threat of litigation through binding outcomes and, as such, has very little actual coercive force, while arguably retaining a degree of psychological coercive power through the involvement of potentially binding court-like procedures.

Thus, in terms of complexity, the method is relatively quite simple compared with litigation. It would be quite straightforward, in many cases, for the cyber-consumer to supply the arbitration service provider with whatever statements and evidence were required, but adequate preparation for arbitration could involve almost as much time and effort as that needed for litigation.

The arbitration redress method can now be evaluated. As this method does not involve judicial power but would have some persuasive power, in terms of difficulty of enforcement,

it is therefore ‘acceptable’. Finally, the method’s complexity is ‘high’; arbitration is not simple. Arbitration is therefore probably not an effective means of solving problems with CCTs. Tabulated, the overall result for arbitration is as follows.

Table 2.4: Arbitration

Method	Difficulty of enforcement	Complexity
4. Arbitration	Acceptable	High

2.15 Industry-based consumer dispute resolution schemes

An ‘industry-based consumer dispute resolution scheme’ is understood here to mean a form of tribunal in the sense that it has been established as a tribunal in relation to any particular industry sector (e.g. telecommunications, banking, finance, insurance, timeshare holiday ownership, etc.), primarily with respect to the hearing of complaints against such bodies by private cyber-consumers. Such schemes seem to be positioned roughly mid-way along a continuum between public and private tribunals because they can possess some of the properties of both, but are probably positioned closer to the private end of that continuum because of the involvement with private cyber-consumers. An industry-based consumer dispute resolution scheme could therefore simply be regarded as a variety of the ADR scheme, or it could perhaps be understood to be a ‘dedicated’ ADR scheme.

In any event, whether ‘ADR’ or ‘tribunal’, from the perspective of CCTs, an industry-based consumer dispute resolution scheme suffers the same major weakness of both: lack of enforceability.

In terms of the enforceability criterion, the method is not especially effective as it is basically concerned with negotiation and, in some cases, the threat of litigation through binding

outcomes and therefore has very little actual coercive force, while retaining a degree of psychological coercive power through the involvement of court-like procedures.

It may, however, have less psychological coercive power than does arbitration because, since it is industry-based, it may be seen by the ‘losing’ vendor as being biased in favour of the industry member. Alternately, an industry-based consumer dispute resolution scheme may have more psychological coercive power over a losing vendor as the industry-based consumer dispute resolution scheme may wish to preserve the public image of its industry and treat its own industry members quite harshly with negative bias.

Thus, in terms of the simplicity criterion, the method is comparatively simple. Supplying an industry-based consumer dispute resolution scheme with information would be simple, although it could involve almost as much time and effort as preparation for litigation.

An overall result for this redress method is as follows. This method does not involve actual coercive power but probably has some persuasive power; its result for degree of enforcement is therefore ‘high’. Finally, the complexity result for this method is ‘high’. Therefore, industry-based consumer dispute resolution schemes are possibly not effective as a means of solving problems with CCTs. Tabulated, the overall result for industry-based consumer dispute resolution schemes is as follows.

Table 2.5: Industry-based consumer dispute resolution schemes

Method	Difficulty of enforcement	Complexity
5. Industry-Based Consumer Dispute Resolution Schemes	High	High

2.16 Codes of conduct

The topic of industry-based consumer dispute resolution schemes, examined above, is concerned with infrastructure (tribunals), whereas this section is concerned with quasi-legislation/legislation. The two topics are related, however.

As already noted, industry codes of conduct—also known as ‘voluntary codes of practice’—are bodies of rules which purport to regulate industries from within in the sense that an industry establishes its own rules, rather than having them imposed from outside by a government, which may also be used as the content of the ‘law’ which an ADR-provider etc. may refer to in its deliberations.

The codes are the basis of industry self-regulation and, while they do come in a ‘statutory’ variety, the non-statutory variety is the norm. An example of the former, in Australia, is the *Franchising Code of Conduct*, found in the *Trade Practices (Industry Codes – Franchising) Regulations 1998* (Cwlth). Statutory codes, however, are by far the exception to the general rule—that codes of conduct are non-governmental in origin—and, in any event, they still are a part of national law, normally having no applicability to CCTs except in the unlikely event that a relevant code, if one could be found, was agreed upon through a contractual choice of law clause.

Non-statutory codes of practice are voluntary codes enforced by trade associations and the like. Whilst these codes are to be commended and encouraged, they apply so far only to the country of location and not to trans-border transactions, and they set up industry and suppliers as judges in their own cause; they are also unsupported by state-backed sanctions. It is highly conceivable that bias or undue sympathy to industry members would be a problem in the event of complaint by consumers, when non-statutory codes are being applied.

The Internet-using business community has a clear incentive to help establish an environment which gives cyber-consumers the confidence to consume, and vendors who voluntarily comply with a code of conduct could encourage such confidence by displaying a kind of Trustmark to indicate the availability of such features as mediation of minor disputes, the provision of various kinds of consumer information such as the identity and location of vendors, refund policy, relevant law, delivery costs and times, and information about the relevant goods. However, as will be further discussed later, Trustmark the mere possession of a Trustmark does not solve the potential problem that a supplier may operate as a judge in their own cause. There is no state-backed adjudication and enforcement mechanism in relation to industry codes generally, and the cyber-consumer is still ultimately at the mercy of the vendor in the event of dispute or, at best, the best efforts of a sympathetic industry association.

There has been a recent attempt to improve this situation, but it serves only to reinforce the criticism. In mid-2003, the ACCC introduced a system of endorsement for ‘high quality’ industry codes of conduct, which would be hard to obtain, easy to lose, and provide the consumer “with some reassurance that the business they are dealing with operates in a fair, ethical and lawful manner” (Find Law, 2004).

This measure was described by the ACCC’s chairman as ‘co-regulation’ — being a mid-point between self-regulation and heavy handed regulation by government, which contains an implied admission that self-regulation is less than completely effective. It also raises the more fundamental issues as to how effective such endorsement would be for foreign cyber-consumers who know nothing of such national bodies, and of what help dis-endorsement would be after a failed CCT.

Furthermore, the code of conduct of either the statutory or non-statutory variety of the vendor's country may apply, which means the cyber-consumer would still be reliant on accessing a foreign quasi-judicial system, thus raising the problems noted in the previous section on online foreign public consumer protection authorities. Industry self-regulation through codes of practice therefore appears to be only a minor means of cyber-consumer redress for failed CCTs.

Assessed against the enforceability criterion, however, the method is completely ineffective in dealing with post-transaction problems with CCTs: the method has no coercive force at all and a minimum of persuasive force. Assessed against the complexity criterion, the method is comparatively less complicated than litigation. It would be relatively straightforward, in most cases, for the cyber-consumer to supply the body administering the code with whatever was required, but to properly prepare for this could involve almost as much time and effort as preparation for litigation.

The overall result for the industry codes of conduct redress method is as follows. It does not involve actual coercive power but may have some persuasive power; its result for difficulty of enforcement is therefore 'very high'. Finally, for complexity, the method is 'acceptable'. Therefore the application of industry codes of conduct may not be effective as a means of solving problems with CCTs. Tabulated, the overall result is as follows.

Table 2.6: Industry codes of conduct

Method	Difficulty of enforcement	Complexity
6. Industry Codes of Conduct	Very High	Acceptable

2.17 Escrow services

Escrow services are those whereby, for a fee, a neutral third party withholds a cyber-consumer's payment to a vendor until goods are delivered to the consumer's satisfaction. A typical escrow service is Escrow.com, described as follows.

Escrow.com reduces the potential risk of fraud by acting as a trusted third party that collects, holds and disburses funds according to buyer and seller instructions. Escrow services are provided by a licensed and regulated escrow agent.

Escrow is well-suited for items purchased on auction sites, automobiles, motorcycles, domain names, jewellery, specialised computer equipment, and other high-ticket items.

Buyers receive and inspect the merchandise before the seller is paid.

Sellers receive their money if the buyer accepts the merchandise (Escrow.com, 2005).

Put as simple as that, escrow services appear to represent a simple and complete solution to problems associated with CCTs. A consumer can simply avoid them altogether by using a trusted third party to hold off delivery of payment to the vendor until the consumer is happy.

Unfortunately, however, there may be potential problems on both sides, including the following:

- Online basic cost: Escrow.com charges a minimum of US\$25, a relatively high price to pay in the context of many low value CCTs for example, eBay recommends purchases over \$500 use an escrow (CarBuyingTips.com, 2005).
- Online complexity in the form of negotiations between online vendor and cyber-consumer as to who will pay what costs, which will simply be unacceptable for many

cyber-consumers engaging in low value CCTs who still desire to purchase internationally, though standard form escrow contracts for CCTs is no solution either. Also, multiple-party dispute resolution can be very complex.

- Online inapplicability: some escrow services may not cover international sales/purchases.
- Online unavailability: there may not be enough suitable escrow service providers available globally and online vendors/consumers may prefer such providers to operate in specific countries.
- Cyber consumer resistance: cyber-consumers may resist handing over money to unknown third parties because of trust or reputation issues.
- Cyber consumer naivety: cyber-consumers may simply forget to use an escrow service and may subsequently require a remedy which is then unavailable (CNN.com, 2005).
- Online vendor resistance to cyber-consumer payment being held by foreign escrow service provider due to anticipated trans-border problems in the event of litigation.
- Online fraud: there is a considerable risk of fraud from the many fake escrow sites on the Internet (CarBuyingTips.com, 2005).
- Online instability: escrow service providers are private organisations and may come into existence at any time and just as suddenly disappear. Thus, such a service could go into liquidation while holding a consumer's payment before delivery of the goods.

Furthermore, the enforceability criterion method is relatively effective as it will generally be a case of payment not being handed over without a satisfactory inspection by the consumer beforehand. Due to all the negative factors listed above, this method does not achieve a perfect result for difficulty of enforcement. Assessed against the complexity criterion, the escrow method has some problems in relation to the complexity, inapplicability, unavailability and instability factors mentioned above, which all serve to complicate use of this method for a cyber-consumer.

The overall result for the escrow redress method then, is as follows. This method does not normally need the involvement of coercive power unless coercion of the escrow service itself is required; its result for difficulty of enforcement is therefore ‘low’. Finally, the method achieves a ‘high’ for complexity. It is likely then that escrow services would not be effective as a means of solving problems with low-value CCTs. Tabulated, the overall result for escrow services is as follows.

Table 2.7: Escrow services

Method	Difficulty of enforcement	Complexity
7. Escrow Services	Low	High

2.18 The United Nations Guidelines

The UN Guidelines were released on April 9, 1985 by resolution 39/248 of the UN General Assembly. The UN Guidelines were re-released in an amended and expanded form by the UN’s Economic and Social Council resolution 1999/7 of 26 July 1999, and were adopted by the General Assembly in late 1999 (un.org, 2005).

Since the differences between the original version, which contained 46 clauses, and the new version, containing 69 clauses, are not relevant here, a detailed comparison between them is not made. Examination of the UN Guidelines here is restricted to the current version.

The structure of the UN Guidelines is as follows:

I. Objectives (cl 1)

II. General Principles (cll 2-8)

III. Guidelines (cll 9-10)

A Physical Safety (cll 11-14)

B Promotion and Protection of Consumers' Economic Interests (cll 15-27)

C Standards for the Safety and Quality of consumer Goods and Services (cll 28-30)

D Distribution Facilities for Essential Consumer Goods and Services (cl 31)

E Measures Enabling Consumers to Obtain Redress (cll 32-34)

F Education and Information Programs (cll 35-41)

G Promotion of Sustainable Consumption (cll 42-55)

H Measures Relating to Specific Areas (cll 56-62)

IV. International Cooperation (cll 63-69)

The redress-related provisions of the UN Guidelines are stipulated by clauses 32 to 34 which provide that governments should establish legal and administrative measures to enable consumers to obtain redress through procedures that are expeditious, fair, inexpensive and accessible (clause 32); that governments should encourage all enterprises to resolve consumer disputes in a fair, expeditious and informal manner, and to establish mechanisms which can provide assistance to consumers (clause 33); and that information on available redress should be made available to consumers (clause 34). The clause of greatest interest here is clause 32.

The UN Guidelines are only guidelines intended to assist countries with their efforts to protect consumers. This is recognised in what little commentary is available on the UN Guidelines. However, the UN Guidelines have been attacked for being 'vague' and 'overblown' almost to the point of uselessness (Weidenbaum, 1987).

For example, the UN Guidelines' objectives to "promote just, equitable and sustainable economic and social development" (clause 1) and to "encourage high levels of ethical conduct" (clause 1(c)) have been criticised for being "high-minded" and "fuzzy" (Weidenbaum, 1987).

Weidenbaum (1987) asks "who will set the standards of 'ethical conduct'" and "consider how substantially a totalitarian interpretation of ethical conduct would differ from that of various free societies". Peterson writes that Weidenbaum would criticise the US Constitution on the same grounds (Peterson, 1987).

Another criticism by Weidenbaum (1987) is that the UN Guidelines seems to be "a blueprint for a centrally directed society", and that "we need only consult the dismal record of any of the world's centrally planned economies to know that taking this objective would hurt rather than help the developing nations", whereas, Peterson (1987) says the US Constitution, which Weidenbaum swore to uphold and defend, is a blueprint for a central government, while the UN Guidelines binds no country to anything, but merely set out goals and objectives for all nations to aspire to in protecting their own people.

Peterson (1987) also argues that without effective governmental regulation, the worst practices of the worst competitors often set the norm in the marketplace. Peterson concludes by arguing that legitimate business throughout the world needs the kind of consumer protections which the UN Guidelines erect as a goal. As no honest business person wants to profit from harming the customer, the UN Guidelines will foster an atmosphere in which legitimate business can indeed prosper.

At this point, an aggrieved consumer could sympathise with both Weidenbaum (1987) and Peterson (1987), there being little of practical effect in the well-meaning UN Guidelines.

The UN Guidelines are also attacked by Weidenbaum (1987) on the grounds that “no convincing case has been made for the participation of international agencies in such a basic domestic consideration as the protection of consumers”. From such a perspective, it is unsurprising that he saw no particular vagueness in the redress aspects of the UN Guidelines found in clauses 32 to 34.

To his credit however, Weidenbaum did think that the UN Guidelines might solve international consumer problems, possibly without knowing in 1987 what such problems could be. In the Internet Age, the nature of such problems is now evident. However, the UN Guidelines are justified in part because they would help solve international issues not relevant to the cyber-consumer, although a straightforward reading of the Guidelines fails to uncover any such global concerns.

In response to the UN Guidelines’ redress recommendations (clauses 32 to 34), countries such as Australia, Canada, Hong Kong, New Zealand, Singapore and the US established various mechanisms for consumers to obtain redress with respect to national consumer transactions, including the introduction of special procedures into previously-existing lower courts, and the creation of new courts and tribunals which specialise in small consumer claims (Harland, 1991).

In some cases, procedural rules were simplified, hearings were sometimes held with the presence of lawyers being disallowed, night and weekend hearings were allowed, and parties were assisted with the preparation of their cases, with limited right of appeal (Harland, 1991).

Despite these advances however, the persistent problem of online fraud and failure of CCTs illustrates that clauses 15 and 69 have failed to provide adequate ‘cyber consumer protection’ in respect of CCTs.

The impact of the Internet was yet to be fully appreciated in 1991 and there was no consideration then of the special difficulties associated with trans-border consumer disputes. This continued to be true for academic commentators as late as 1997 (Harland, 1997; Ramsay, 1997).

2.19 The Organization for Economic Cooperation and Development Guidelines

The OECD is a Paris-based international body comprising 25 countries participating in a permanent cooperation designed to coordinate the policies of the member nations. The OECD makes available all information relevant to the formulation of national policy in every major field of economic activity. Its principal goals are:

- To promote employment, economic growth, and a rising standard of living in member countries, while maintaining stability.
- To contribute to sound economic expansion of both member and non-member nations in the process of development.
- To further the expansion of world trade on a multilateral, non-discriminatory basis in accord with international obligations. Policies are formulated and ideas shared at meetings held throughout the year.

This form of cooperation, rooted in the growing interdependence of national economies, began in April 1948, when a group of 16 European countries founded the Organization for European Economic Cooperation (OEEC) to administer the Marshall Plan and to work together for post-war recovery. The OECD, succeeding the OEEC, was established on

September 30, 1961, in order to broaden the scope of cooperation (Microsoft Encarta Encyclopaedia, 1996).

Upon consideration of this, both the status of the OECD, in terms of its heritage, aims and purposes, and its relevance to the phenomenon and potential of CCTs, is apparent.

The OECD's Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce that is, the OECD Guidelines, was released on April 9, 1999 (oecd.org 2005).

The OECD Guidelines were “designed to help ensure that consumers are no less protected shopping on-line than they are when they buy from their local store or order from a catalogue” (oecdpublications.gfi-nb.com, 2003).

The OECD Guidelines, however, are “non-binding” and “the overarching principle is that consumers shopping online should enjoy transparent and effective protection that is not less than the level of protection that they have in other areas of commerce” (oecdpublications.gfi-nb.com 2003).

The OECD Guidelines commence with a brief preamble, followed by an annex containing the guidelines structured as follows:

Part One - Scope

Part Two - General Principles

I. Transparent and Effective Protection

II. Fair Business, Advertising and Marketing Practices

III. Online Disclosures

- A. Information about the business
- B. Information about the goods and services
- C. Information about the transaction

IV. Confirmation Process

V. Payment

VI. Dispute Resolution and Redress

- A. Applicable law and jurisdiction
- B. Alternative dispute resolution and redress

VII. Privacy

VIII. Education and Awareness

Part Three - Implementation

Part Four - Global Cooperation

In terms of redress provisions, Part VIA of the OECD Guidelines (Applicable Law and Jurisdiction) states that B2C cross-border transactions are subject to the existing framework regarding the problems associated with applicable law and jurisdiction such as divergent conflict of laws rules, uncertainty, expense, complexity, lengthy delays in obtaining judgment and potential language difficulties.

E-commerce poses challenges to this existing framework and therefore consideration should be given to whether it should be modified. When considering any modification, governments should seek to ensure that, while facilitating e-commerce, the framework provides fairness to consumers and business no less than that afforded to other forms of commerce while providing consumers with redress without undue cost or burden (oecd.org 2005).

While, once again, the OECD Guidelines is only a set of guidelines, they indicate and reinforce the view that the existing situation with respect to CCTs is replete with difficulties and that governments should be responsible for providing a solution, a position which supports the positive preference for interventionism in this thesis.

Part VIB (Alternative Dispute Resolution and Redress) states that consumers should be given meaningful access to fair redress without undue cost or burden, and that governments should develop policies to resolve consumer disputes arising from B2C trans-border transactions. Furthermore, in implementing these policies, governments should employ information technologies innovatively. However, in order to meet these objectives at an international level, national and international governments, academics and others, need to conduct further studies (oecd.org 2005).

While these are commendable principles, in practice little is being achieved through the OECD Guidelines at an international level. The OECD's first major report on the implementation of the OECD Guidelines (oecd.org 2001), maintained that the Guidelines recognise the need for member countries to adopt and adapt laws to ensure that consumers are protected in the online environment. To this end, in the EU, member states have been taking steps to introduce directives based upon the Guidelines (olis.oecd.org 2005).

This kind of regional law-making is not quite consistent with the OECD Guidelines' Part VIB—which provides that “governments should develop policies to resolve consumer disputes arising from B2C cross-border transactions” as the full effect of the Internet on world-wide consumerism demands.

This criticism is borne out by further points made in the report, such as “in Canada, the national and provincial governments have agreed to work towards united and modernised consumer protection laws related to electronic commerce”, “in Mexico, the Federal

Consumer Protection Law was modified in May 2000”, and “in Australia, the development of legislative amendments continues”. All of these are regional and regionally-focussed initiatives and therefore doomed to irrelevance where international cooperation is required to provide a unified solution to the problem of effective justice for cyber-consumers and CCTs (olis.oecd.org 2005).

Other initiatives inspired by the OECD Guidelines and noted in the report are that “Japan and Korea agreed to co-operate through various efforts, including initiating a project aimed at mutual recognition of Internet trademark and the evaluation of websites in ‘sweep days’ ” (olis.oecd.org 2005).

The criticism here is not of the OECD Guidelines as such, but of the fact that those purporting to be guided by it are persisting with parochial mind-sets: the initiatives are all regional and, in some cases, even legally insignificant. For example, a trademark would not practically assist with a breached CCT except in extremely limited circumstances (olis.oecd.org 2001). A trademark provider could conceivably be sued for misrepresentation by an aggrieved consumer, but that is not likely to represent a general effective solution for breached CCTs.

In respect of the ‘Cross-border enforcement cooperation’, many cases of CCTs involve ‘fraud’ as such, also could still trigger an irresolvable dispute; international cooperation is needed beyond that between the US and Canada only; the most recent proceedings along these lines were in March 2000, enforcement cooperation is of little assistance without the pre-existence of judgments for CCTs that are recognisable across borders. Therefore, what is needed is wide international cooperation on effective and simple access to internationally and online recognised redress procedures and, for a comprehensive solution, the uniting of the substantive content of cyber-consumer protection laws, internationally.

2.20 The European models

In common with both Australia and the US, the EU, at least economically, is an example of a federal system of government (Bogdanor, 2003).

Bogdanor (2003) says that the EU certainly satisfies the federal principle. There is a constitutionally guaranteed division of legal sovereignty between two layers of government divided territorially. Sovereignty is divided between the EU itself and the member states. The component units that the member states retain are of course, very significant, if not preponderant law-making powers, but these powers are limited by the Treaty of Rome and the amending treaties (riia.org 2005).

Hence, the EU law models examined here may reasonably be understood as laws of Europe (as if they were the laws of a sovereign nation), and amount to a second example of what may be achieved cooperatively between separate states, in the manner of the Trade Practices Act.

The assessment in this section of the two EU law model law, the Distance Sales Directive and the E-Commerce Directive, necessarily includes some preliminary description and analysis of two associated but independent bodies of private international law: the Rome Convention (rome-convention.org, 1980) and the Brussels Regulation (curia.eu.int1986) (europa.eu.int 2001).

The Distance Sales Directive came into force in May 1997 (europa.eu.int 1997). It aims to protect consumers engaging in ‘distance contracts’, and applies to all companies engaging in online transactions with EU consumers. Notably, the Distance Sales Directive includes a right of withdrawal in favour of consumers that cannot be waived by contract.

The E-Commerce Directive came into force in July 2000. It provides a general legal framework for the conduct of e-commerce within the EU and by the EU Member States with outside parties (europa.eu.int 2000).

It can be seen that the general criticisms of private international law made in Chapter Eight (for example, lack of experience), even from the perspective of a lawyer in general practice, and especially from the perspective of the average cyber-consumer, are understandable. While this view could be challenged as being ‘merely subjective’ and grounded in lack of expertise, the more objective problems with private international law are less difficult to ignore. For example, some cyber-consumers may want to understand how to conduct their own actions, and complex private international law rules will often prevent this; private international law rules are subject to unforeseeable and unilateral alteration, virtually necessitating a constantly-updated specialist legal skill; and private international laws, from one country to the next, are just as likely to be inconsistent, as they are to be in agreement with each other, in many cases requiring skill with multiple sets of private international law rules. The issue now is whether these problems can be alleviated.

2.21 United States law

The most important federal consumer protection law in the US is the *Uniform Commercial Code* (the Code) of 1952 (Fullerton, 1997). It is worth mentioning that it is only ‘federal’ in that it is available as a universal guideline for each US state—thus the actual code for each US state can be different.

The purpose of the code is to “establish a uniform law to govern commercial transactions that often take place across state lines” (Barnes, 2005).

There is no express distinction made between B2B (business to business) and B2C (business to consumer) transactions. However, by defining “between merchants” as “any transaction with respect to which both parties are chargeable with the knowledge or skill of merchants” there is an implied difference in the treatment of B2B and B2C transactions under the code, thus ensuring that consumers are specifically protected. Further, the code would be a good candidate for inclusion in an international project uniting the various consumer laws, and containing the usual range of ‘standard’ consumer protection provisions such as provisions concerning implied warranties of title, merchantability and fitness for purpose, together with provisions concerning buyer’s rights to performance and recourses for dispute resolutions in the event of non-performance.

The relevant US private international laws, when the code is the law governing CCTs, are the so-called ‘long-arm statute’ laws. A long-arm statute has been defined as “a law that allows one state to claim personal jurisdiction over someone living in another state” (County of Santa Cruz, 2005). Each US state has its own long-arm statute(s).

In considering a matter with potential foreign elements, a US state court begins deliberations by examining whether jurisdiction over a foreign party is allowed under that particular state’s long-arm statute, and whether that jurisdiction would fall within the due process principle of the Fourteenth Amendment to the US Constitution (Debussere, 2002). It is the due process clause of the Fourteenth Amendment which enables a state to create a long-arm statute.

Under US law, a court in the state in which the consumer resides will have jurisdiction over a foreign defaulting Internet seller in relation to a CCT, when the minimum contacts of a non-resident defendant with a forum are such that the exercise of jurisdiction does not offend “traditional notions of fair play and substantial justice” Further, the defendant must have such a degree of “minimum contact” with the forum that “they might expect the necessity of

litigating there, for example by doing business within it, however a defendant need not have physically entered a forum in order to be subject to its jurisdictional reach” (Cordera, 2001).

In US law, then, the focus is on the activities of the *supplier* and not on the *consumer* as the US courts are required to conduct the ‘minimum contacts analysis’ of the supplier’s activity referred to above. Furthermore, a minimum contacts analysis which results in a court declaring itself competent to hear a matter in relation to foreign websites must have established that three extra conditions have been satisfied: the defendant must have performed a transaction within the forum, the exercise of jurisdiction in the forum is reasonable (i.e. does not place an excessive burden upon the defendant), and the website in question must be sufficiently ‘active’, i.e. it must do more than passively make information available; it must also allow for the creation of contracts, take payment, and exhibit other indicators of interactivity (Debussere, 2002).

The mere act of a corporation selling goods across any US state boundary will often satisfy this requirement for US jurisdictions. The result is that, while approaching the same issue from a different perspective, US law often arrives at a similar point to that of the Europeans under the Brussels Regulation: the consumer gets to litigate in their local court.

This will have cost and simplicity advantages for the US consumer. However, the difference under US law is that the US consumer can be subject to contractual choice of forum (i.e. jurisdiction) clauses (which would have no effect in Europe unless they favour the consumer). In the case of *Carnival Cruise Lines Inc. v Shute* 499 U.S.585 (1991) the US Supreme Court held that forum selection clauses in consumer contracts would be upheld where they were freely bargained for (i.e. given in exchange for consideration, without undue burden on the consumer) because of the cruise line’s international character, which increased

the likelihood and expense of being brought to court outside the US. By analogy, comparison of the borderless world of the Internet leads to a similar conclusion.

The US approach to redress for consumers in respect of disputed CCTs is both consumer-friendly and arguably fair to Internet business, although one should question how effective it would be in respect of CCTs. As to enforceability, however, it seems that the problem of actually enforcing the decision made by a consumer's local court where the defendant foreign Internet merchant has no assets in the forum jurisdiction (unlike under EU law, as noted above), still exists under present US law.

2.22 Conclusion

This chapter examined the term 'DA' and its stages of development. According to previous studies and following the legal trends of the FTC, it has been revealed that there is a gap between the legislations and the actual 'consumer protection' term. Hence, a wide gap exists between deception and the consumer's knowledge prior to understanding the advertisement and determining whether it contains a true or a false message. It also shows that consumer protection laws do not technically benefit the consumer after being deceived in any way, though they do include several clauses that constrain the advertiser or vendor to present a truthful and fair advertisement. However, the consumer still remains largely unprotected before, during and after a transaction, thereby giving vendors the opportunity to continue practising deception for their own personal gain.

Furthermore, as the main topic of discussion in this thesis is online DA and online consumer protection whether local or international, this section also examined (to a certain extent) Australian protection law, private international law, cyber crime and E-commerce law. This

chapter only briefly touched upon these laws, as Chapters Seven and Eight will discuss in more depth these laws and their implications for cyber-consumer protection. .

The following chapter focuses on the concepts of DA from the legal and behavioural dimensions in order to determine the consumer's cognitive process when exposed to a deceptive advertisement.

CHAPTER 3

RESEARCH ISSUES: ADVERTISING DECEPTION

3.1 Introduction

Previous chapters mentioned the cognitive processes which are considered to limit the perception or recognition of DA. This chapter examines in more detail these cognitive processes: exposure to the deceptive advertising, attention, comprehension and prior knowledge, fusion (interest) and processes of belief formation. Questions are raised about the ways in which DA influences the consumer's purchasing decisions.

Some researchers have tried to interpret the effect of DA on purchasing decisions based on the resolutions issued by the FTC, as the hub of the legal dimension, and based on the fact that the FTC issues resolutions deeming a given ad as being deceptive as a result of applying one of the criteria of deception to the ads (ftc.gov, 1971). This is done based on a certain assessment of the effect that the advertising deception has on the consumer's purchasing decisions or the actions taken by the consumer.

Also, this section offers some contributions in an effort to interpret the effect of DA on the consumer's purchasing decisions, from a behavioural perspective or dimension, where these contributions depend upon the Multi Attribute Model of Attitude and processing of the information implied in the DA message. These contributions require discussion, in order to establish a framework to determine the effect of DA on consumers' purchasing decisions.

In light of the above, this chapter considers the following points:

- The effects of DA on purchasing decisions: the interpretation of the legal dimension.

- The effects of DA on purchasing decisions: the interpretation of the behavioural dimension.

Below is a detailed discussion of the suggested frameworks for ascertaining the effects of advertising deception on consumer purchasing decisions.

3.2 The effects of deceptive advertising on purchasing decisions: interpretation of the legal dimension

The legal dimension and the measurement of advertising deception have been mentioned previously.

In discussing the legal dimension, and defining and measuring advertising deception, it became clear that the most apparent shortcoming of this dimension was that it did not take into consideration the consumer's point of view concerning DA.

In facing the methodological shortcomings of dealing with advertising deception, the FTC declared its Advertising Substantiation Program in 1971. This program did not achieve its intended objective — limiting the practice of advertising deception — because manufacturers resorted to testimonies of product experts to support the advertising claims. In time, it became clear that these testimonies were mere promotions and did not express facts about qualities of the product (ftc.com, 1971).

In order to prove the existence of advertising deception, the FTC then resorted to considering evidence from consumers, maintaining that such evidence complements the opinions of product experts, but is not a substitute for them.

However, instead of taking into account the important and effective role played by the cognitive processes of consumers, the FTC resorted to evidence in a manner that allowed consumers to make the judgment that DA was deliberately intended. This dragged the FTC into lawsuits filed by manufacturers and vendors. The FTC used questionnaires addressed to the consumer which consisted of questions requiring ‘yes’ or ‘no’ responses, which encourages the consumer’s natural tendency to answer ‘yes’ (yes-saying bias) (ftc.gov, 1971).

In order to address the shortcomings of the FTC’s process of determining DA, and so as to reach a better understanding of the consumer’s opinion in judging them, the FTC sought the help of researchers in the field of behavioural sciences to work with its experts in determining DA.

Preston (1987), working with the FTC, reached the conclusion that the interpretation of the effect of the DA on the consumer’s purchasing decision is determined by the following aspects.

First, the probable effect of the advertising deception is based upon its effect on the cognitive processes through which the consumer reaches an understanding and an interpretation of the advertising message.

Second, the cognitive processes of the consumer to understand and interpret the advertising message becomes more complicated as the advertising message contains more implied claims, or describes the evaluative traits of the advertised product. They are those intangible traits which the judgment of the extent of their availability in the product is subject to the consumer’s evaluation, and, accordingly, judgments passed on them differ from one consumer to another.

It is worth mentioning that Preston's (1987) interpretation of the effect of advertising deception on the consumer's decision clarified the importance of studying cognitive processes as these determine the effect of the DA message, and that the purchasing decisions indicate the cognitive processes employed by the consumer after exposure to the DA message. This means that it is possible to predict the purchasing decisions of a consumer if the pattern of the cognitive processes, or the way in which the DA message is received by the consumer, is determined.

Preston's (1987) viewpoint can be criticised on the following points.

First, Preston maintains that cognitive processes are influenced by the DA message in the sense that they determine the purchasing decision perceiving the advertising deception; it is not the final stage which determines the effect of the advertising deception on the consumer's purchasing decision.

Second, Preston does not specifically define the cognitive processes that are subjected to the effect of the DA message, and therefore determine the effect of the DA message, which in return influences the purchasing decisions taken by the consumer.

Therefore, we can say that the use of the legal dimension only, when interpreting the effect of the advertising deception on the consumer's purchasing decision, is inadequate and unreliable as a measure of advertising deception. Instead of acknowledging the fact that Preston (1987) is a marketing researcher, the FTC used his interpretation as a basis for its viewpoint regarding the influence that advertising deception has on the consumer's decisions and actions (ftc.gov, 1971).

3.3 The effects of deceptive advertising on purchasing decisions: interpretation of the behavioural dimension

Given the ambiguous interpretation offered by the legal dimension concerning the ways in which DA influences purchasing decisions, some researchers have tried to interpret the effect of advertising deception on the purchasing decisions taken by consumers, or on actions taken by consumers, after exposure to the DA message. Some of these contributions are discussed below.

According to the multidimensional approach, the consumer's attitude to a product is determined by the sum of the interactions between the beliefs of the correlations between certain traits and a certain product, and the consumer's assessment of the relative importance these traits represent to him/her (Heafner, 1972).

In light of this model, the effect of advertising deception on the purchasing decision is realised through the DA message in one of the following dimensions.

In the first dimension, the DA message leads to forming a certain belief of the existence of a connection between the subject matter (product) of the deceptive message and a certain trait; in this case, belief increases in the formula. The DA message raises the tendency towards purchasing the product and, accordingly, influences purchasing decisions (Heafner, 1972).

In the second dimension, the DA message leads to the consumer making a higher estimation of the relative importance of a certain trait of the subject matter (product) in a DA message. The DA message exaggerates the relative importance of certain traits of the advertised product, so the relative importance of the belief increases in the formula. This leads also to a

greater tendency to buy the product and therefore influences the purchasing decision (Heafner, 1972).

Gardner's (1975) opinion significantly contributes to determining a method (the standard belief method) for measuring deception in the ad. However, there is a difference between the consumer perceiving a certain degree of deception, and Gardner's contribution, which is nevertheless still useful for measuring advertising deception.

Moreover, if we conclude that Gardner's (1975) opinion is sound, we recognise that the influence of the DA's message on the consumer's purchasing decision is achieved by creating tendencies to purchase the product, which in turn is the result of the interaction between the belief about certain features of the product, and the extent to which these are important to the consumer.

In this case, this assumes that tendencies to purchase the product have to be shaped before the purchasing decision is made. This is true in the case where consumers make a purchasing decision about a product of great interest to them. The consumer, in such a case, absorbs the information to a maximum extent before making the purchasing decision. Conversely, this does not seem to be the case when consumers are making decisions about products that interest them to a lesser extent. Accordingly, prior to making a purchasing decision, the consumer uses the information to a minimum extent and does not form any tendencies towards purchasing the product.

In this case, it is difficult to determine the effect of the DA message on the forming of tendencies. That is why we consider Gardner's (1985) viewpoint inadequate as a means of interpreting the influence that advertising deception has on purchasing decisions; instead, we acknowledge his contribution of a method by which to measure advertising deception.

In the same vein, Armstrong (1975) interprets the way in which the DA affects purchasing decisions; he determined the influence of advertising deception on purchasing decisions by considering the effect of the DA message in terms of the following dimensions.

The first dimension influences the perception processes of the advertising message or exposure to the DA message. Accordingly, perception influences the purchasing decision (Armstrong, 1975).

The second dimension influences the processes of creating beliefs which result from the consumer's interaction with the contents of the advertising message. Hence, the influence of the DA on the purchasing decision is determined by the influence of the DA message, either on the consumer's perception of the advertising deception, or on the beliefs created as a result of exposure to the DA message, or as a result of their interaction (Armstrong, 1975).

The interpretation offered by Armstrong (1975) about the influence of the advertising message on purchasing decisions added a new aspect to the study of advertising deception, that of perception, indicating the consumer's exposure to the DA message. Unless the consumer is exposed to the DA message, that DA message cannot influence the purchasing decision.

One aspect of Armstrong's (1975) interpretation depends on the relative importance that the consumer attributes to the deceptive ad; and not to the relative importance of a certain trait or a set of traits.

This interpretation contributes significantly to the study of the influence of advertising deception on the purchasing decision, where the DA is considered to be deceptive by virtue of the information it contains, or its bogus claims are deceptive because of their influence on

long-term memory. The consumer's purchasing decision is influenced by these processes of perception.

Horton's (1984) refers to several cognitive processes which determine the perception of DA. Instead of the importance of the role played by these processes, the influence advertising deception has on the purchasing decisions exceeds the cognitive processes stage to the stage which directly precedes the actual purchasing. That stage is the creation of purchasing tendencies and intentions. Consequently, Horton's (1984) interpretation of the influence of the advertising deception is inadequate.

3.4 The effects of deceptive advertising on purchasing decisions

Through the aforementioned, it becomes clear that the legal dimension of the ways in which the DA influences the purchasing decisions is not suitable. This is because of the lack of clarity regarding the cognitive processes by which the DA influences the purchasing decisions.

The interpretation of the behavioural dimension of the influence DA has on the purchasing decisions also became clear because the behavioural dimension did not define an integrated framework of the influence DA has on cognitive processes, and therefore the influence that cognitive processes have on purchasing decisions.

Because both the legal and behavioural dimensions are inadequate for the purpose of interpreting the influence that the DA has on purchasing decisions, we suggest a framework through which the influence of the DA on the purchasing decisions could be interpreted.

Figure 3.1 illustrates this framework.

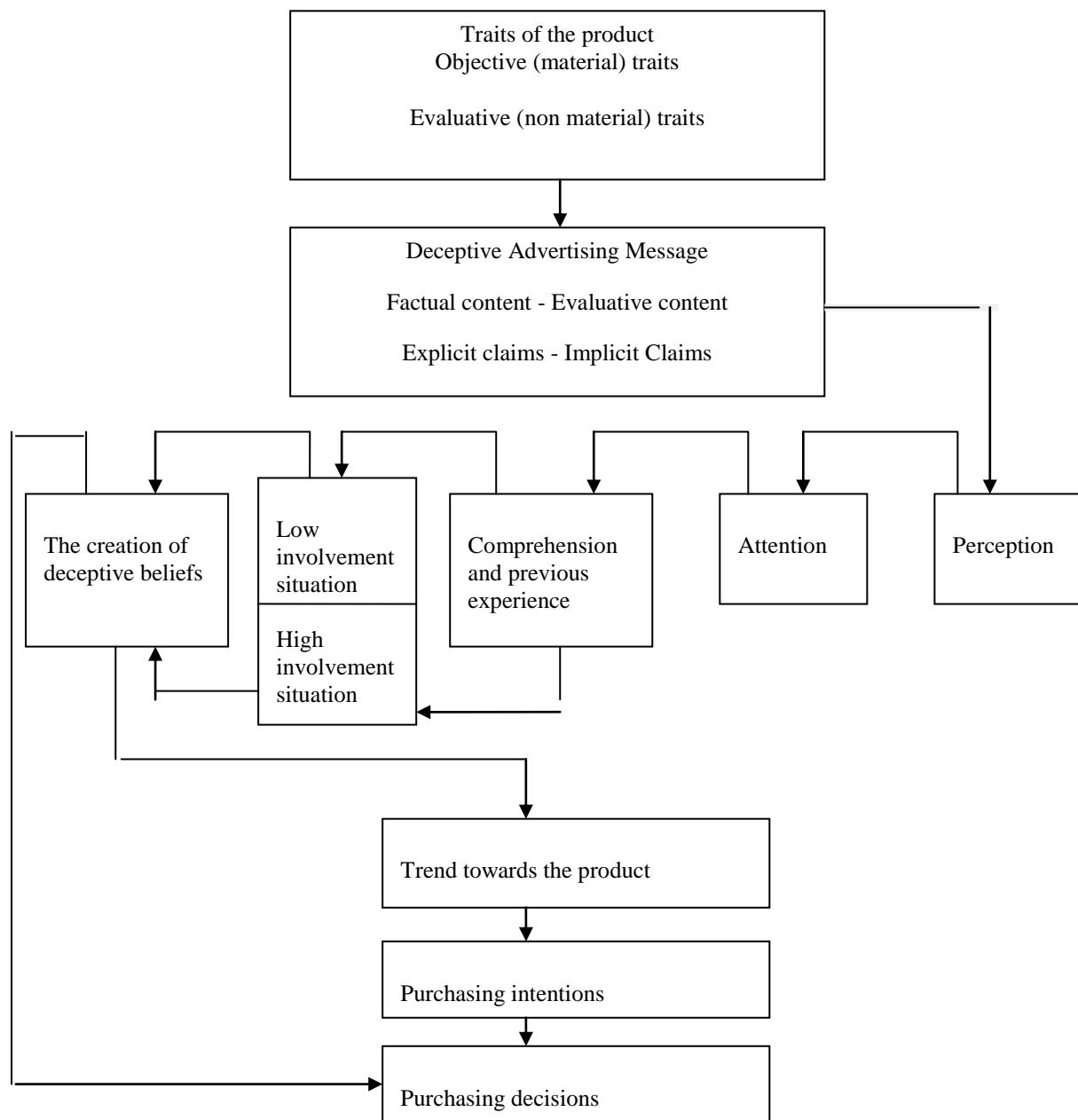


Figure 3.1: Influence of deceptive advertising on consumer purchasing decisions

The framework illustrated in Figure 3.1 focuses on the influences that DA has on the consumer's purchasing decision in the following aspects.

First, the (material) objective traits and then (non-material) evaluative traits of the product influence the process in which the DA message influences the consumer's purchasing

decisions. That is supported by studies concluding that the more material objective the traits were, the lower the chance of the DA message influencing the purchasing decision.

Second, the traits of the DA message, that is, the factual content of the advertising message which focuses on information about the product's material traits, and the evaluative content which focuses upon the evaluative aspects of the product, determine the process by which the DA message affects the purchasing decision. The more the message is built on the factual content regarding the product, the less influence the deceptive message has.

Third, the contents of the cognitive process, which were determined (perception or exposure to the deceptive message, attention to the content of the deceptive message, comprehension of the deceptive message and previous experience with the product in question, the process of creating beliefs), are considered determinants of the consumer's perception of the advertising deception.

Fourth, the integration of the results of the cognitive processes, which were determined in the above-mentioned framework, has to be seen in terms of the influence that each of these cognitive processes, on its own, has on the consumer's perception of the advertising deception. This has already been discussed in this thesis.

Fifth, the integration of the cognitive processes that were determined in the framework and their influence is defined by the content of the advertising message, either the factual content or the evaluative content. The more the advertising message is built on the evaluative content, the more complicated the employment of the cognitive processes become.

Sixth, in the case of low involvement (limited use of information) the influence that advertising deception has on purchasing decisions is more direct. The cognitive processes in this case are subject to the influence of the advertising deception on the purchasing decisions.

Seventh, in the case of high involvement, the advertising deception seeks to influence the purchasing decisions by means of orientation toward the subject matter of the product ad. This orientation, then, creates a purchasing intention to purchase the product, or to perform a certain action in order to purchase that product.

Eighth, multi-attitude models are useful for measuring orientation towards a product; but they cannot be used to determine the influence of the DA message. Instead, it is necessary to determine the influence that the DA message has on the purchasing decisions, and analyse the cognitive processes which precede the processes of creating an attitude, since the DA message might have some influence despite no attitude or tendency being created regarding the product (as is the case in low involvement).

Ninth, the transformation of the trends, which are formed as a result of the cognitive processes which convert perception, understanding and interpretation of the DA message into purchasing intentions, is contingent upon the condition where purchasing intentions are under attitudinal control.

This means that the absence of environmental factors hinder the transformation of the orientation into intention and the decision to purchase the product or to take a certain action regarding the product. When these environmental factors do intervene, the formation of an attitude toward the product is affected by factors other than those defined in the previous framework. It is worth mentioning here that the relationship between attitude and purchasing behaviour merits a study of its own; however, this falls outside the parameters of this thesis. for considerations related to limitations of the research which are not discussed in this thesis.

3.5 Conclusion

This chapter focused on the effect of DA on purchasing decisions from legal and behavioural perspectives, concluding that the interpretation of the legal aspect of the effect which advertising deception has on the purchasing decisions is not adequate, since it does not define the cognitive processes that are involved in the DA message.

Furthermore, the interpretation of the behavioural aspect of the effect of the advertising deception on purchasing decisions is also inadequate because the behavioural aspect does not offer an integrated framework for the effect that advertising deception has on the cognitive process, and consequently, the effect of these cognitive processes on the purchasing decision.

This chapter also offered a suggested framework by which to interpret the effect of the advertising deception on the purchasing decisions, considering that the cognitive process mediates the perception of the advertising deception.

The following chapter discusses whether or not a cyber-consumer who engages in a CCT with a local or foreign vendor, via the Internet or otherwise, has any effective means of seeking redress in the event of any fraudulent behaviour by the vendor in relation to CCT contracts.

CHAPTER FOUR

CONCEPTUAL FRAMEWORK

4.1 Introduction

The consumer's identification of the deceptive aspects of an advertisement is fraught with difficulties, as a result of the producer's practice of presenting the objective (or tangible) aspects of the product, or the subjective (intangible) aspects of the product, or the DA in relation to the results achieved by the product, or the deception resulting from the different offer methods (representation), be it audio, video or graphic (Vishal, 2006).

Moreover, the great boom in production (both goods and services) of all types, and the emergence of new products, all make it more difficult for the consumer to identify aspects of deception in advertisements, especially when the advertisement implies claims related to characteristics of goods and services which the consumer has not used previously, and therefore has limited or no experience with them (Methenitis, 2007; Vishal, 2006).

From the legal perspective, decisions are made about DA following the application of a set of standards to the contents of the advertisement. These standards have been determined in light of previous advertisements which consumers thought were deceptive, or the rulings issued by courts, or by the efforts of scholars in this field established the Federal Trade Commission to monitor the commission extended, later on, to include the deceptive ads (Millstein, 1969; William, 1998).

The legal concept of DA, which was based on decisions issued by the Federal Trade Commission, as the legal assembly which has the right to monitor the deceptive advertisements, was not welcomed by scholars of marketing. Decisions issued by the FTC

were constantly changing; they did not take into account the consumer's awareness of the DA when exposed to the advertisement; consumers vary in their awareness of DA although they have been exposed to the same advertisement (William H. Donahue Jr 1998) (Methenitis, M 2007).

Because the law and the scholars differ in their interpretation of DA, the matter needs to be thoroughly discussed by both parties in order to reach a suitable definition of the behavioural implications of DA (Richards, 1990).

In another dimension, researchers have made contributions in the area of measuring the DA, using various measuring approaches. These need to be discussed in order to determine which is the most appropriate for measuring the DA, and should be based on measuring the behavioural aspects and reflect the nature of deception measurements applied to advertisements.

However, if the advertiser is practising DA, in order to maximise the effectiveness of the advertisement, this raises questions about the extent of the relation between effectiveness of the ad and deception in it, and whether the ad needs to be deceptive in order to be effective. Can an advertisement be effective without the use of deception? (Belch & Belch, 2004).

4.2 Deceptive advertising

An advertisement is any information given to the general public by a seller or manufacturer. It is very important for the advertisement to contain true information and no misleading facts about the product or services; also if the advertisement contains a picture, the picture must reasonably and clearly present the item or product.

For many decades, advertisements have contained either false or misleading information, sending an unclear and deceptive message to the consumer. The advertiser resorts to vague advertising claims, making it difficult to pin down the deception in a direct manner. Also, the advertiser uses tactics to draw the consumer's attention, such as colours, symbols or logos, endorsements and magnitudes in order to make the ad more persuasive, with the intention of influencing the consumer's purchasing decision.

Online advertising has become one of the most common means of advertising, for both business owners and consumers. Because online advertising is not monitored effectively, fraudulent and deceptive acts are rapidly increasing in number and have become a worldwide issue especially for those who are unfamiliar with online shopping; high demand requires stricter guidelines and intensive monitoring to secure online business owners and adequately protect cyber-consumers.

Furthermore, different strategies for online advertising such as banner ads, pop-up ads and online video ads have been intentionally designed to attract a larger number of consumers worldwide; this is one of the main causes of the increasing rate of unsatisfied and deceived consumers. Deceptive vendors have their own lures to attract consumers that include bait-and-switch schemes and blatant strategies.

The majority of internet users who shop online (cyber-consumers) are unaware of the common forms of online DA and lack knowledge in that area, whereas some may have their own suspicions about some of the tactics practised by the advertiser. This worldwide problem has done considerable harm, causing both financial and psychological problems for consumers. In some cases, online fraud is one of the main causes of identity theft; known as phishing schemes, this alone is a very serious crime.

4.3 Cyber legislation and cyber-consumer protection

It is clear that cyber-consumers are not well protected when making an online transaction due to the lack of, or unregulated, legislation. Cyber-consumers making online purchases internationally know only what the vendor tells them—claims may be true or false and the consumer is at high risk. There is currently no law in place to protect CCTs whether local or international. Furthermore, the purpose behind cyber-consumer protection (cyberspace) law is to protect vulnerable cyber-consumers through legislative constraints on deceptive practices; in other words, specific cyber legislation must be incorporated into current law.

4.4 Laws for federated cyber-consumer protection

According to the ACCC, the current laws include consumer protection law, contract law and private international law. However, none of these laws applies to cyber-consumers or CCT. Hence, current laws cannot provide cyber-consumer protection. Now that the Internet has become the main source of shopping for the majority of the global population, the consumer is at a much higher risk. Once the consumer has made an online international transaction, the consumer can be exposed to any type of fraudulent behaviour or deception. Conducting transactions internationally makes it more difficult for the deceived to take further legal action against the deceiver as a result of the lack of online foreign lawyers and online foreign public consumer protection authorities.

4.5 Cyber-consumer cognitive process and behaviour analysis

Cognitive processes determine the way in which the consumer recognizes deception in advertising and online fraudulent schemes. Consumers rely on the advertised message in order to make a purchasing decision, thus, the beliefs defer from one consumer to another.

Previous studies have proven that consumers lack knowledge and awareness in recognising deceptiveness in advertisements, because they are unaware of and unfamiliar with advertisers' deceiving schemes; advertisers have their own tactics to structure the ad and create a message that is open to multiple interpretations by the consumer.

Furthermore, advertisements are presented to the consumer in a form that attempts to brainwash consumers so that they focus on the desired message, which deceives consumers by leading them to overlook the rest of the message.

4.6 Cyber solutions for cyber-consumer protection

Cyber consumers making online international transactions are the most affected in cyberspace for several reasons. The main reason for cyber crime practices is the lack of cyber-consumer protection and non-existent or ignored cyber laws and legislation. For example, any random person can create a website with a fake business name and fake contact details through which to collect consumers' personal information and promote and sell products to the public even though the business does not exist.

Online vendors are not required to register their business before launching a website specifying the service they provide to the public, due to the lack of government legislation. The responsibility for passing and enacting such legislation rests with the government to

ensure that individuals or business owners register their online business or webpage to confirm their legitimacy before placing it online. .

The Internet has become an easy target for cyber criminals to practise their online scams and fraud in order to collect as much as possible personal data and information from cyber-consumers, such as bank account information, credit card details and so on. This fraudulent practice has been occurring for over a decade and is rapidly increasing and dangerously spreading widely across the globe, becoming more and more a major crime that needs to be controlled and reduced rather than increased by the hour. And yet surprisingly, not enough has been done in order to put an end to such crime. Even though the Internet has been around for many years and cyber crime is still practised on a daily basis, there are no government laws that can be applied to address cyber crime and for cyber-consumer protection. Cyber-consumer protection means protecting the consumer beforehand, prior to an online transaction being made, in order to effectively prevent the incidence of online deception or cyber-crime.

In regard to consumer protection, the Australian Trade Practices Act 1974 applies the law and protects consumers' rights only after the fact, that is, after the consumer has been deceived or harmed by fraudulent behaviour. In order to truly uphold consumer rights, the law should protect the consumer from untrustworthy vendors beforehand, thereby preventing any sort of deception or fraudulent behaviour before occurring. This can be done by amending current, or introducing new, guidelines and legislation specifically for consumers online and in realspace.

4.7 Conceptual overview of the Cyber Consumer Protection Framework for the Prevention of Deceptive Advertising

Cyber-consumers are urging for a protection framework to prevent cyber deceptiveness.

In this section, a conceptual overview of the proposed framework is presented. It addresses three objectives.

Objective 1 is to provide a detailed study and analysis of the cognitive processes and behaviours of cyber-consumers and CCT, and provide alerts that help protect consumers from online fraudulent behaviour and deceptiveness when engaging in online consumer transactions, through legal and theoretical perspectives on consumer protection and CCTs as a phenomenon of cyberspace.

Objective 2 is to provide a Cyber Consumer Protection Framework for the prevention of DA and to validate its adequacy and effectiveness, based on the extended existing legislation of redress for cyber-consumer protection at both national and international levels, as well as CCTs.

Objective 3 is to seek a range of potential solutions within a framework on how to prevent DA and how to recover the losses before and after a fraudulent event occurs, including relevant models of laws enacted or proposed by the UN, the EU, the OECD, the US and others with a focus on uniting such model laws in order to address the currently ineffective methods for CCT redress problems, and to assess the likely effectiveness of the various initiatives/solutions (if any) to uniting or unifying such laws.

In order to achieve the thesis objectives, the proposed conceptual framework consists of seven components, discussed in Chapters 5–11. The first part of Figure 3.2 (on this page)

shows the three objectives, with the remainder of Figure 3 (over the page) showing the components.



Figure 3.2: Conceptual framework

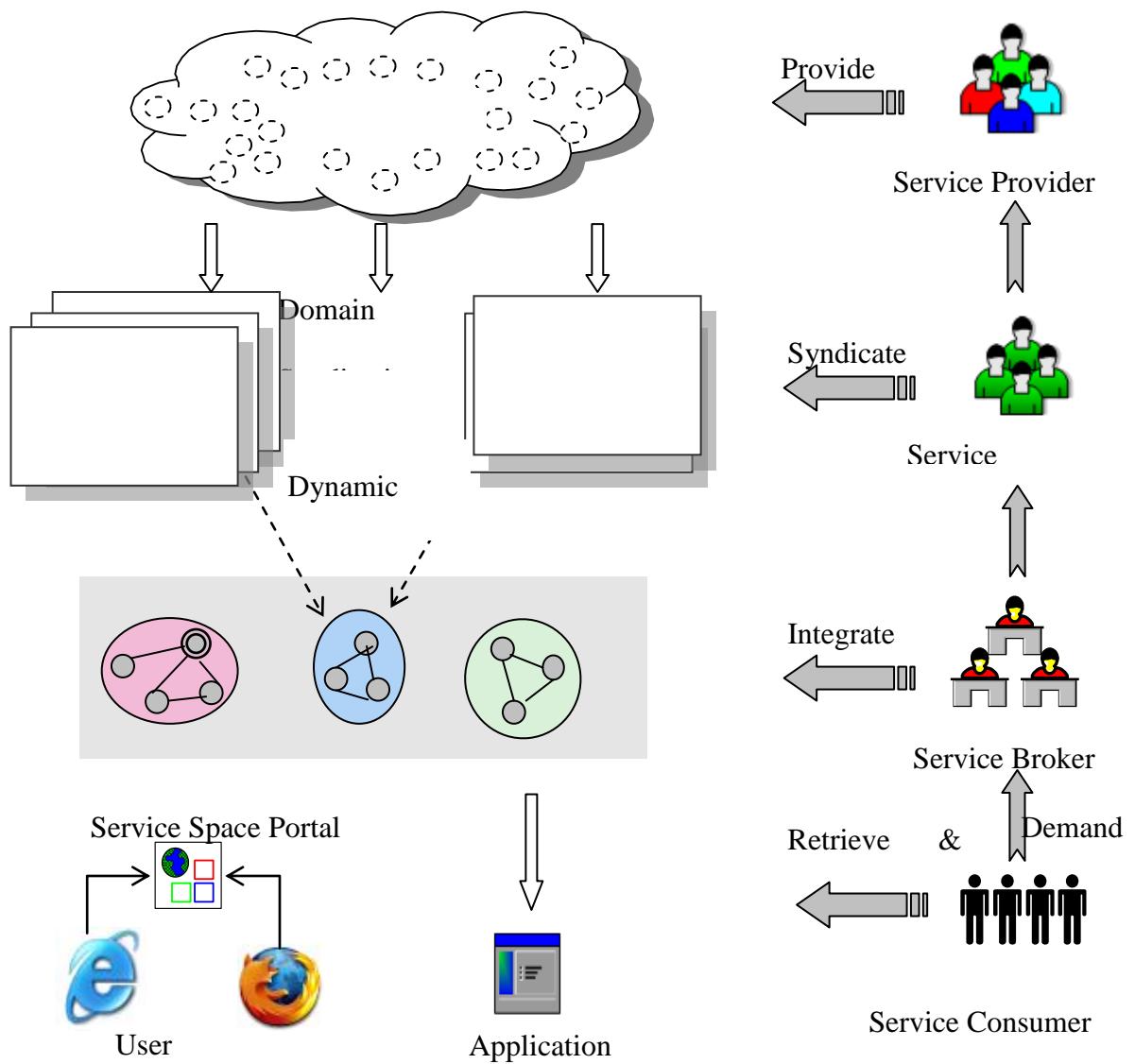


Figure 3.3: Overview of the conceptual proposal of Cyber Consumer Protection Framework for preventing deceptive advertising

4.8 Conclusion

This chapter identified deception in advertising and what makes an ad deceptive in order to attract consumers. Furthermore, this section pointed out the weaknesses in cyber-consumer protection methods, laws and CCT. Current laws do not cover cyber-consumers or CCT. In this section, a Cyber Consumer Protection Framework was developed to help prevent deceptive advertising, addressing the thesis objectives with the aim of arriving at potential solutions and redress methods.

The following chapter discusses further issues related to cyber-consumer protection and the conceptual definition of online DA and cyber-consumer protection.

CHAPTER 5

CONCEPTUAL DEFINITION OF ONLINE DECEPTIVE ADVERTISING AND CYBER CONSUMER PROTECTION

5.1 Introduction

Advertising is used to publicise a product, service, or idea. Many types of advertising are available for the purpose of building brand awareness and increasing product sales. Advertising is present in almost every aspect of daily life.

DA starts when the advertising message, implicitly or explicitly, leads to the formation of deceptive beliefs in consumers. In this case, the advertising message is called a ‘deceptive advertisement’.

The concept of DA is not defined clearly enough, and there is discrepancy of definition between the legal perspective and the behavioural perspective. While the legal side is interested in the act of deception by the advertiser, the behavioural side is interested in the effect the DA message has on the components of cognitive processes, since they are considered determinants of the consumer’s cognition of the advertising deception. Accordingly, the concept of advertising deception needs further study and discussion. DA requires a comprehensive definition which can be applied to any case of advertising deception and the specific deceptive means used by the advertiser.

The way the consumer understands and interprets the advertising message, in light of the context in which it occurs, raises many questions which form the basis of the study in an

effort to create a framework by which the effect of the cognitive processes can be determined as cognitive determinants of the commercial deception.

A consumer's decision to purchase is reached as a result of awareness of many influences. If the DA message was received according to the cognitive structure of the consumer, then we should wonder about the effect of the advertising deception on the consumer's decision to purchase.

There is the need to develop a framework by which we can study the cognitive processes which determine how consumers can identify DAs. This research represents a contribution in this direction.

5.2 Defining deceptive advertising

Taking into consideration the previous efforts in defining DA, from the perspective of behavioural theory, a definition might be introduced which corresponds to both the behavioural and the legal dimensions and takes the following into consideration:

- The definition should focus on the consumer's reaction and not opinions of experts.
- The definition allows the advertiser to use innovative styles in the advertisement.
- The advertiser is allowed to make any claims at all as long as they are true.

In light of the above, a definition of DA should encompass the following understandings:

- The ad includes explicit or implicit claims.
- Those claims are received through the consumer's cognitive processes.

- Those claims lead to the formation of beliefs related to the characteristics of the product which is advertised. Those claims can be determined as false, or as being impossible to prove as facts.
- It is possible that the advertisement has a negative effect on the consumer's behaviour and purchasing decisions.

5.3 Aspects of deceptive advertising

5.3.1 First definition

DA results when the advertisement includes explicit or implicit claims, provided that those claims are received by the consumer's cognitive processes; this means that the naïve or negligent consumer is not considered in determining the deceptive advertisement.

5.3.2 Second definition

The definition relies on beliefs as major determinants of the cognitive processes on the basis that these constitute or play a fundamental part in the consumer's purchasing decisions. (This is discussed in detail in Chapter Five.)

5.3.3 Third definition

The suggested definition treats the DA as being a probability, which accords with the preventive goal of protecting the consumer against DA. Accordingly, the deceptiveness in the advertisement is determined in terms of its probable effect on the consumer, and not its actual effect on the consumer.

5.3.4 Fourth definition

The suggested definition takes into consideration that the formed beliefs, resulting from exposure to DA, play an important part in the consumer's purchasing decisions. By extension, those beliefs which are formed as a result of exposure to DA, but which do not affect the consumer's purchasing decisions, are not included within the scope of DA.

DA is sometimes referred to as misleading advertising or as false advertising—the practice of making claims or statements in advertising a product that are untrue, greatly exaggerated, or unsupportable by the advertised product or service. Although DA can sometimes occur accidentally, the DA label is typically reserved for advertising that is purposely false, incorrect or misleading. This can include print advertising, television and radio commercials, online advertising (offers made through the Internet), and just about every other type of advertising available.

During the relatively intensive popularisation of print and television advertising in the 20th century, there was little regulation and legislation regarding what could be claimed in an advertisement. DA could be used to make claims about a product that were untrue or unfounded. Today, advertisers and manufacturers are strictly required to remain honest in advertising a product, and though the truth may still sometimes be stretched at some point, it is at least more accurate.

The term ‘deceptive’ in advertising claims, whether explicit or implicit implies that the ad becomes deceptive, not due to the information it contains, but when purposely omitting information that should be included, or what is understood from the context or theme which accompanies the advertisement. Though DA may not always be downright illegal, it can often push the boundaries of moral or ethical behaviour. Advertising is the practice of putting the word out on a new or existing product in an attempt to make that product attractive and

known to consumers. The ethical responsibility of advertising is often considered by customers and consumers to be honest, and when people feel that an advertisement has misled them or is deliberately deceiving, the response can be vigorously negative (Kristal, 2002; Richards, 1990).

5.4 Australian Competition and Consumer Commission methodology

According to the methodology of the ACCC, the advertisement is considered deceptive if any of the following apply:

- The claim is false:

The claim mentioned in the advertisement is considered false if it omits the facts related to characteristics of the advertised product (Cohen, 1980).

- The claim is partially true and partially false:

This applies to advertisements which include claims that have more than one meaning, one of which is true, the other being deceiving or false. According to the ACCC, the advertisement is considered to be deceptive, although a part of it is true.

- The claim contains insufficient information:

In this case, the advertisement is considered to be deceptive not because of what it contains, but because the advertising message does not include all necessary information related to any physiological or psychological side-effects of the product. In other words, the ad should (but does not) include ‘reservations’ about the product’s effectiveness, and its uses. Hair or skin care products, for example, should use affirmative disclosure including that the product may

have some side-effects, or that it should be used for a short-term period or on a small area first to test for any allergies which might be aggravated by the use of this product.

- The ad is true, while the proof used to affirm it is false:

Here, the advertisement expresses a fact, but the evidence which is presented to support this fact is false. Therefore, the advertisement makes promises which it cannot guarantee; for example, weight loss products or programs that promise a five-kilogram loss in one week — as the product or program results will vary from one consumer to another, since some may lose less and some may lose more.

- The advertisement is literally or technologically truthful, but the overall effect is false:

This means that the deceptiveness in the advertisement might be produced by means of innuendo, without any blatantly false or deceptive claims. According to the ACCC, some legislation recognises this form of deception when it is deemed that the advertising claims are judged by their ‘general fabric’. As expressed by the Supreme Court: “An advertisement must be judged from its general fabric, not its single thread”.

5.5 Indications of deceptive advertising

Since the advertiser sometimes resorts to using vague advertising claims, which make it difficult to directly recognise DA, previous researchers and ACCC experts have attempted to find alternative ways to define DA.

Cohen (1980), indicates that when the stimulus is vague, the consumer cannot make a differentiation or an assessment of the product’s characteristics by means of assessment criteria (price, performance, maintenance cost), but can make a differentiation by evaluating

the alternatives or the surrogate indicators which exist in the environment or the purchasing attitude that determines the purchasing decision.

Hence, any deception in the advertisement can be recognised if the consumer is aware of the indicators by making comparisons between products when comparisons by direct means are difficult (Methenitis, 2007).

Signifying indicators

The indicators that can signify deception in advertising include one or more of the following: colours, symbols, endorsements, magnitudes and claims about the product's uniqueness:

- Colours are considered to have an individual or personal connection with the consumer.
In the advertisement, colours could be used to indicate that the product has certain benefits or advantages.

For example, advertising a synthetic detergent product as having blue granules or being a blue colour, assumes that the consumer believes the colour connotes the detergent's superior performance (Richards, 1990).



Picture 1: Sample showing usage of colours

- Individuals use symbols repeatedly as an evaluative alternative to measuring the advantages connected with a certain product or to evaluate the existence of certain characteristics of a product. Symbol operations include that the individual, in an arbitrary manner, arrives at certain meanings through symbols (Cohen, 1980).

Levey (1968) also sees that some advertisers attempt to sell their symbol, either in a planned or unplanned manner, in the same way that other advertisers sell actual products. He sees that it is important to symbolise the product in a planned manner.

Bonnie and Robert (1987) conclude that there is a high proportion of deception in the names of products, and their connected logos, and that the deception in the names of products and the logos used to distinguish the product will represent one of the advertising deceptions in the future.

This thesis finds that deception practised through the use of the logo is an implicit deception resulting from the association made by the consumer between the advertised logo and certain product features, if the logo is used to distinguish the product led to deception of the consumer.



Picture 2: Sample Symbols/Logos

- The advertiser resorts to the use of endorsements which accompany the advertisement's message, in order to influence the consumer's reception of the message advertised.

Researchers indicate that the higher the consumer awareness of the credibility of the source of the advertising, the more receptive he becomes to the advertising, and the more influence the advertising has on the consumer's behaviour (Carolyn, 1994).



Picture 3: Example of an Endorsement

A deception is practised on the consumer if the ad contains false endorsements which support the existence of certain characteristics. . The difficulty of those endorsements arises as a source of deception in the ad where those endorsements depend on preference and personal opinion (Belch & Belch, 2004).



Picture 4: Example of an Endorsement

- Magnitude indicates the personal appraisal of the individual within the framework of the whole range of the magnitude. This means the individual determines his adaptation level relative to a certain magnitude depending on the range of value recognised by the individual.

Accordingly, it is possible for a judgment or estimation about the importance of a certain variable to be made in light of the ‘frame of reference’ or the range of value within which the estimation was done.

- Uniqueness claims are those that maintain that the advertised product is the only product which has the advertised characteristics. It also means that it is the only product which offers a certain service or which possesses a certain trait (Wilkes & Wilcox, 1974).

The FTC considers that the phrases related to traits or quality of the product ‘imply uniqueness’ if they were formulated in a manner hinting at or inspiring uniqueness of these qualities or traits.

An example is when three products are used for the same purpose but each is advertised as if its traits are unique, although these traits are also characteristic of the others. The study concludes that each of the three products has the same fruits, but the way in which each is advertised misleads the consumer into thinking that the product has unique features; hence, a deceptive impression has been created by the advertiser (Wilkes & Wilcox, 1974).



Picture 5: Examples showing claims of uniqueness

Thus, in the case of monopolistic competition, which prevails in some product markets, producers seek to make their products distinctive, in terms of either their features or their quality, regardless of the fact that essentially they have the same characteristics as other similar products, and are therefore not unique at all. Accordingly, the advertising claim that such products are one of a kind is deceptive, unless it is really supported with objective evidence.

5.7 The effects of deceptive advertising on purchasing decisions

From the aforementioned, it becomes clear that the legal dimension of the ways in which DA influences purchasing decisions is not suitable. This is because of the lack of clarity of the cognitive processes which determine how DA influences purchasing decisions.

It becomes clear, also, that the interpretation of behavioural dimensions influences the effect that DA has on purchasing decisions. That is because the behavioural dimension does not provide an integrated framework of the influence DA has on cognitive processes and, accordingly, the influence cognitive processes have on purchasing decisions.

In light of the unsuitability of the legal dimension in interpreting the influence DA has on purchasing decisions, and the inadequacy of the behavioural dimension in interpreting the influence that DA has on purchasing decisions, here, a framework is proposed by which the influence of DA on purchasing decisions could be interpreted.

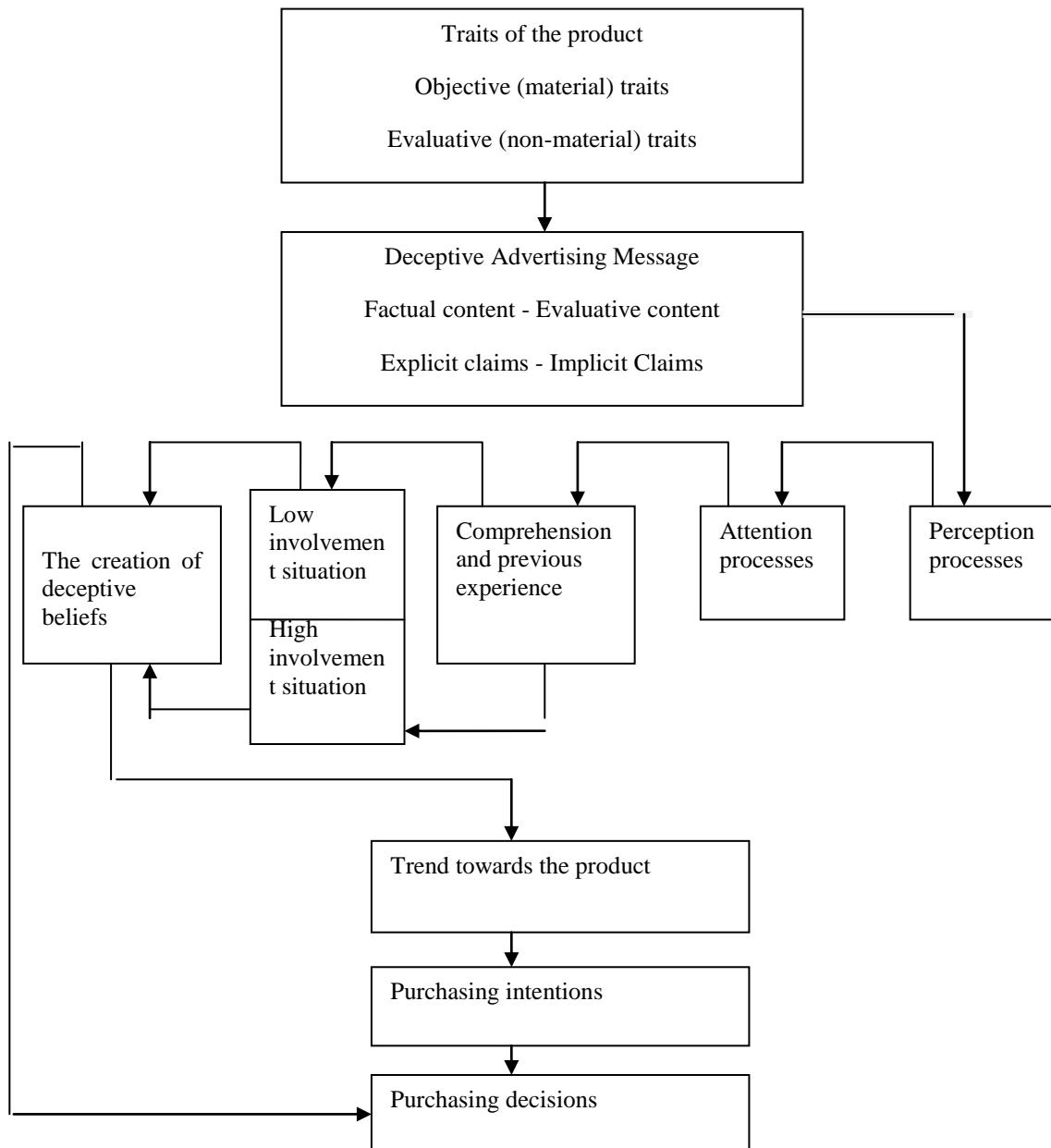


Figure 5.1: Influences of deceptive advertising on consumers' purchasing decisions

5.8 Online deceptive advertising

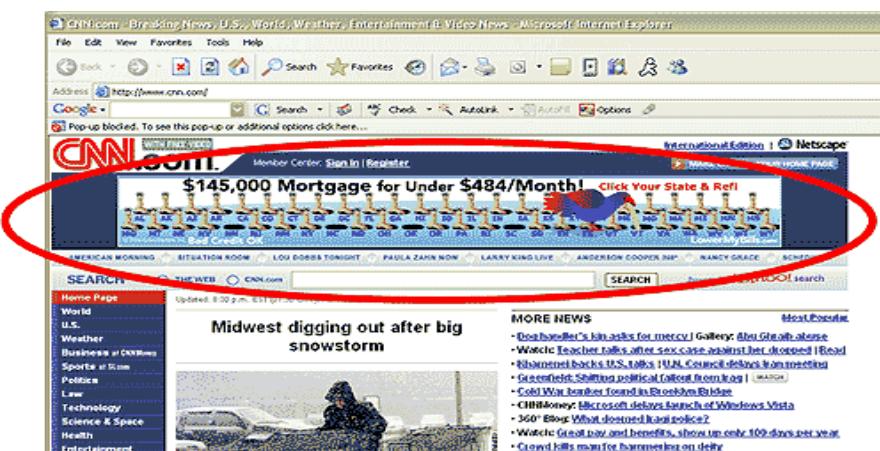
Online advertising and business websites are key elements of modern integrated advertising. There are many different online advertising formats including banners, ads that look like website content and online video ads. Banner ads are like the billboards of the offline world; they are traditional and effective methods of advertising that most people expect to see. Ads disguised as online content can be deceiving and misleading, especially for consumers

unfamiliar with online shopping. Compared to many other online advertising strategies, video ads are relatively new. In addition, pop-up ads and interstitial ads are common online advertising strategies.

5.9 Common strategies for online advertising

5.9.1 Banner ads

Banner ads have become very common but raise concerns for advertisers and potential customers. Sometimes, the ads are placed next to the logo of the website, such that it does not interfere with the rest of the page's content. In this way, the website's logo is no longer the centre of attention; rather, the ad itself draws the viewer's attention. Plain banner ads are one of the less obtrusive online advertising formats.



Picture 6: Example of a Banner Ad

Ads that look like content are among the most common online advertising formats. They are intentionally designed to blend in with or match the layout of the website so viewers will be distracted and interact with the ad and accidentally leave the original website. These ads are popular because their deceptiveness/tactics can lead to a larger mailing list or purchase for the advertiser.

Banner Ads will be seen on websites relevant to your industry and clientele.



Our contemporary banner advertisements provoke your potential clients' buying interests, sparking their desire for your products in a powerful and interactive way, allowing direct access to your website!



Picture 7: Examples of Banner Ads

5.9.2 Online video advertisements

Online video advertisements have taken the place of some banner ads. These types of advertisements are difficult to ignore because the audio and sound can rapidly catch one's attention. Some advertisers make it very difficult for the video to be paused or exited, leaving the website visitors no choice but to view or hear the ad to the end.



Picture 8: Example of Video Ad

5.9.3 Pop-up ads

Pop-up ads are advertisements that usually appear in a separate window. A website might have one or more pop-ups, each advertising a different product or service. This kind of online advertising can be minimised with a pop-up blocker, but not all pop-ups can be blocked. Some studies show that website viewers consider pop-up ads as one of the most distracting and annoying types of online advertising formats.



Picture 9: A Pop-Up Ad

Also known as in-between ads, interstitial advertisements interrupt the viewing of a website to introduce a product, service, or another website. These ads take over the entire page, and the viewer is usually asked to click ‘next’ to continue doing what they came for. Sometimes this kind of ad includes videos and does not give the viewer the option to skip it. Like most ads, interstitial advertisements can be unwelcome if not wisely integrated.

5.10 Deceiving advertisers

A precise definition of deceptive advertisers, also known as unfair advertisers, can be very lengthy and full of legalese. It basically comes down to exactly what it sounds like—business practices that take advantage of, or deliberately attempt to deceive, consumers. Common examples of practices by a business that may be considered unfair and deceptive include false or misleading advertising, deceptive pricing, advertising rewards that are not actually awarded, claiming a sponsorship or affiliation that does not exist, and failing to identify the purpose of a telemarketing call.

DA was more recognizable in the past, whereas today it is difficult to determine how regularly it still occurs. Many jurisdictions have laws against DA and consumers now have the opportunity to report advertisers who fail to honour their advertising claims.

A company accused of DA may face some type of penalty. Unfortunately, however, many advertisers are still able to use subtle forms of DA to mislead consumers without facing any legal consequences.

There are a variety of ways by which a company/business can deceive potential customers. Generally, deception occurs when an advertiser misstates or lies outright about its products; but it can also occur when an advertiser fails to disclose a vital fact about its products. A deceptive advertiser can also be guilty of DA when it bases its advertisements on fallacious research. Likewise, discrediting or misrepresenting another company's products can also fall under the heading of DA. Even bait- and-switch schemes, whereby a store lures a consumer in for a product that is unavailable or that is not really selling in the hope of attracting consumers to buy a more expensive product, count as DA.

5.10.1 Bait and switch schemes

The bait-and-switch scheme is a fraudulent sales tactic that is punishable by law, as DA. Although the law forbids this type of deception, it is commonly used, and one can find examples of it in virtually any advertising circular for major department stores, electronics and computer stores, and automobile retailers. The purpose of the bait-and-switch tactic is to attract customers to visit a store or business by advertising very low prices. Once the customer is in the store, the salespeople attempt to offer the customer over-stocked items or items at higher prices.

The bait-and-switch scheme begins with the bait followed by the switch. The bait is a deliberately deceptive advertisement for a product at what seems to be an extremely low cost. Sometimes these products, such as leather lounge suites, are of very low quality. Other times, the price may apply to one specific style or model of an item. In general, the bait is stocked in very low numbers or not available at all branches. In some cases, only one or two of the items found are at the low price, if available at all.

For example, the advertisement below is offering a complete set of glasses for the price of \$59. We all know that each brand and particular model is priced differently. Clearly, the advertisement does not say ‘limited stock only’, ‘available to selected items’ or ‘offer while stock lasts’. The other part to this advertisement is clearly a bait: ‘2 pairs, Low price. Always.’ The message has become confusing; is it something they are promising the consumer always (unlimited offer)? A current sale that is available for a limited time only? Does it exist at all? Also, the interpretation of ‘1 low price’ may vary from one consumer to another.



Picture 10: Example of Bait-and-Switch

The switch begins once the customer has been convinced by the deceptive ad and walks into the retail store. The salesperson will inform the customer that the store has sold out of the

advertised item and will offer a similar item at a higher price. Alternately, the salesperson may push hard to be certain that the customer is convinced that the lower-priced advertised product is of substandard quality and lower value for price, and try to sell a better value/quality product at a higher price.

Bait-and-switch can also be used to attract customers to the retail store in order to try selling unrelated old stock at high prices or any other item purchased at the time. With determination, a customer could ignore the salesperson and purchase the advertised item at the low-price, although the quality of the item should be carefully evaluated before deciding to purchase. One might also want to avoid purchasing other items from a retail store where the prices seem higher than usual. It may be less costly to purchase needed items from a store that does not use bait-and-switch schemes.

To avoid prosecution for bait- and-switch schemes, advertisers essentially add in very small print that ‘no rain checks are available’, ‘offer whilst stock lasts’, or’ limited stock available’. The fine print of an advertisement may warn customers that the advertisement is clearly employing a bait-and-switch scheme.

In the case of a true bait-and-switch scam, the store can be sued for fraud. However, such lawsuits are frequently not successfully resolved without a great deal of time and documentation. What customers can do to lessen their likelihood of becoming victims of bait-and-switch schemes is to report this activity to the ACCC. Reports can be made over the Internet, and can usually be completed within a few minutes. The ACCC keeps records of companies with significant customer complaints. Evaluating an ACCC report on a retailer can help a consumer to decide whether s/he wants to plough through the bait-and-switch schemes of a store, or give their business to more deserving retailers.

Furthermore, while many advertisers are careful to avoid blatant DA, some companies subtly deceive on a regular basis. Unfortunately, many companies are able to get away with this behaviour.

Thus, before a company faces legal consequences, a consumer or competitor must prove that the company made a false statement, that the statement was deceptive, and that the statement could influence decisions to buy. Likewise, the party who files the claim must also demonstrate that the false advertising affected them or that they will probably be affected in some way. Since plaintiffs in circumstances of DA have to prove their cases, subtle forms of this deception often slip through unreported.

For example, the following ad promises longer-looking lashes and 70 per cent more lash lift. Clearly, the ad is false and misleading. Below are two pictures, the mascara ad and another picture of the same model used in the ad. It is clear that the model in the advertisement is either wearing fake lashes or the ad was photo shopped.



Picture 11: Example of Bait-and-Switch Advertising

5.10.2 Blatant deceptive advertising

Blatant cases of DA are often less common in countries that have laws against it. In the past, it was far more common for advertisers to make outrageous claims about their products since they did not have to fear any sort of legal punishment. Many years ago, an advertiser for instance, might claim that his products could make a person taller or guarantee results that were not possible or likely to be proven, whereas today advertisers generally find it more difficult to get away without having to face any legal punishment, because deceived consumers and competitors have the right by law to report any deceptive act or false claim and bring legal action against the advertiser. It is also important to note, however, that blatant DA is still common in countries that lack enforceable laws against it.

Advertising that is considered false, misleading, or deceptive is a violation of the law. Advertisers, for example, cannot make claims that they know to be untrue. Advertisers may also not be allowed to claim sponsorship or endorsement of a product that they do not actually have. In addition, sales tactics where one product is advertised but the seller really only has a different product available for sale may also be considered an unfair and DA. An example of blatant advertising is shown below.



Picture 12: Example of Blatant Advertising

The advertisement above shows a cosmetic product that is well-known worldwide. The product claims to be an anti-wrinkle and anti-aging facial cream that keeps a woman looking younger. Clearly the real-life picture of the same model is sending a false and misleading message. There are obviously very significant differences between the two pictures of the model. It is obvious that a lot of editing of the model's face using sophisticated computer software such as Photo Editor or Photoshop makes the product's message appear more truthful and authentic.

5.11 Cyber-consumer

In the past, a consumer was responsible for understanding what he or she was buying and under what terms. Known as *caveat emptor*, a Latin term meaning ‘let the buyer beware,’ this perspective allowed sellers to use any schemes available to convince a potential buyer to purchase their goods or services. Eventually, jurisdictions around the world began to enact legislation aimed at protecting consumers by declaring many practices to be deceptive. Jurisdictions differ with regard to what they consider to be deceptive trade practices; however, most focus on practices that are intended to mislead or deceive consumers.

The majority of Internet users who shop online (cyber-consumer) regularly or on a day-to-day basis may have their own suspicions about the most common types of deceptive online advertisements, but according to the ACCC and other watchdog organisations, previous studies have shown that most reported Internet fraud incidents involve the online auction trade. Consumers who have used online auction websites have often reported cases of fraud such as failure to deliver merchandise, deceptive or misleading descriptions of products, and providing false business contact information. Internet fraud involving online auction sales make up at least 60 per cent of all DA reports forwarded to the ACCC.

Successful resolution of online auction Internet fraud can be challenging. Experts in this area suggest that buyers obtain as much contact information as possible when communicating with unknown sellers. Occasionally, a deceptive seller or buyer can be tracked down through a single email address, but investigators prefer physical identifiers such as post office boxes, telephone numbers, street addresses or business licence information. Potential bidders should make an effort to learn as much about a seller as possible before entering into any kind of financial transaction.

An online auction is an online service whereby goods are sold to the highest bidder. By being open to the public, an auction ensures a wide range of bids, and sometimes items auctioned online can fetch surprisingly high prices. The bidders, in turn, create their own market, determining on an individual basis how much they want to pay for a particular item, rather than having prices dictated by the seller. There are a number of various types of auctions conducted around the world.

Generally, an online bid is considered legally binding. This means, a participant agrees to pay the amount which he or she bids. In high-profile auctions, bidders may be asked to deposit money in escrow accounts, or to provide other proofs that they are capable of paying for the items they bid on.

5.12 Forms of online fraud or deception

Other forms of online fraud or deception, such as phishing for personal financial information, are second and third in line after online auction fraud. Although online auction websites take several steps to verify buyer and seller identities, these safeguards are not fool proof. A sophisticated or deceptive website for a non-existent business can be created within days, and often not much contact information is provided; for instance, the only contact information available could be just a free or web-based email address. Online deception or fraud has been applied and practised successfully due to lack of real-world accountability for online transactions.

Another common form of online fraud or deception is identity theft. Some cyber-consumers are unaware of online fraudulent behaviour and may provide an exceptional amount of personal information to any online seller; this information may include a current residential address, personal phone numbers and email addresses.

In most cases, even more personal information, such as bank account information, may be obtained through low-level hacking of unsecured websites. Once an identity thief has enough information to impersonate someone's online persona, all sorts of online fraud can be perpetrated; unauthorised purchases using a victim's credit card are quite common, followed closely by access to private banking information and accounts.

Also, the Nigerian Scam is another form of online fraud, whereby recipients of a gratuitous email are asked to provide a safe bank account to process the transfer of frozen or illegal funds. The scammers usually ask the intended victim for a fee to cover processing costs. Once this initial money has been collected, the scammers disappear after cleaning out the victim's bank account. A similar example of online fraud advises the deceived victim of winning an unknown foreign lottery ticket, convincing the victim that their name was chosen randomly. The scammers promise to forward the winnings in exchange for a substantial processing fee.

Furthermore, phishing is also a very common type of online fraud. This form of scam occurs by way of an email sent to the victim that appears to be from a legitimate online banking service provider. Real-world banks advise recipients that personal information will only be discussed within a branch, and never make a request via email or online. Also, the bank may warn customers of any recent unauthorised purchase or any other suspicious activity that requires immediate action.

When a victim follows the link provided in the fraudulent email, they may be directed to a very sophisticated copy of the original banking website. Any personal account information provided in the submission form goes directly to the scammers, not to the legitimate website owners. These masters of online fraud can create false identities for themselves or sell the information to equally dangerous third parties.

5.13 Defining deceptive advertising

DA can be defined from both legal and behavioural perspectives.

5.13.1 Defining deceptive advertising: the legal dimension

According to the definition provided by the FTC, deception exists when the ad includes a representation, omission, forgetfulness or a negligence regarding certain claims. It is then probable that those claims will tend to deceive the consumer, who is considered to be of sound mind (Cohen & Richards 1990).

Such advertising claims are important because of their effect(s) on the consumer's behaviour and his/her purchasing definition (Cohen & Richards, 1990).

5.13.2 The definition of the Federal Trade Commission

It becomes clear that DA is created through advertising claims, whether explicit or implicit. Accordingly, the ad is deceptive, not due to the information it contains, but because it omits information which should be included, also what is understood from the context or theme, which accompanies the ad (Kristal, 2002; Richards, 1990).

The FTC treats DA as a probability, (i.e. the deception might occur as a result of exposure to the advertising message, without considering the actual emergence of deception, or that harm was inflicted on the consumer) (Moore, 1969).

The definition provided by the FTC includes an important aspect in the legal dimension of DA (Preston & Richards, 1986) pertaining to the rationality and soundness of the consumer's mind. Therefore, if the consumer was unthinking or credulous or even negligent, the legal

protection against DA, in such cases, does not apply. In other words, ‘Let the Consumer Beware’.

Since the FTC, as a federal body, has certain financial allocations, it includes in its definition of DA what makes its monitoring of DA a possibility, so the deception, according to the FTC’s definition, is a “Deception in a Material Respect” (Moore, 1969).

That is, in light of limited financial resources, it is unexpected that the legislation will be responsible for monitoring all advertisements.

The FTC examines the advertising claims, which should be monitored in order to eliminate DA, in light of the following factors (Exkhhardt, 1970):

- The cost of issuing and applying legislation related to monitoring deceptive advertisement claims.
- The number of consumers who might become subject to deception by means of deceptive advertisement claims.

The FTC’s interpretation of deceptive advertisement claims is based on the fact that its goal is to protect society and not to punish the advertiser (Cohen, 1969). Its original role is to prevent fraud, not to exact penalty.

The preventive goal of the FTC means that it does not see the necessity to prove the intention of the advertiser (or the producer) in practising deception in advertisements, since its goal is to protect competition in commerce, thereby protecting both the consumers and the producers, and not to punish the producer for bad intentions (Cohen, 1969).

Haefner (1972) depended on specific product experts to study deception in the ad. He identifies deception in the ad as the degree of incredibility of the ad, which should be determined by an unbiased expert.

Heafner's (1972) methodology, which depends on product experts determining deception, makes this definition of DA untenable, since it does not take into consideration the cognitive aspects of the consumer when confronted with DA.

Webster (1974) introduced a definition of DA suitable for the methodology of the FTC. In determining the DA, Webster saw deception as "The act of misleading through falsehood and misrepresentation" (Webster, 1974)

This definition ignores a major aspect of deception in the ad, as it focuses on the deceptive act performed by the advertiser, without considering how this influences the consumer. Generally, the criticisms of the methodology of the FTC also apply to this definition.

The legal dimension in the legislation of DA is focused on a group of criteria which are used to prove the ability of advertising claims to deceive to consumer. Those criteria might be direct or through alternatives of measuring deception in the ad (Cohen, 1969).

In order to provide consumer protection, there are a number of laws that need to be taken into consideration including consumer protection (Australia), private international law, cyber crime and e-commerce.

5.14 Conclusion

This chapter focused on discussing the interpretations of DA generally, and the different types of DA and their effects on consumer purchasing decisions.

It also considered online DA and described various fraudulent schemes, the effects these have on cyber-consumers and the relationship between an advertisement's deceptive message and the effects this has on consumers' purchasing decisions.

This chapter concluded that it is not necessary for advertisements to include elements of deception in order to effectively transmit their messages. Non-deceptive advertisements can be effective, and this will be for both the short and long term. However, the effectiveness of a deceptive advertisement message will be only for the short term.

This chapter also offered a suggested framework to interpret the effect of the advertising deception on the purchasing decisions, taking into consideration that the cognitive process mediates the perception of the advertising deception.

In the following chapter, advertising deception is identified and its relationship with consumer behavioural and legal trends is discussed.

CHAPTER 6

NEW CYBER LEGISLATION: LIBERTARIANISM VERSUS INTERVENTIONISM

6.1 Introduction

This chapter discusses whether or not a cyber-consumer who engages in a CCT with a local or foreign vendor, via the Internet or otherwise, has any effective means of redress in the event of non-delivery or wrong delivery of goods or any fraudulent behaviour by the vendor in relation to CCT contracts.

This chapter also explains the need for protection of consumers both generally and in cyberspace. ‘Consumer protection’, is closely related to the thesis topic of redress for CCTs, and is in fact the wider context for the thesis topic.

This chapter will offer a range of justifications for, and approaches to, realspace and cyberspace regulation for consumer redress/protection and other purposes. Each justification and approach can be classified as either ‘libertarianism’ or ‘interventionism’, defined below.

This chapter describes how the conflict between libertarianism and interventionism is manifested in the debate about the regulation of cyberspace—about who should regulate cyberspace, if anyone at all, and how. It presents practical examples from the literature of libertarian and interventionist solutions to the problems of cyberspace regulation.

It is established in this chapter that, for the purposes of protecting consumers engaging in low-value CCTs, unless the libertarians can solve their enforcement problems, the only truly cost-effective solutions will be those proposed by the interventionists. As Perritt (2000)

argues, self-regulation will not be acceptable in the long run unless it is backed up by real sanctions for violators and unless the ground rules within the self-regulatory regime are appropriately linked with widely-shared norms of conduct.

The Internet now makes it possible and easy for retailers to supply consumer goods internationally. There is currently no law to effectively protect CCTs, especially low-value CCTs. Further, aside from the fact that shopping in the global market made available by the Internet until a better vendor is found is inefficient for vendors, the focus here is on average consumers. In any event, consumers often know only what vendors tell them, hence the ‘lack of information’ justification for consumer protection. Added to this is the practical point that retailers probably are unlikely to become consumer-friendly simply because a few consumers may shop around.

Thus, unregulated or under-regulated market forces will not financially protect CCTs, generally speaking, and certainly not in respect of pre-transaction problems. Thus interventionist solutions—the aim of which, consistent with the purpose behind consumer-protection law generally, is to protect relatively vulnerable consumers through legislative constraints against deceiving practice of vendors—are seen as preferable where there are the effectiveness and legal certainty of cyberspace self-ordering is limited, and especially where some aspects of the performance of CCTs necessarily occur in realspace and beyond the influence of any potentially self-regulated cyberspace.

This chapter considers why consumers should be provided with any sort of remedy at all, and suggests where an actual effective remedy for non-delivery or wrong-delivery in CCTs might be located within the existing regulatory framework. It begins with a consideration of who a ‘consumer’ is, as this is an important element of the definition and assessment of remedies for CCTs. This is the case not only because of the general nature of the consumer as a ‘non-

commercial' party, but also because the monetary scope of a consumer transaction affects the fundamental relationship, which is assessed by the methodology proposed later. Further, the definition and consideration of key terminology in this chapter is an important step in preparing the tools needed to analyse the problem, to accurately report findings and to accurately describe potential solutions.

6.2 Consumers

What is a ‘consumer’? Dictionary definitions of the term include “one who uses a commodity or service for a non-commercial purpose” (Butterworths, 2002), “one that acquires goods or services for direct use or ownership rather than for resale or use in production and manufacturing” (Dictionary.com), and “a person who buys a product or service for personal use” (AskOxford.com). According to Oughton (1991), a consumer could also be either “an individual not acting in a business capacity”, or “a supplier acting [as a consumer] in the course of a business”.

Goldring (1993) cites Section 4B of the Trade Practices Act, which initially defined a consumer as any person acquiring goods or services at a price of \$15,000 or less, and notes that the dollar amount was increased to \$40,000 by 1986 to provide additional protection for small business purchasers; note also that as at 1998, Section 4B of the Act allows the amount of \$40,000 to be exceeded if the goods or services purchased were of a kind ordinarily acquired for personal, domestic, or household consumption and the consumer did not acquire the goods or services for the purpose of re-supply or to use in trade or commerce.

These definitions are basically similar; that is, a consumer, for legal purposes, is the ultimate end user of goods or services.

This thesis includes all of the above ideas regarding the definition of a consumer. For the purpose of this thesis, a consumer is defined as one who purchases goods or services for personal, domestic or small business consumption. ‘Business’ is included because the justification for the provision of protection to individuals engaging in effective redress for low-value transactions applies equally to small businesses.

Also, this thesis incorporates the commonality of the definitions as well as incorporating and not distinguishing between the semantic differences such as one who *uses* a commodity or service as opposed to one who *acquires* goods or services; and incorporates the various definitions which, in prescribed circumstances, allow businesses to act (and be treated) as consumers.

The rationale for this broad approach is so that a remedy for a failed CCT should not be unavailable merely because of a trivial technical/semantic difference between definitions concerning what a consumer is.

6.3 Cyber-consumer protection

To establish the relevance of this section, it is worthwhile at this point to recall the distinction drawn between cyber-consumer redress and cyber-consumer protection. Redress, in this thesis, means any method provided by any of the law models considered here by which a cyber-consumer who is an aggrieved party to a CCT would seek a remedy from a merchant for non-delivery, wrong delivery of goods or fraudulent behaviour. Redress is the major concern in this thesis, rather than the wider but related issue of cyber-consumer protection.

Cyber-consumer protection is a broader concept and covers issues of regulation of the bargaining phase and regulation of contract terms as well as access to justice issues. Thus,

redress and protection are related but they are not the same. For example, if there is greater protection through uniform and implied terms, then arguably there will be fewer disputes and these will be less costly because there will be no need for arguments over private international law rules on applicable law.

Thus, there is a strong argument that issues of effective redress for CCTs should not be considered in isolation from the unequivocal issues of consumer protection law for CCTs. This link between redress and protection is the context for justifications for consumer protection law, in both realspace and cyberspace.

Taperall (1974) notes the fundamental difference between suppliers and consumers, necessitating consumer protection law:

Private individuals are increasingly finding themselves to be in a disadvantageous position in dealing with the business community, attention has been devoted to such matters as the poor quality frequently found in goods and services; the failure to provide adequate information, deceptive practices and the unfairness of many one-sided contracts.

Two elements which justify the intervention of the state in the protection of consumers are implied by this quotation: lack of information and inequality of bargaining power. It suggests that consumers are in a disadvantaged position with respect to business.

Goldring (1993) observes that by the end of the 18th century, what was to become the Sales of Goods Act 1893 (UK) had evolved to govern transactions between merchants with equal economic power between them, and not those involving persuasion by certain “unscrupulous or reckless” suppliers to uninformed consumers. He goes on to say that “by definition, consumers are not equal to the providers of what they consume”.

This view echoes Oughton’s (1991) statement regarding the inequality of bargaining power between supplier and consumer: “a consumer is not in a position of obtaining equality of

bargaining power due to difficulties in obtaining information”, information, that is, about the things supplied by suppliers. Thus, a consumer may have unequal bargaining power *because* he or she suffers from information asymmetry. As noted below, however, there can also be discrete rationales for consumer protection.

Oughton (1991) notes that under legislation such as The Consumer Protection Act 1987 (UK) and The Food and Safety Act 1990 (UK), a supplier of goods and services can be guilty of a criminal offence without proof of any criminal intent. He also adds that the rationale for this is that because of “a general lack of information on the part of consumers, the ability of the consumer to make a prudent shopping decision is diminished”. In other words, consumer protection law compensates for an inequality of bargaining power between the supplier and the consumer, based on differential product knowledge or information.

Oughton (1991) points out:

This inequality, has always existed where suppliers are specialists who tell the consumer only what the supplier wants the consumer to hear – but has actually increased since World War II because of the surge in both the volume and the sophistication of new consumer goods such as television sets, and services such as car servicing, which have become available on the market since that time and regarding which consumers generally would understand less than suppliers. Without the legislative protection of consumers, commerce would suffer from lack of consumer trust.

Regarding lack of information, Coteanu (2005) notes:

It’s detrimental effect on the loss in consumers’ surplus that they experience due to the lack of information on price, terms and conditions, characteristics of product and services and to the difficulties in verifying through experience the performance and the characteristics of product or service advertised and the lack of information in cyber-consumers’ transactions is much worse than in the off-line environment.

At this point, it should be noted that inequality of bargaining power and lack of information are two principal justifications for consumer protection law. A consumer may suffer from

inequality of bargaining power not just because of the lack of information but also where, for example, the transaction is ‘forced’ upon them through a standard form contract presented to the consumer by the vendor. The consumer may be aware of and understand the relevant issues all too well but, because of the circumstances, there may be no real potential for negotiation of terms (Coteanu, 2005).

Furthermore, Ramsay (1989), refers to inequality of bargaining power resulting from “the high transaction costs of redress” and from the high cost of “consumer organization”. These are situations where the consumer has relatively less bargaining power than the vendor because the individual consumer cannot afford the cost of litigation or other means of redress; nor can they afford the costs involved in making arrangements for collective bargaining against dishonourable vendors.

According to Goldring (1993) individual consumers are relatively weak; they are individuals, while suppliers and manufacturers of goods and services these days more often than not are large corporations. This power relationship often causes consumers to feel awed and intimidated when they wish to obtain recourse against a supplier or manufacturer from whom they have acquired something which does not meet their expectations. The obstacles facing them are immense. To talk of a ‘free market’ of equal individuals is absolute nonsense. In very few cases at all can the consumer be said to be the equal of the supplier or the manufacturer.

Coteanu (2005) indicates the inequality of bargaining power in the online world thus: “the authoritarian process of designing terms and conditions which means that the online contracts are prepared by business and imposed on consumers worldwide”.

Also, in justifying the need to protect consumers, we can note the following general points. Apart from the consumer’s ignorance about a product compared to the vendor’s knowledge

about his or her own goods, services and business practices, consumers are also protected from the sly practices and negligence of vendors. They are also protected from their ignorance concerning consumer rights, and ignorance concerning remedies available in the event of legitimate complaint.

It is arguable that there are two classes of justification for consumer protection: express and implied. Express justification is based on either lack of information or inequality of bargaining power at the initial stage of forming a contract, and underpins modern consumer protection laws, that is, laws which post-date the establishment of those theoretical justifications. An example of such a law is Section 52 of the Trade Practices Act which prohibits misleading and deceptive conduct of a corporation engaged in trade or commerce.

To clarify implied justification, it should be noted that the general right to a remedy for abuses concerns a real remedy not a theoretical one. Therefore, any remedy which, in practical terms, is generally beyond the reach of the average consumer for reasons of any one or more of cost, difficulty of enforcement or complexity, would not be any kind of remedy at all. A cost-effective remedy for under-performing CCTs would therefore be coexistent with the implied justification for intervention in the form of consumer protection.

Finally, a point made at the beginning of this chapter is worth revisiting. It was noted that cost-effective redress, actual or potential, may depend upon state-regulated/interventionist consumer protection, and such intervention needs justification. At this point it can be said that such redress definitely would depend on an interventionist solution, and such solutions are justified. The following section considers the theoretical background a little more closely.

6.4 Libertarianism and interventionism

In this thesis, the terms ‘libertarianism’ and ‘interventionism’ are the labels given to two broad approaches to consumer redress/protection. There is a limited relationship between those approaches here and the broader interventionist/libertarian distinction in separate but associated bodies of theory such as law and economics, and regulatory theory. Moreover, this section examines the role of interventionism in the provision of cost-effective redress for CCTs. As will be seen, only interventionism can resolve the problem since cost-effective redress for CCTs without interventionism is unfeasible.

6.4.1 Libertarianism

Libertarianism, also known as the *laissez-faire* (which originally comes from the French for ‘let things alone’) school of thought, is the socio-economic or political doctrine that an economic system functions best when there is no interference by government because competition between private individuals is more effective than the state as a regulator of economic life (Encyclopedia Columbia, 2005).

Libertarianism is now used generally as a synonym for strict free-market economies, but it is used here as a label for the arguments advanced by those who wish to see cyberspace and realspace free from government intervention (Stanford University, 2007).

6.4.2 Interventionism

Interventionism is used generally as a name for the view that there are some circumstances where regulation through government intervention is justifiable (e.g. consumer law, law of contract), and is used specifically here as a label for the view that the best CCT redress

solutions will be those provided by court-based dispute resolution or, with sufficient enforceability, government-provided alternative dispute resolution methods.

6.4.3 Common ground between libertarianism and interventionism

As defined above, libertarianism and interventionism appear to be mutually exclusive: government is either involved in the regulation of human affairs or it is not. It is acknowledged, however, that some who espouse a libertarian approach may still accept some intervention, where there is no ordering by market forces, for example. Thus, there are libertarians who are partly interventionist and vice-versa.

There are at least two other reasons why the labels are not as mutually exclusive as they initially appear to be.

First, some libertarians may object to interventionism not just because there is any kind of intervention, but because of the reason for the intervention. For example, they may object to intervention because of some perception of an unacceptable political agenda behind the intervention. Such libertarians might then be interventionist in different circumstances.

In this thesis, however, such a distinction is unnecessarily abstract and distracting, as it is the CCT redress methods, as a matter of simple fact or reasonable argument, that are labelled simply as either interventionist or libertarian (e.g. litigation versus transaction insurance, respectively), and each method is judged in terms of its cost-effectiveness according to the framework established in this chapter.

Second, rather than being simple opposites, libertarianism and interventionism represent the ends of a scale of graduated difference between two extremes. For example, there is the protection solution of ‘responsive regulation’ that is located somewhere between the two

extremes because it seeks to make use of private incentives to achieve regulatory goals (Ayres, & Braithwaite, 1992).

Goldring (1996), in favour of interventionism, argues that “consumers do not form a cohesive group, and even if they did, it is doubtful that market forces could in practice provide adequate protection for those who lack the information ... necessary for survival in the modern economy,” and that “governments which are formed from the whole spectrum of political parties accept the necessity for intervention in the market.” Goldring also sees this as a repudiation of the “unreal theories of the free marketeers”.

In contrast, Vogel (1995) argues that the alleged incompatibility between efforts to promote free trade and effective consumer and environmental regulation has been “exaggerated” and “misplaced,” claiming that in fact it can be shown that trade liberalisation efforts can actually improve the effectiveness of consumer and national environmental regulations. “By contrast, ‘eco-protectionism’ threatens both free trade and, ironically, the improvement of environmental quality and consumer protection as well”.

While eco-protectionism is not explained, presumably the reason why eco-protectionism may be so, if it is true, is that international eco-protectionism may diminish free trade and therefore decrease profits, resulting in the need for increased local environmental exploitation to replace profits lost from international trade; but if suppliers are allowed to operate in a free and non-eco-protected market, they will wish to comply with whatever environmentally-conscious consumers reasonably demand in order to enjoy the benefits of continued demand.

According to Vogel (1995), increased trade liberalisation and decreased eco-protectionism increase global economic inter-dependence, which, in turn, must improve global consumer protection through the ‘natural’ forces of supply and demand. The question arises as to

whether such natural forces are sufficiently effective to fulfil the aims of consumer protection as described above.

Vogel (1995) goes on to say that “it is no longer possible to understand the making of consumer regulation exclusively in national terms. Regulation is being shaped more and more by political and economic forces outside the nation state”, suggesting that there might be challenges to satisfying the demands of trans-border consumer protection requirements.

6.5 Libertarianism versus interventionism in cyberspace

As noted earlier, cyberspace is where the vast majority of CCTs are transacted in practice. It is therefore worthwhile to consider ongoing scholarly debate about the governance of cyberspace.

Regarding the development of thinking about cyberspace regulation, Boss (1992) and Ritter (1992) both describe how an issue for the Congress on Uniform Commercial Law in the 21st Century, held in May 1992, was how the United Nations Commission on International Trade Law might promote uniformity in commercial law to stimulate the global trading community, and the potential development of model rules regarding Electronic Data Interchange in connection with international commercial transactions. This shows how early thinking about e-commerce was exclusively in terms of B2B transactions.

Furthermore, as seen from the early 1990s, because e-commerce law arguably had to be developed almost as a result of a legislative gap, an opportunity was seen (by the commentators of the period) to avoid the anticipated need to laboriously unify national e-commerce laws at a later date as none existed.

Therefore, the new e-commerce laws could be unified if, from the start countries, had studied and approached these problems together in order to develop a common understanding upon which a *universal* system could be established (Boss, 1992). However, with the rise of national e-commerce laws since 1992, the opportunity presented by these visionary and idealistic views was missed, and the theoretical advantages of having a harmonious universal system for regulation of B2C transactions remain unfulfilled to this day.

A libertarian theme of interest to Boss (1992) was industry self-regulation through industry-generated codes of conduct. Two criticisms of this were that because commercial entities sometimes try to create their own rules (in the absence of any national or international framework to guide e-commerce), legal uncertainty could result, and such uncertainty could increase the cost of transacting. Further, self-regulation was thought of as inadequate to deal with the legal requirements for writing and signatures in different countries.

By 1994, the narrow focus of the earlier writers had begun to widen, and there was a growing maturity in the cyberspace regulation issue with an escalation of the debate between the interventionists and the libertarians. One of the most debated points of contention was whether cyberspace creates unique legal issues or just the same old issues in a new medium.

Hardy (1994) argues that “in applying existing law to cyberspace old analogies just don’t cut it”. He offered a hybrid view that in some respects there is nothing new in cyberspace; but in other respects, the circumstances of cyberspace do indeed give rise to new legal questions. Despite the question about whether existing laws designed with other media in mind should be applied to the new medium as well, he argued that no legal questions are unique as they all involve human conflict; but when the policy considerations that underlie an existing rule no longer make sense when applied to cyberspace, entirely new rules may be worth having.

Hardy's thinking was not so much in terms of who should regulate cyberspace, but whether the required regulation might be any kind of legally-novel phenomenon.

Hardy (1994) also argued that rapidly-changing technology implied a need for flexible regulation of behaviour and, in some cases, purely decentralised rules should be applicable — where the parties establish their own contractual arrangements to suit themselves rather than using some sort of judicial or legislative resolution.

Another important concern raised by Hardy (1994) is the possible range of responses to the potentially new cyberspace issues. These include legislative responses, case-by-case adjudication for the build-up of precedent, international conventions, citizens creating their own customs, service providers regulating their own patch of cyberspace, and even a modest degree of disorder. In recognition, it can now be seen that *all* of these responses are operative, to some degree or other. Hardy also argues the need for contracts as the “second level of behaviour regulation” after problem avoidance, that is, for contracts as “the basic control mechanism for much cyberspace activity”, but suggests that when contracts cease to function, “the only solution will be a statutory or judicial one”. Hardy's thinking thus contains elements of both libertarianism and interventionism.

To their credit, it now appears that Hardy (1994), Ritter (1992) and Boss (1992) all had at least an unconscious appreciation of the need to take social and technological complexity into account in their analyses, resulting in views consistent with the conclusion that simplistic solutions may be inappropriate. Other issues of importance at that time, beyond the debate regarding the possibility of new laws for cyberspace, included questions about whether cyberspace was itself something new (e.g. a new form of community where people meet and talk, build and define themselves, in ways not possible in realspace), and privacy issues.

By 1996, the early vacillation about whether or not there should be new laws for cyberspace was being attacked vigorously. Johnson and Post (1996) introduced new libertarian perspectives into the debate.

Cyberspace requires a system of rules quite distinct from the laws that regulate physical, geographically-defined territories because global computer-based communications undermine the feasibility and legitimacy of laws based on geographic boundaries, and cyberspace phenomena have no clear parallel in the non-virtual world. Just as a country's jurisprudence reflects its unique historical experience and culture, the law of cyberspace will reflect its special character, which differs markedly from anything else found in the physical world. For example, the law of the Internet must deal with persons who 'exist' in cyberspace only in the form of an e-mail address and whose purported identity may or may not accurately correspond to physical characteristics in the real world. In fact, an e-mail address might not even belong to a single person.

A potentially more important aspect of this new approach, however, was a clarification and a development of the interventionist versus libertarian debate. Interventionists argued that because people involved in cyberspace still actually inhabit realspace, conventional lawmakers and enforcers must continue to remedy problems created in realspace by those acting in cyberspace.

Conversely, libertarians maintained that "questions remain about who sets the rules and how they are enforced. We believe the Net can develop its own effective legal institutions", that "the community of cyber-consumers and service providers is up to the task of developing self-governance" and that "the self-regulating structures of cyberspace seem better suited to dealing with the Net's legal issues" (Johnson, & Post, 1996).

Johnson and Post's (1996) idea of cyberspace may give it the potential to be 'self-regulating'. For example, the current domain name system evolved from decisions made by engineers and the practices of ISPs, and every computer system operator who determines an individual's 'existence' in cyberspace, and who dispenses a password, imposes at least some requirements as conditions of continuing access. System operators have an extremely powerful enforcement tool at their disposal to enforce such rules — banishment — and communities of users have marshalled plenty of enforcement weapons to induce wrongdoers to comply with local conventions.

Thus, for Johnson and Post (1996), engineers, system operators and users are the law-makers and enforcers of cyberspace. This pre-supposes or implies two points, however: firstly, that merchants, for example, who set up stand-alone websites, will (at least) usually be effectively subject to these engineers, system operators and users; and secondly, that all relevant conduct of such parties would be able to be regulated by engineers, system operators and users, assuming that they choose to do so.

Both these points can be logically rebutted. 'Cyberspace' conduct will not always be constantly scrutinised and monitored for unacceptable behaviour, and this appears to be even more the case with a deliberately unregulated cyberspace. Furthermore, the offline performance of cyberspace merchants is simply beyond the purview of such people.

Johnson and Post (1996) cited the medieval *lex mercatoria*, or merchant law, - as a historical precedent for workable self-regulation. Just as the medieval merchants developed their own law out of necessity, Johnson and Post argue that "dispute resolution mechanisms suited to this new environment also seem certain to prosper", invoking the idea of "virtual courts" and "virtual magistrates" again, without noting that these suggestions apply only to the regulation of behaviour that is actually online. In other words, such views seem not to explain or even

acknowledge how these “self-ordering” suggestions could regulate post-transaction breaches of online contracts later detected offline, nor by what authority the “virtual courts” of cyberspace would enforce their rulings in realspace across international borders. If, however, this is a misunderstanding of their position, and what is really being said is that any loss or damage deriving from acts initiated in cyberspace can be remedied by law created by the non-government inhabitants of cyberspace itself, then the point may be uncontested, so long as some effective legally-predictable enforcement regime is available.

However, it is doubtful whether such a regime can in fact be provided by the non-governmental inhabitants of cyberspace. Such parties could not know about real-world post-transaction breaches of online contracts.

Lessig (1996) responded to the libertarians by saying that they “want to argue for a separation between realspace law and cyberspace law that I don’t believe can yet be sustained, nor do I believe that it should … we, here, in this world will keep a control on the development here” (Lessig, 1996).

To that might be added the point that arguably cyberspace is within realspace and thus might be subject to realspace laws. In contrast to the argument that realspace regulation is ineffective or even futile for cyberspace, Lessig (1996) also argues that cyberspace *will* be regulated by realspace interventionist regulation to the extent that it affects realspace life.

Another possible libertarian argument by Lessig (1996) is that unlike realspace where the state tries to convince citizens to adopt norms of behaviour to obey the law, in cyberspace because of the unavoidability of ‘code’ software controls, the state does not need to “convince” anyone of anything: it is a matter of either obey or stay out, and there is simply no opportunity to do otherwise. Thus “law as code is a start to the perfect technology of justice”.

This argument appears to make Lessig less of an interventionist and more of a libertarian than he appears at first sight. The difference then between Johnson and Post's (1996) libertarianism and that of Lessig is that the 'self-regulatory code' of Lessig's cyberspace is state-controlled, which is still a form of interventionism. This is evidenced by such statements by Lessig (1996), as from this perspective, the Communications Decency Act of 1996, and the NII White Paper on Copyright are the very same thing: ... the aim of both is to subsidize technologies of control – to increase the ability to select who gets access to what – and the medium cyberspace is perfectly designed for that control.

However, it is worth noting that neither side in this debate shows how their solutions would apply to breaches of consumer contracts formed in cyberspace because of unremedied non/wrong-delivery of goods in realspace.

According to the editors of the Harvard Law Review (1999), libertarian views still have some influence. For example, "some form of Internet regulation seems both unavoidable and desirable". This may be understood to mean that even self-regulation, if effective, would be better than none. Such libertarians have, however, departed from the earlier position that cyber law and realspace law are forever separate, by asserting that "the old libertarian assertion that cyberspace is immune from territorial regulation is susceptible to an empirical rebuttal": realist commentators who disagree with them need only refer to examples of successful Internet regulations to refute their argument.

According to Gordon (1998), ISPs in Singapore are controlled by the Singapore Broadcasting Authority and must abide by the agency's strict guidelines regarding 'objectionable content'. This could range from pornography to "areas which may undermine public morals, political stability or religious harmony". Furthermore, each ISP must be registered with the government, and can be held liable for any content to which it gives access.

Regulation of the Internet in China began in February 1996 when the government required ISPs to use only government-provided phone lines. Now users must register with the police, and sign a pledge not to harm China's national interests (Gordon, 1996).

In respect of public international law, one method used for solving trans-border enforcement problems is by the creation of multi-lateral agreements to overcome the inadequacies of separate national regulation. This will be of interest if international government-level cooperation is contemplated as a possible solution.

Halpern & Mehrotra (2000) argue that in respect of the global clash between geographically-bounded trademarks and the limitless reach of the Internet, discrepancies in international trademark rights have been resolved through international treaties and that, until recently, this conventional treaty approach has been successful. With the recent, incredible explosion of e-commerce however, such a traditional process has become economically obsolete and is being replaced by the development of an Internet common law (Halpern, & Mehrotra, 2000).

Under this new 'law', bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) are "a prime example of how the conventional method of multinational cooperation is being supplanted by the new approach of individual consent and norms" (Halpern & Mehrotra, 2000).

Furthermore, Halpern and Mehrotra (2000) concede that the private ordering that has come to dominate the Internet is premised on the underlying support of the state government agencies responsible for consumer protection, which for example, still play an essential role in defining and enforcing the default rules that contracts must rely upon as background rules.

Regarding "Internet Common Law authorities" like ICANN:

One of the biggest challenges of ODR Online Dispute Resolution is its enforceability. Sometimes enforceability in ODR is readily achievable. ICANN, as an Internet common law authority, is an excellent example of this. When a panellist in a UDRP Uniform Dispute Resolution Policy process transfers a domain name, ICANN can easily enforce that decision because it has absolute control over the database that assigns domain names to their owners. In B2C e-commerce disputes, this type of absolute enforceability is not possible. If, for example, a product is shipped to a purchaser and the wrong amount of money is charged, the shipper (or the ODR-provider) cannot compel the purchaser to return the item or to pay more money (Online Dispute Resolution for Business, 2002).

Finally, aside from interventionist ideology, the question arises as to whether it is actually possible to regulate the Internet as a technical rather than a legal issue. An entire book could be written on this topic, with the libertarian/interventionist debate being just one part of it. Also, it is well known that rogue website operators can simply change location if faced with regulation unacceptable to their activities. However, an exhaustive treatment of this topic is beyond the scope of a thesis on redress for CCTs.

Internet protocols embody features that present a wide range of very substantial technical difficulties to the would-be regulator of Internet gambling. Addressing the challenges of unlicensed and extra-jurisdictional providers is a great deal more challenging as there is limited scope for effective unilateral initiatives. The intractability of technical difficulties confronting hard forms of national regulation together with the international jurisdictional problems, are likely to remain insurmountable obstacles (Clark & Dempsey, 2000).

6.6 Conclusion

The two major trends regarding the regulation of cyberspace generally and of CCTs in particular are seen in the ongoing debates between the libertarians such as Johnson and Post (1996) and the interventionists such as Lessig (1996), Netanel (2000), Rule (2002), Halpern and Mehrotra (2000), and the debate about private international law problems for CCTs.

The debate between libertarians and interventionists seems more contentious and therefore unpredictable. It is extremely likely, in the international and inchoate environment of cyberspace, that there will be both self-ordering *and* regulatory intervention by national and supra-national bodies, at least for the foreseeable future, as a result of local and immediate needs and realities. Government objectives driven by developing social policies, regulatory interventions of any or all kinds ('command and control', 'light touch' and 'responsive') are equally conceivable. Also, it should be remembered that because this thesis is concerned principally with problems and suggesting potential solutions, an exploration at the level of *what kind* of regulation or of a theoretical question as to purpose (such as whether regulation should act as a proxy for the market or instead of it), is beyond its scope.

There seems little doubt that there will always be self-ordering in cyberspace to some extent—just as there has always been some self-ordering in realspace—but given the fact that governments have both the power to involve themselves in regulation of cyberspace, and extensive motivation for doing so, the broad debate has already changed from whether governments should be involved, to what should be regulated by them, and how.

In the latter case, the consensus of opinion is that a continued resort to private international law rules to solve problems with fraud and CCTs is simply unworkable. Such rules are unpredictable given the virtually infinite range of rules that could be applied in many

situations involving CCTs, and complex where transactional facts are complex and therefore involve delays and costs disproportional to the value of the transactions involved, especially for low-value CCTs.

When considering the possible solutions to the problem, one can see the beginnings of convergence between the separate debates about interventionism and private international law. In Boss's (1992) "universal system developed cooperatively by different countries", in Hardy's (1994) "statutory or judicial solution", in Post's (1996) "promotion of the common welfare", in Goldring's (1998) "multi-lateral international agreements" and "broadly-based effort to establish international consumer protection norms", and in Tokeley's (1997) "cyber-jurisdiction which would regulate the internet independent of national laws", one may be seeing the beginnings of a single resolution to both debates.

Such a solution may also provide an answer to the problem of vendors not performing as expected in offline/post-transactions.

The introduction to this chapter stated that the legal context for the regulation of cyber-consumer protection and CCTs necessarily exists at the interface of four main categories of law: consumer protection law, contract law, private international law and cyber law. This view implies a very clear goal: to construct a conceptual framework from those four disparate categories as a general regulatory theory of CCTs. Such a conceptual structure should serve conveniently as a guiding principle for steering a path towards a clear workable solution.

This chapter has established the evaluative approach used in this thesis to address the theoretical background based upon cyber-consumer protection justifications (express and implied) and the interventionist/libertarian distinction. This chapter has also noted some legal protections for consumer transactions, the assurance of the validity of electronic contracts, a description of scholarly debates and potential solutions concerning the problems of fraud and

cyber-consumer protection, and contributions regarding the development of cyber law. These separate strands can now be woven together into the beginnings of a specific regulatory theory of CCTs in the form of a simple formulation: non-delivery or wrong-delivery in a valid and binding CCT justifies protection for the consumer party.

CHAPTER SEVEN

EXTENSION OF LAW FOR FEDERATED CYBER- CONSUMER PROTECTION

7.1 Introduction

The legal context in this chapter resembles the legal framework for the regulation of CCTs, which necessarily exists at the interface of four main categories of law: consumer protection law, contract law, private international law and cyber law.

7.2 The existing body of law

7.2.1 Consumer-protection law

Consumer-protection law is that body of law created by and applied within nation-states intended to correct power imbalances between suppliers and consumers resulting from differences in product knowledge (Oughton, 1991).

7.2.2 Contract law

Contract law refers to the body of law concerning the existence and enforceability of consumer contracts (Nygh & Davies, 2002).

7.2.3 Private international law

Private international law is the body of law concerned with resolving conflicts which arise in private law matters because of interactions between different legal systems, such as where a

consumer contract is formed in one country and is breached in another (Nygh & Davies, 2002).

7.3 Potential solutions and redress: current methods

As explained in the previous chapters, the focus of this thesis is to discuss existing methods and suggest potential CCT redress methods.

As a preliminary, the following point should be noted. There is a very pragmatic, utilitarian underpinning of the assessment scheme proposed in this section. This is one possible approach that could be used from amongst a number of alternatives. Other approaches, such as ‘cyber-consumer rights’ or ‘fairness’ approaches, for example, are essentially theoretical. The utilitarian approach used here is preferable where there is a need to provide results which are practical and immediately useful.

In the interests of clarity and simplicity, a table is used to summarise the comparative approach undertaken throughout the thesis. The various CCT redress methods are evaluated according to a clearly-defined set of criteria, with the results used to progressively fill in the blank cells within the table. The table is a tool for formal and consistent evaluation of the various redress methods considered throughout, and reappears in the final chapter to present the overall conclusions of the thesis.

Two criteria—difficulty of enforcement and complexity—are used to evaluate the redress methods considered, such that each approach obtains a result for any two of these options: ‘very low’, ‘low’, ‘acceptable’, ‘high’ or ‘very high’. For example, litigation could get a ‘low’ for difficulty of enforcement and a ‘high’ for complexity.

Other consumer-protection criteria such as honesty, fairness, safety, knowledge, choice, privacy, peace of mind, and the right to a remedy for abuses, are either implicit within the two criteria chosen or, with the exception of the right to a remedy for abuses, irrelevant to the objectives of this thesis as discrete criteria. Safety, for example, is relevant to CCTs for the purchase of goods.

There are 13 CCT redress methods assessed in this thesis and noted in Table 7.1. These redress methods are organised and considered under three categories as follows:

1. litigation-based redress under current legal regime (method 1)
2. current non-litigation-based redress (methods 2 to 8)
3. potential non-litigation-based redress (methods 9 to 13).

There is a significant difference in the degree of treatment given to the various redress methods with each receiving the degree of consideration that is warranted. Methods 2 to 8 are covered, to different extents, in the first part of Chapter Eight. Methods 9 to 13 are covered in the last part of Chapter Eight.

After being assessed according to the two evaluation criteria (difficulty of enforcement and complexity), each of the 13 redress methods is given an overall estimate of its effectiveness.

Here it should be noted that the overall conclusions reached in Chapter Eleven regarding the various redress methods examined, are based upon the findings in Chapter Nine in respect of methods 1 to 8. Methods 9 to 13 are only potential redress methods. This latter distinction is explained further in Chapter Nine, where the potential protection methods are considered in detail.

The law models covered in Chapter Ten are evaluated by this thesis in order to assess their potential contribution to the formulation of a solution a united international consumer redress/protection regime.

Table 7.1: Potential cyber-consumer protection solutions and evaluation of redress methods

Method	Difficulty of enforcement	Complexity
--------	---------------------------	------------

Table 7.1.1: Litigation redress under current legal regime

1. Litigation

Table 7.1.2: Redress methods

2. Online Foreign Lawyers
3. Online Foreign Public Consumer Protection Authorities
4. Alternative Dispute Resolution / Online Dispute Resolution
5. Arbitration
6. Online Industry-based Consumer Dispute Resolution Schemes
7. Industry Codes of Conduct
8. Escrow Services

Table 7.1.3: Potential solutions

9. Online Transaction Insurance
10. Online Trustmarks
11. Cyber-consumer Education
12. Cyber-consumer Complaints Bulletin Boards
13. National Deregistration of Vendor Websites

7.4 Difficulties with current legislation

There are two major challenges—enforcement and complexity.

7.4.1 Federation protection with enforcement

Enforceability means that the method of redress can be imposed compulsorily upon a party to the CCT (assuming that physical enforcement in the real world is actually possible and not merely hypothetical) either directly through litigation or indirectly through legal or equitable/moral obligation. Alternatively, enforceability may be thought of as having compulsion in varying degrees of strength.

Thus ‘difficulty of enforcement’ is a variable depending on the degree of compulsion involved. By way of illustration, ‘consumer education’ as a remedy for solving CCT problems would normally be understood to involve no compulsion, thus having ‘high’ difficulty of enforcement, since the information offered by way of consumer education would

normally be unilaterally offered simply as good advice for avoiding such problems in the first place, on a take it or leave it basis.

On the other hand, ADR and arbitration would generally be understood as having comparatively less difficulty of enforcement associated with them, at least in some cases. ADR may involve enforceability by way of a process which might result in a binding (and thus enforceable) agreement. Arbitration can be binding where a quasi-judicial judgment may be binding and thus enforceable against the relevant party (Butterworths, 2002).

Litigation is highly enforceable (i.e. ‘low difficulty of enforcement’) when the party sued is within the relevant jurisdiction because it involves state-backed enforcement powers, but may be less enforceable when the other party is not within the jurisdiction.

Where all current or potential remedies are part of an array of potential solutions of varying degrees of effectiveness, it would be inappropriate to consider only highly enforceable redress methods. This is because less enforceable redress methods still have the potential to provide what a legitimately aggrieved consumer may be seeking. For example, they may be effective to the extent that a vendor, the subject of action under one or more less-enforceable redress methods, might see a certain result as inevitable and produce the remedy the consumer is seeking in order to avoid future, more expensive, and strongly enforceable action by that consumer.

7.4.2 Federation to address complexity

For our purposes, the definition of complexity is the opposite of or the lack of ‘simplicity’. Simplicity is the state of being simple, where ‘simple’ is defined as freedom from complications, and a state where there is an absence of confusion or complexity. CCT redress

methods are evaluated in terms of simplicity according to the extent to which those methods are accompanied by complexity, confusion or complications.

Thus, complexity, confusion or complications may involve a range of factors of various types, such as degree of difficulty in learning, using or applying the remedy, potential waiting time, inconvenience and stress, and include objective and subjective complications. Such factors can overlap with each other, and they can even overlap with cost and enforceability criteria. Simplicity is thus a catch-all criterion, a clear advantage of which is that it limits the total number of criteria being used to evaluate CCT redress methods.

Therefore, complexity (lack of simplicity) is used as a criterion to evaluate the redress methods listed in the table because, first, it would be an advantage to a consumer to be able to avoid unnecessary complications between similar or equal redress methods; and second, the criterion is general enough to cover a wide range of remaining factors after consideration the cost and enforceability factors in relation to the methods. On that basis, an ideal redress method might be one which is cheap, enforceable, not too difficult to use, speedy and relatively stress-free.

7.5 Conclusion

This chapter has explained the evaluative approach used in this thesis to address the theoretical background based upon cyber-consumer protection justifications (express and implied) and the interventionist/libertarian distinction. This chapter has also noted some legal protections for consumer transactions, the assurance of the validity of electronic contracts, a description of scholarly debates and potential solutions concerning the problems of fraud and cyber-consumer protection, and contributions regarding the development of cyber law. These separate strands can now be brought together into the beginnings of a specific regulatory

theory of CCTs in the form of a simple formulation: in the case of fraud, non-delivery or wrong-delivery in a valid and binding CCT, where protection, for the consumer party, is justifiable.

CHAPTER EIGHT

INTERNATIONAL COOPERATION FOR CYBER CONSUMER PROTECTION

8.1 Introduction

This chapter examines the commentary from academic, judicial and other sources concerning the specific redress and enforcement provisions of the model cyber-consumer redress/protection laws proposed by Australia, the UN (un.org, 1999), the OECD (oecd.org, 1999), the EU (europa.eu.int, 1997) and the US. The various law models are considered in both descriptive and prescriptive terms, that is, the objective characteristics of the models, and how those characteristics might be used, if at all, in the formulation of a solution to the redress/protection problems of CCTs. In the context of the theoretical framework and methods described in Chapter Seven and this chapter, both are considered.

The discussion presented here is intended to facilitate the process of constructing a single international cyber-consumer redress or protection law from the models examined, if such a solution were to be adopted. As this thesis demonstrates, an international cyber-consumer redress/protection law is needed because current forms of redress for online fraud and deceptiveness and CCTs are either ineffective or non-existent.

A secondary aim of this chapter therefore, is to briefly consider the basic kinds of international consumer laws that might be inspired by the law models examined in this thesis in order to protect an international cyber-consumer. There are both minimal and comprehensive versions of the two basic kinds of laws, and here we consider the minimal version first.

The most basic distinction between any current national consumer protection law and a workable international consumer protection law is, in practice, the inability of national consumer-protection laws to provide redress and enforcement across international boundaries, for the reasons considered in Chapter Seven and this chapter, and also, to a lesser extent, in Chapter Nine. While there are plenty of examples of relatively effective national consumer protection laws worldwide — at least within territorial reach — there are, as yet, no truly international (global) cyber-consumer protection laws. This will become increasingly problematic for transnational retailers and consumers alike.

As already noted, if it is not possible to fully amalgamate national consumer redress laws generally into a single international cyber-consumer redress law, a minimal solution would be to internationally enforce provisions of national consumer-protection laws through international treaty. However, this solution would still require national governments to work in concert, since only they can enforce the individual and collective authority of nation states to provide the enforcement powers necessary for workable CCT redress.

Thus, the minimal form of an international cyber-consumer protection redress/law would be an international law providing only for effective transnational enforcement of judgments based on existing national law: a basic set of redress provisions that work across international borders by establishing international public law based on the relevant private laws in the current regime. In other words, the signatory states would bind themselves to do their part to eliminate the transnational enforcement problems in the current regime.

Such a solution would not go very far towards providing customer protection against online fraud and solving problems with CCTs generally. A comprehensive international consumer law, however, would include the minimal international/cyber-consumer redress law together with the following extra features to make it a full-scale international online consumer-

protection law: its enforcement provisions would be made effective for online fraudulent behaviour and CCTs through the provision of an appropriately efficient infrastructure (perhaps a cyber-jurisdiction); it would not have, nor need to have, any private international law content; and it would have substantive cyber-consumer protection provisions of the type found, for example, in Part V of the Trade Practices Act. There could, however, be versions of these international cyber-consumer laws that fall between the minimal and comprehensive extremes.

It is likely that the least that would be needed would be something mid-way between those two extremes: the minimal version together with unified private international law, facilitated by an efficient infrastructure. Such a version, interestingly, may be actually harder to create than the comprehensive version which contains nothing that would unite multiple nations. That prospect only makes the comprehensive version more appealing.

A question arises here as to how a minimal international consumer-redress law could be an international cyber-consumer law at all. It could simply be an international agreement only for the mutual enforceability of CCTs involving parties in signatory states who have chosen a particular national cyber-consumer protection law under a contractual choice of cyber-consumer law clause. Consider, for example, a scenario where the US and Australia are signatories to such an agreement. The parties to a CCT are an American cyber-consumer and an Australian online vendor, and the CCT is subject to a clause agreeing that US cyber-consumer law is the law governing that CCT. Should the CCT fail through non-performance by the online vendor, the Australian Government would agree, under this version of the law, to exercise all power necessary to prosecute the local vendor under that US cyber-consumer law or to be responsible for enforcing the judicial ruling made by a US court.

Alternatively, a dedicated single online cyber-jurisdiction for online fraud and CCTs could achieve a better result with the consent and the backing of all signatory states, especially if there were (effectively) ‘fully united’ cyber-consumer protection provisions involved. This ‘comprehensive’ international cyber-consumer protection law, if one could be agreed to, is also tidier as it would avoid the need for physical duplication of judiciaries and the potential for divergent judicial practices.

By way of general introduction to, and summary of, the differences between the law models proposed by the UN (the UN Guidelines), the EU (the Distance Sales Directive and the E-Commerce Directive) and the OECD (the OECD Guidelines), note that whilst overlapping in their purposes to some extent, they do address different fields. While the UN Guidelines are concerned with the broad principles of global consumer protection, however conducted, the Distance Sales Directive is concerned with the regulation of consumer contracts formed by using any means of distance communication for the benefit of citizens of the EU Member States.

The E-Commerce Directive, by comparison, is concerned with general principles for the conduct of e-commerce for the benefit of EU citizens, whether or not they are participating in e-commerce as consumers. Finally, the OECD Guidelines are concerned with the broad principles of consumer protection, specifically where consumer transactions are concluded by means of e-commerce technology.

Of those four law models, the most readily applicable for the purposes of creating a minimal international cyber-consumer protection law is the Distance Sales Directive. While both the EU models are enacted laws, the Distance Sales Directive is formulated more as a set of practical rules, whereas the E-Commerce Directive more closely resembles the abstract principles found in the two guidelines.

Australian and US consumer-protection law, while neither follows the UN and OECD guidelines or the EU directives, are considered here to broaden the scope of enquiry and to include examples of online laws which, incidentally, contain substantive cyber-consumer protection provisions. The sources of such provisions would be of interest to any future efforts to create an ideal international/cyber-consumer protection solution.

8.2 Australian international cooperation

The principal consumer protection law in Australia is the Trade Practices Act, a Commonwealth law. While internationally/online, the Trade Practices Act has little status, it is useful to consider here as it provides an example of how a law can be successfully created to override the divergent laws of separate geographical areas (i.e. the states) (Windeyer & Young, 1964). Its utility here is therefore its usefulness as a principle or example, and not in its status.

The Trade Practices Act came into force on October 1, 1974. It was introduced to provide uniformity of business rules for fair trade in relation to both B2B trade and B2C trade. Thus, the Act regulates both anti-competitive trade practices and misleading or deceptive trade practices throughout Australia. Our interest here is the Act's federalist 'trans-border' and 'online' nature. .

The Act applies to the activities of corporations and the commercial activities of non-corporations who engage in online interstate or overseas trade or online commerce in Australia. Section 109 of Australia's Constitution provides that "when a law of a State is inconsistent with a law of the Commonwealth, though not applicable to the cyber-consumer, the latter shall prevail, and the former shall, to the extent of the inconsistency, be invalid."

The Act therefore applies to matters involving more than one State, and it overrides prior inconsistent State consumer protection-related laws. The Act was introduced to address the diversity and inconsistency of consumer protection laws between the States, such as the *Misrepresentation Act 1972* (South Australia) and the *Contracts Review Act 1980* (New South Wales) which had no close equivalents in the law of other States. To some extent, therefore, the Act is a successful attempt to ensure the universal recognition and enforcement of judgments within a multi-state environment, and to unite substantive content, albeit not including the cyber-consumer.

In addition to concerning itself with Australian interstate matters, the Act also applies to overseas trade or commerce, and thus purports to have an extra-territorial application. For example, Section 4(1) refers to trade and commerce ‘between Australia and places outside Australia’, Section 6(2) refers to the Act having effect in respect of contracts relating to trade or commerce ‘between Australia and places outside Australia’, and section 67(b) provides that where a contract for the supply of goods to a consumer purports to substitute the law of some other country for the provisions of the Act, the Act applies regardless. Once again, this may be effective if enforcement is sought against assets of a foreign vendor *within* the jurisdiction, if there are any.

This is the basic problem with domestic consumer protection laws which purport to exercise full extra-territoriality: such claims are necessarily hypothetical when it comes to the enforcement of judgments (based on such law) over assets outside the geographical scope of that law.

In respect of CCTs where the foreign vendor has no assets within the Australian consumer’s jurisdiction, the Act provides a remedy no better than the litigation redress method described in Chapter Nine. So, domestic consumer protection laws, such as the Act considered here, are

useless in connection with failed CCTs where they cannot be effectively applied against the foreign assets of uncooperative non-performing foreign vendors. This is true even if the foreign vendor in question adopts the domestic consumer protection law through a choice of law clause.

8.3 United Nations cooperation

The UN Guidelines were released on 9 April 1985 by resolution 39/248 of the UN General Assembly. The UN Guidelines were re-released in an amended and expanded form by the UN's Economic and Social Council resolution 1999/7 of 26 July 1999, and were adopted by the General Assembly in late 1999 (un.org 2005).

Since the differences between the original version, which contained 46 clauses, and the new version, containing 69 clauses, are not relevant here, a detailed comparison between them is not made. Examination of the UN Guidelines here is restricted to the current version.

The structure of the UN Guidelines is as follows:

I. Objectives (cl 1)

II. General Principles (cll 2-8)

III. Guidelines (cll 9-10)

A Physical Safety (cll 11-14)

B Promotion and Protection of Consumers' Economic Interests (cll 15-27)

C Standards for the Safety and Quality of consumer Goods and Services (cll 28-30)

D Distribution Facilities for Essential Consumer Goods and Services (cl 31)

E Measures Enabling Consumers to Obtain Redress (cll 32-34)

F Education and Information Programs (cll 35-41)

G Promotion of Sustainable Consumption (cll 42-55)

H Measures Relating to Specific Areas (cll 56-62)

IV. International Cooperation (cll 63-69)

The redress-related provisions of the UN Guidelines are clauses 32 to 34 which provide that governments should establish legal and administrative measures to enable consumers to obtain redress through procedures that are expeditious, fair, inexpensive and accessible (clause 32); that governments should encourage all enterprises to resolve consumer disputes in a fair, expeditious and informal manner, and to establish mechanisms which can provide assistance to consumers (clause 33); and that information on available redress should be made available to consumers (clause 34). The clause of greatest interest here is clause 32.

The UN Guidelines are only guidelines, intended to assist countries in their efforts to protect consumers. This is recognised in what little commentary is available on the UN Guidelines. However, the UN Guidelines have been attacked for being ‘vague’ and ‘overblown’ almost to the point of uselessness (Weidenbaum, M., 1987).

For example, the UN Guidelines’ objectives to ‘promote just, equitable and sustainable economic and social development’ (clause 1) and to ‘encourage high levels of ethical conduct’ (clause 1(c)) have been criticised for being ‘high-minded’ and ‘fuzzy’ (Weidenbaum, M., 1987).

Weidenbaum (1987) asked ‘who will set the standards of ‘ethical conduct’?’ ‘Consider how substantially a totalitarian interpretation of ethical conduct would differ from that of various free societies’. Peterson wrote that Weidenbaum would criticise the US Constitution on the same grounds (Peterson, E., 1987).

Another criticism by Weidenbaum (1987) is that the UN Guidelines seems to be ‘a blueprint for a centrally directed society’, and that ‘we need only consult the dismal record of any of the world’s centrally planned economies to know that taking this objective would hurt rather than help the developing nations’.

Whereas, Peterson (1987) says the US Constitution, which he adds, Weidenbaum swore to uphold and defend, is a blueprint for a central government, while the UN Guidelines bind no country to anything, but merely sets out goals and objectives for all nations to aspire to in protecting their own people.

Peterson (1987) also argues that without effective governmental regulation, the worst practices of the worst competitors often set the norm in the marketplace. Peterson concludes by arguing that legitimate business throughout the world needs the kind of consumer protections which the Guidelines erect as a goal. Since no honest business person wants to profit from harming the customer, the Guidelines will foster an atmosphere in which legitimate business can indeed prosper.

At this point, an aggrieved consumer could sympathise with the viewpoints of Weidenbaum (1987) and Peterson (1987), there being little of practical value in the well-meaning UN Guidelines.

The UN Guidelines were also attacked by Weidenbaum (1987) on the grounds that ‘no convincing case has been made for the participation of international agencies in such a basic domestic consideration as the protection of consumers’. From this perspective, it is unsurprising that he saw no particular vagueness in the redress aspects of the UN Guidelines found in clauses 32 to 34.

To his credit however, Weidenbaum did think that the UN Guidelines might solve international consumer problems, possibly without knowing, in 1987, what such problems could be. In the Internet Age, the nature of such problems is now evident. However, the UN Guidelines are justified in part because they would help solve ‘international issues’ not relevant to the cyber-consumer although a straightforward reading of the Guidelines fails to uncover any such global concerns.

In response to the UN Guidelines’ redress recommendations (clauses 32 to 34), countries such as Australia, Canada, Hong Kong, New Zealand, Singapore and the USA established various mechanisms for consumers to obtain redress with respect to national consumer transactions, including the introduction of special procedures into previously-existing lower courts, and the creation of new courts and tribunals which specialize in small consumer claims (Harland, D., 1991).

In some cases, procedural rules were simplified, hearings were sometimes held with the presence of lawyers being disallowed, night and weekend hearings were allowed, and parties were assisted in preparation of their case, with limited right of appeal (Harland, D., 1991).

However, despite these advances, the persistent problem of online fraud and failure of CCTs indicate that Clause 15 and clause 69 have been unable to provide unequivocal ‘cyber-consumer protection’ in respect of CCTs.

The impact of the Internet was yet to be fully appreciated in 1991 and there was no consideration then of the special difficulties associated with trans-border consumer disputes. This continued to be true for academic commentators as late as 1997 (Ramsay, I., 1997) (Harland, 1997).

8.4 OECD cooperation

The OECD (the Organization for Economic Cooperation and Development), is a Paris-based international body composed of 25 countries participating in a permanent cooperation designed to coordinate the policies of the member nations. The OECD makes available all information relevant to the formulation of national policy in every major field of economic activity. Its principal goals are:

- (1) To promote employment, economic growth, and a rising standard of living in member countries, while maintaining stability.
- (2) To contribute to sound economic expansion of both member and non-member nations in the process of development.
- (3) To further the expansion of world trade on a multilateral, non-discriminatory basis in accord with international obligations. Policies are formulated and ideas shared at meetings held throughout the year.

This form of cooperation, rooted in the growing interdependence of national economies, began in April 1948, when a group of 16 European countries founded the Organization for European Economic Cooperation (OEEC) to administer the Marshall Plan and to work together for post-war recovery. The OECD, succeeding the OEEC, was established on September 30, 1961, in order to broaden the scope of cooperation (Microsoft Encarta Encyclopaedia, 1996).

Upon consideration of this, both the status of the OECD, in terms of its heritage, aims and purposes, and its relevance to the phenomenon and potential of CCTs, is apparent.

The OECD's Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce that is, 'the OECD Guidelines' was released on 9th April 1999 (oecd.org 2005).

The OECD Guidelines were 'designed to help ensure that consumers are no less protected shopping than they are when they buy from their local store or order from a catalogue' (oecdpublications.gfi-nb.com 2003).

The OECD Guidelines however, are 'non-binding' and 'the overarching principle of the Guidelines is that consumers shopping should enjoy transparent and effective protection that is not less than the level of protection that they have in other areas of commerce' (oecdpublications.gfi-nb.com 2003).

The OECD Guidelines commence with a brief preamble, followed by an 'annex' containing the guidelines in the following structure:

Part One - Scope

Part Two - General Principles

- I. Transparent and Effective Protection
- II. Fair Business, Advertising and Marketing Practices
- III. Online Disclosures
 - A. Information about the business
 - B. Information about the goods and services
 - C. Information about the transaction
- IV. Confirmation Process

V. Payment

VI. Dispute Resolution and Redress

A. Applicable law and jurisdiction

B. Alternative dispute resolution and redress

VII. Privacy

VIII. Education and Awareness

Part Three - Implementation

Part Four - Global Cooperation

In terms of redress provisions, Part VIA of the OECD Guidelines (Applicable Law and Jurisdiction) states that B2C cross-border transactions are subject to the existing framework for, and thus the existing problems associated with, applicable law and jurisdiction such as divergent conflict of laws rules, uncertainty, expense, complexity, lengthy delays in obtaining judgment and potential language difficulties.

E-commerce poses challenges to this existing framework and therefore consideration should be given to whether the existing framework should be modified. When considering any modifications to the existing framework, governments should seek to ensure that, while facilitating e-commerce, the framework provides fairness to consumers and business no less than that afforded in other forms of commerce while providing consumers with redress without undue cost or burden (oecd.org 2005).

While, once again, the OECD Guidelines is only a set of guidelines, they indicate and reinforce the view that the existing situation with respect to CCTs is replete with difficulties

and that governments should be responsible for providing a solution, a position which supports the positive preference for interventionism in this thesis.

Part VIB (Alternative Dispute Resolution and Redress) states that consumers should be provided with meaningful access to fair redress without undue cost or burden, and governments should develop policies to resolve consumer disputes arising from B2C trans-border transactions. Furthermore, in implementing these policies, governments should employ information technologies innovatively. However, governments both national and international, together with academics, should conduct further studies if these objectives are to be met at an international level (oecd.org 2005).

While these are commendable principles, in practice little is being achieved by applying the OECD Guidelines, at an international level. The OECD's first major report on the implementation of the OECD Guidelines (oecd.org 2001) stated the Guidelines recognise the need for member countries to adopt and adapt laws to ensure that consumers are protected in the online environment. To this end, in the European Union, member states have been taking steps to introduce directives related to the Guidelines (olis.oecd.org 2005).

This kind of regional law-making is not consistent with the OECD Guidelines' Part VIB – which provides that 'governments should develop policies to resolve consumer disputes arising from B2C cross-border transactions' as the full effect of the Internet on world-wide consumerism demands. This criticism is borne out by further points made in the report, such as 'in Canada, the national and provincial governments have agreed to work towards united and modernised consumer protection laws related to electronic commerce', 'in Mexico, the Federal Consumer Protection Law was modified in May 2000', and 'in Australia, the development of legislative amendments continues'. All of these are regional and regionally-focussed initiatives and therefore doomed to irrelevance where international cooperation is

required to provide a unified solution to the problem of effective justice for cyber-consumers and CCTs.

Other initiatives inspired by the OECD Guidelines and noted in the report are that Japan and Korea agreed to co-operate through various efforts, including a project aimed at mutual recognition of Internet trustmarks and the evaluation of websites in ‘sweep days’ (olis.oecd.org 2005).

The criticism here is not of the OECD Guidelines as such, but of the fact that those purporting to be guided by them persist in having parochial mind-sets: the initiatives are all regional and, in some cases, are legally insignificant. For example, a trustmark could not in terms of practicality, assist with a breached CCT except in extremely limited circumstances (olis.oecd.org 2001). A trustmark provider could conceivably be sued for misrepresentation by an aggrieved consumer, but that is not likely to represent a general effective solution for breached CCTs.

In respect of the ‘cross-border enforcement cooperation’, many cases of CCTs involve ‘fraud’ as such, also could still trigger an irresolvable dispute; international cooperation is needed beyond that between the US and Canada only; the most recent proceedings along these lines occurred in March 2000, but enforcement cooperation is of little assistance without the pre-existence of judgments for CCTs that are recognisable across borders. Therefore, what is needed is wide international cooperation which provides effective and simple access to internationally and online recognised redress procedures and, for a comprehensive solution, the uniting of the substantive content of cyber-consumer protection laws, internationally.

8.5 European cooperation

In common with both Australia and the USA, the EU, at least economically, is an example of a federal system of government (Bogdanor, V., 2003).

Bogdanor (2003) says that the EU certainly satisfies the federal principle. There is a constitutionally guaranteed division of legal sovereignty between two layers of government divided territorially. Sovereignty is divided between the EU itself and the member states. The component units, the member states, retain, of course, very significant, if not preponderant, law-making powers, but these powers are limited by the Treaty of Rome and the amending treaties (riia.org 2005).

The EU law model examined here, may reasonably be understood as laws of Europe (as if they were the laws of a sovereign nation), and amount to a second example of what could be achieved cooperatively between separate states, in the same manner as Australia's Trade Practices Act.

The assessment in this section of the two EU law models, the Distance Sales Directive and the E-Commerce Directive, necessarily includes some preliminary description and analysis of two associated but independent bodies of private international law: the Rome Convention (rome-convention.org 1980) and the Brussels Regulation (curia.eu.int1986) (europa.eu.int 2001).

The Distance Sales Directive came into force in May 1997 (europa.eu.int 1997). It aims to protect consumers engaging in ‘distance contracts’, and applies to all companies engaging in transactions with EU consumers. Notably, the Distance Sales Directive includes a right of withdrawal in favour of consumers that cannot be waived by contract.

The E-Commerce Directive came into force in July 2000. It provides a general legal framework for the conduct of e-commerce within the EU and by the EU Member States with outside parties (europa.eu.int 2000).

It can be seen that the general criticisms of private international law made in Chapter Eight (for example, lack of experience) even from the perspective of a lawyer in general practice, and especially from the perspective of the average cyber-consumer, are understandable. However, while this view could be challenged as being ‘merely subjective’ and grounded in lack of expertise, the more objective problems with private international law are less difficult to ignore. For example, some cyber-consumers may want to understand how to initiate their own actions, and complex private international law rules will often prevent this; private international law rules are subject to unforeseeable and unilateral alteration, virtually necessitating a constantly-updated specialist legal skill; and private international law rules, from one country to the next, are just as likely to be inconsistent, as they are to be in agreement with each other, requiring skill with multiple sets of private international law rules in many cases. The issue now is whether these problems could be alleviated.

8.6 United States cooperation

The most important federal consumer protection law in the US is the *Uniform Commercial Code* (the Code) of 1952 (Fullerton, J., 1997). It is worth mentioning that it is only ‘federal’ in that it is available as a universal guideline for each US state – thus, the actual Code for each US state can be different.

The purpose of the Code is to ‘establish a uniform law to govern commercial transactions that often take place across state lines’ (Barnes, A., 2005).

There is no express distinction made between B2B (business to business) and B2C (business to consumer) transactions. However, by defining ‘between merchants’ as ‘any transaction with respect to which both parties are chargeable with the knowledge or skill of merchants’ there is an implied difference in the treatment of B2B and B2C transactions under the Code, thus specifically ensuring that consumers are protected. Further, the Code would be a good candidate for inclusion in an international consumer law uniting project, containing the usual range of ‘standard’ consumer protection provisions such as provisions concerning implied warranties of title, merchantability and fitness for purpose, together with provisions concerning the buyer’s rights to performance and remedies in the event of non-performance.

The relevant US private international law when the Code is the law governing CCTs is known as a ‘long arm statute’ law. A ‘long arm statute’ has been defined as ‘a law that allows one state to claim personal jurisdiction over someone living in another state’ (County of Santa Cruz, 2005). Each US state has its own long-arm statute(s).

When considering a matter with foreign elements, a US state court begins deliberations by examining whether jurisdiction over a foreign party is allowed under the relevant state's long-arm statute, and whether that jurisdiction would fall within the due process principle of the Fourteenth Amendment to the US Constitution (Debussere, F., 2002). It is the due process clause of the Fourteenth Amendment which enables a state to create a long-arm statute.

Under US law, a court in the state in which the consumer resides will have jurisdiction over a foreign defaulting Internet seller in relation to an CCT, when the minimum contacts of a non-resident defendant with a forum are such that the exercise of jurisdiction does not offend ‘traditional notions of fair play and substantial justice’ (International Shoe Co. V. Washington, 1945).

Further, the defendant must have such a degree of ‘minimum contact’ with the forum that ‘they might expect the necessity of litigating there, for example by doing business within it, however a defendant need not have physically entered a forum in order to be subject to its jurisdictional reach’ (Cordera, ., 2001).

In US law, then, the focus is upon the activities of the *supplier* and not on the consumer, as the US courts are required to conduct the ‘minimum contacts analysis’ of the supplier’s activity referred to above. Furthermore, a minimum contacts analysis which results in a court declaring itself competent to hear a matter in relation to foreign websites, must have established that three extra conditions have been satisfied: the defendant must have performed a transaction within the forum, the exercise of jurisdiction in the forum is reasonable (i.e. does not place an excessive burden upon the defendant), and the website in question must be sufficiently ‘active’. That is, it must do more than passively make information available, it must also allow for the creation of contracts, take payment, and exhibit other indicators of interactivity (Debussere, F., 2002).

The mere act of a corporation selling goods across any US state boundary will often satisfy this requirement for US jurisdictions. The result is that, while approaching the same issue from a different perspective, US law often arrives at a similar point to the Europeans under the Brussels Regulation: the consumer gets to litigate in their local court.

This has advantages for the US consumer in terms of both cost and simplicity. However, the difference is that under US law, the US consumer can be subject to contractual choice of forum (i.e. jurisdiction) clauses (which would have no effect in Europe unless they favour the consumer). In the case of *Carnival Cruise Lines Inc. v Shute* 499 U.S.585 (1991), the US Supreme Court held that forum selection clauses in consumer contracts would be upheld where they were freely bargained for (i.e. given in exchange for consideration, without undue

burden on the consumer) because of the cruise line's international character, which increased the likelihood and expense of being brought to court outside the US. By analogy, comparison of the borderless world of the Internet leads to a similar conclusion.

The US approach to redress for consumers in respect of disputed CCTs is both consumer-friendly and arguably fair to Internet business, although one should question how effective it would be in respect of CCTs. As to enforceability, however, it seems that under present US law, the problem still exists of actually enforcing the decision passed down by a consumer's local court where the defendant foreign Internet merchant has no assets in the forum jurisdiction (unlike under EU law, as noted above). .

8.7 Conclusion

Every model examined in this chapter is beset by the problems of disjointed and inconsistent consumer protection standards, disparate private international law rules, high cost and limited enforcement powers, leading to lack of consumer confidence in entering CCTs and in the enforcement of judgements regarding failed CCTs.

A comprehensive international consumer protection law is desirable. It may be an extraordinarily difficult business to create such a law, as evidenced by the comments of Donohue and Goldring above "it usually takes a couple of years to draft an internationally acceptable convention and requires diplomatic conferences with all the contracting states participating to introduce necessary changes because of its status as a treaty" – however, there are numerous examples showing the success such a process (Diedrich, 2000). "The Vienna Sales Convention ... is the most successful convention having regard to the number of contracting states and its acceptance in practice" (Diedrich, 2000). This seems to suggest the need to reconsider solutions.

Finally, the Internet has internationalised consumerism and CCTs will continue to be popular. The use of national consumer-protection laws in CCTs through choice of law clauses can involve complex private international law issues such as jurisdiction, recognition and enforcement, and dealings between consumers and online merchants regarding governing law would usually be slanted towards the merchant through use of standard form ‘take it or leave it’ contracts.

This is inappropriate for the average cyber-consumer. Despite the advantages of a ‘minimal international consumer protection law’ (i.e. a non-unified international consumer protection law with effective redress provisions) noted earlier, a full international consumer protection law would mean that the tangled problems of private international law, choice of law, adjudicatory jurisdiction, recognition and enforcement of foreign judgments, plus uncertainty and complexity of these factors could be neatly side-stepped with international agreement to submit to a single law. If the rules of international commerce, maritime law, criminal law, telecommunications and postal services law, etc. have become ‘geography-neutral’ or globalised, the content for international/cyber-consumer protection laws, possibly subject to some in-built flexibility for local or cultural differences, could also be agreed upon and made geography-neutral.

The technique by which international legislative unity may be achieved has been suggested by Goldring (1998). The first stage is the ‘comparative law study’ of the relevant law of the prospective signatory states, “designed to reveal similarities, differences, and points likely to require specific attention”.

The second stage is ‘formulation’ in which a proposed text is produced either in the more-common form of a draft international treaty/convention, or as a draft model law. As may be expected, Goldring (1998) warns that, because of the process of compromise and negotiation

that is often involved in this stage the text is more commonly the lowest common denominator of national interests but even then, there may be irreconcilable differences.

Goldring (1998) calls the final stage “legislation or model law?” and advises that legislation in the form of the directives used by the EU are a form of international treaty which Member States are obliged (by the 1957 Treaty of Rome) to implement, meaning that the terms of the treaty become part of the national law of each signatory state. Conversely, with a model law, “there is no formal compulsion to adopt the whole or any part of the text. Local drafters are tempted to add their own embellishments and variations to provide for local circumstances.” The ‘model law’ approach (in Goldring’s sense) is not recommended here, as such an approach may be forever likely to remain a mere curiosity for legal specialists.

CHAPTER NINE

CYBER-CONSUMER COGNITIVE PROCESS AND BEHAVIOUR ANALYSIS

9.1 Introduction

In previous chapters, it became clear that the legal approach to DA, in terms of its definition and measurement, is not adequate on its own, since it does not consider the cognitive effect of the advertising message on the consumer. On the other hand, the behavioural perspective focuses on studying the cognitive processes through which the advertising message is received, and via which a certain belief is reached leading to an effect on the consumer's purchasing decisions.

The consumer's cognitive processes are considered the main determinants of his/her recognition of DA. They indicate the set of cognitive components by means of which the consumer deals with the explicit or implicit claims being made by the advertised message (Olson & Dover, 1978). It is worth mentioning that the method of the advertising message is affective with regard to recognising the deception in the advertising message.

In the framework, this thesis approaches those issues that are related to the consumer's recognition of them, and does not allude to their individual outcomes.

Some studies in this area determine some cognitive processes and their effects on the process of recognising advertising deception, as well as the processes used for identifying advertising deception, understanding it and forming false beliefs that express those cognitive processes which mediate the process of recognising DA.

Discussion of results from previous studies pertaining to the cognitive processes which mediate the consumer's recognition of advertising deception lays the foundation for the suggested framework of determinants of recognising DA and its span of effects.

In light of the above, the following section covers:

- Recognising advertising deception: previous studies.
- The framework suggested for determinants of advertising deception.

9.2 The suggested framework for the determinants of online deceptive advertising

Building on the previous studies in the field of recognising DA, the cognitive processes which mediate the cyber-consumer's recognition of DA, which are considered as determinants for recognising DA by the consumer, can be determined as follows: recognition (exposure); attention; comprehension and prior knowledge; involvement; beliefs.

Each of these aspects is discussed in detail below.

9.2.1 Recognising (exposure)

The term 'recognition' is used in different ways. In terms of its effect as a cognitive variable in recognising DA, it indicates sensory processes or those advertising claims which are received from the external environment through the consumer's exposure to those advertising claims.

Later, those claims become part of the cognitive process. Hence, this term also indicates the sensory register of external influences.

Consumers are faced with many advertising messages to choose from and interpret differently, depending on the structure of their personality, their aspirations and previous experiences.

Previous studies indicate that perceptual field identification or exposure, concerning the volume of the advertising message, the speed at which the content of the advertising message is presented, and the frequency of message presentation or message repetition, contribute to the consumer recognising the advertising deception.

Figure 9.1 illustrates the affective span of the processes of exposure to the ad as a cognitive variable mediating the DA.

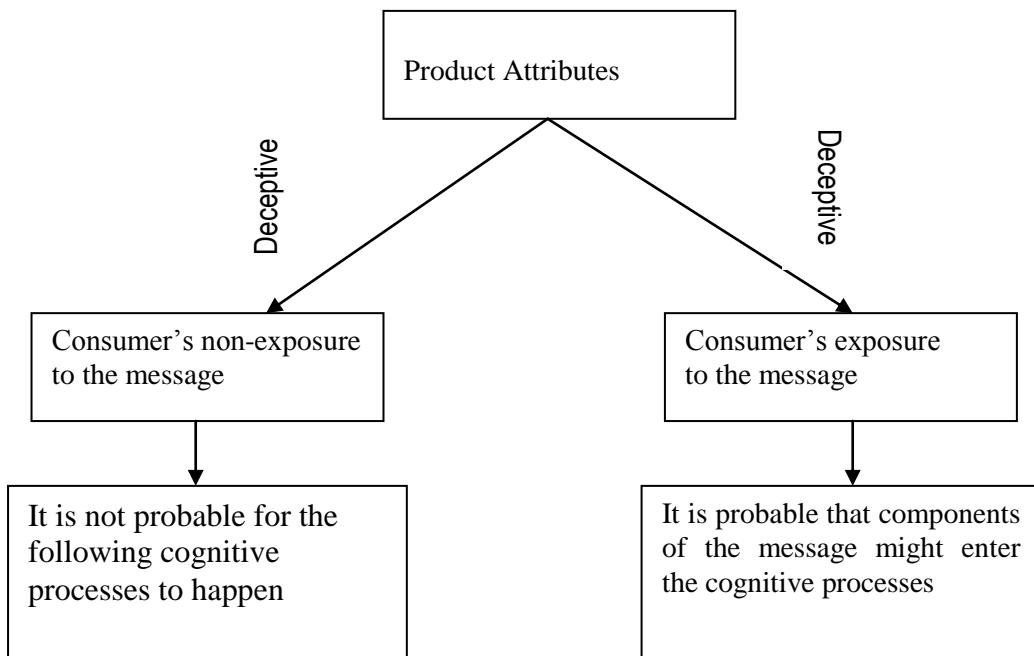


Figure 9.1: The affective span of the process of exposure to the ad in recognising the deceptive message

It is possible that the consumer might be deceived not as a result of exposure to the DA message, but as a result of acquiring information about this message from other sources — friends, for example.

According to the behavioural approach, the source of deception of the consumer must be the exposure to the advertising message, to its content of explicit or implicit deceptive claims, in order to judge the message as being deceptive.

9.2.2 Attention

The concept of attention indicates the state of mind. It is taking possession of the mind, which allows the recipient of the advertising message to deal with information implied in the message. Hence, it implies a certain state of mind that leads the consumer to receive the advertising message by focusing on certain information and overlooking other information (Johnston & Dark, 1986).

The attention process is comprised of:

- Recognising or identifying the advertising message as being the stimulation of the attention process (stimulus recognition).
- Testing the elements which are implied in the cognitive process.
- Retention of the previous elements in the memory (Maloney, 1977).

Although a consumer's recognition is considered unlimited, the span of mental apprehension of the advertising message is considered limited, represented by the number of elements the consumer can remember after exposure to the advertising message. The element in the advertising message represents information included in the message.

When exposure is limited, four or five elements might be remembered. The advertising message, if recognised via the consumer's senses in the previous stage, might enter into a critical stage, which then is the consumer's attention.

Although Gardner (1975) did not use attention as a cognitive element mediating recognition of DA, he maintained that attention plays a role in the formation of deceptive beliefs, which are connected with the advertising claims contained in the advertising message. This interprets the advertiser's attempt to attract the consumer's attention towards the advertising message as being effective in regard to recognising the beliefs which lead to deception of the consumer.

Processes of attention lead to the deception of the consumer's interpretation of some of the pictures accompanying the ad, which make the consumer inattentive to deceptive information, while, in turn, focussing on, or directing attention towards, the pictures contained in the advertising message. Accordingly, a misconception is created in the consumer.

The ads also include some colours within the advertising message and are presented visually in strategic places to give the advertising message a certain context.

Those processes draw the consumer's attention to the framework in which the advertising picture is presented (location, colours, images) without paying attention to the content of the advertising message — non attention — thereby deceiving the consumer.

This is why the advertiser tries to create a special kind of attention; that is, the consumer's attention is drawn to non-basic information upon which the consumer makes the purchasing decision. In such cases, consumers make decisions based on incomplete information. This makes it possible for advertising messages to deceive consumers.

Previous studies of ads which target children, and which offer ‘something free’ together with the product, conclude that children in the age group 10–15 years, and their families, make the decision to purchase in light of the advertising claim contained in the message about the existence of ‘freebies’ without identifying the important information contained in the message and upon which the purchasing decision *should* be made.

The result is that non-attention to important information and directing attention to the information targeted by the advertiser, might lead to non-recognition of advertising deception by the consumer (Shimp, 1978).

Other studies (Scammon, 1978) in the comparative advertising field about the features of advertised products compared to those of rival products, indicate that the consumer was deceived by ads as a result of having his/her attention directed to non-relevant or non-basic features of the product, prior to making a purchasing decision.

In a similar vein, other studies (Morris & Millstein, 1984) conclude that the ads warning about the side-effects of drugs are less effective in realising their objectives when those ads are not accompanied with a certain sound or context. We can conclude from this that attention affects recognition of the advertising deception.

Cohen (1976) and Wilkie (1982, 1985, 1986) conclude that the dependence on full disclosure policy and the affirmative disclosure policy, as policies controlling advertising deception, are not effective in protecting against advertising deception since the consumer can ignore (not be attentive to) this full or affirmative disclosure.

Hence, the process of attention represents a basic stage in the cognitive processes which mediate recognition of the advertising deception and affect the cognitive processes inside the consumer’s mental framework as illustrated in Figure 9.2, which represents the affective span

of the attention process as a cognitive variable mediating the process of advertising deception.

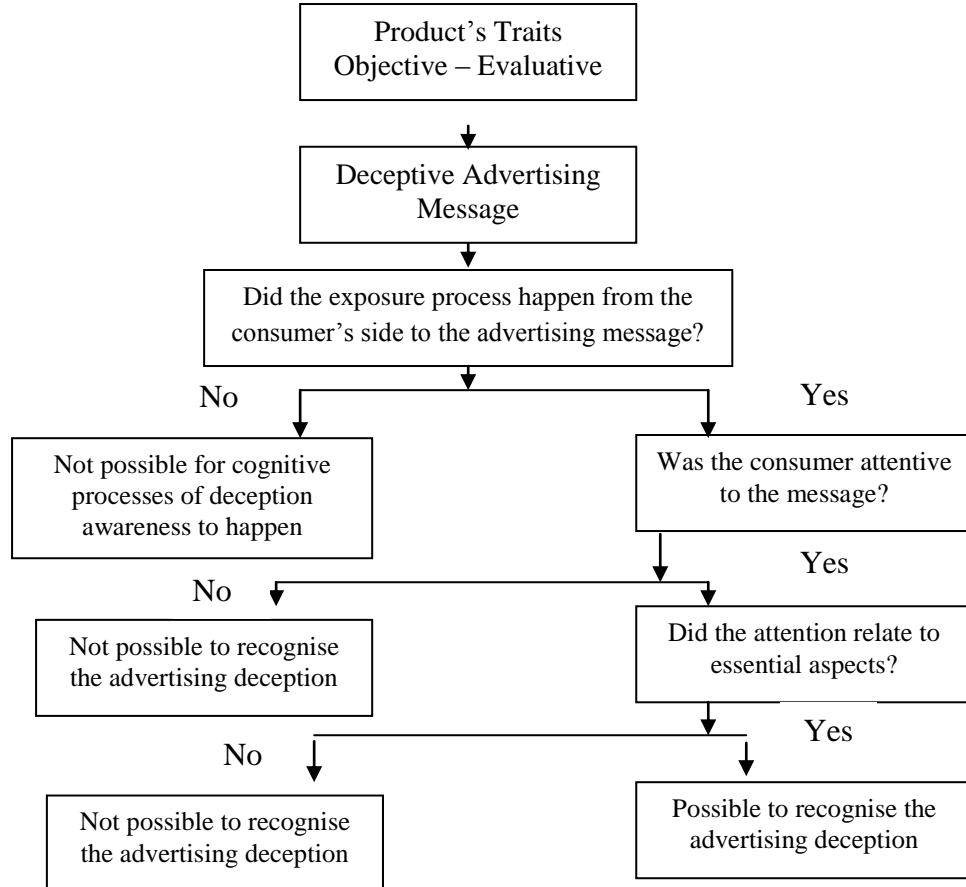


Figure 9.2: The affective span of the attention process in recognising deceptive advertising

9.2.3 Comprehension and prior knowledge

Comprehension indicates cognitive processes through which consumers understand their behaviour and the aspects related to the surrounding environment. It includes the consumers' interaction via data reception and the information contained in advertising messages.

Prior knowledge, then, intervenes in crystallising comprehension, and then the consumer, in turn, can comprehend the advertising message (Richard, D., & Olson, J., 1988).

Results of studies indicate that there are differences in interpreting advertising claims contained in advertising messages (Hutchinson, 1987).

Processes of comprehension do differ since comprehension might take the following forms (Jacoby & Hoyer 1982):

Automatic comprehension, where the consumer does not plan for it is controlled comprehension which takes place when the consumer is directed on a particular course.

There is comprehension which leads to material or tangible meanings and comprehension which leads to non-material intangible results.

Consumers' ability to understand and comprehend the content of the advertising message is dependent upon the prior knowledge available, which exists in the consumer's memory and includes certain meanings and prior beliefs and a special expertise of the consumer. All of these are interacting factors which determine the level of comprehension which the consumer directs in certain circumstances toward a certain advertising message (Ford G., and Richard Y., 1982).

Two types of consumer knowledge can be identified. First there is the expert consumer – this consumer has available knowledge and details about a certain product or a certain mark of the product. This type of consumer is able to comprehend the advertising message which includes information about the product of interest.

The second type is the novice consumer; this is the consumer who has no experience with the product and hence there is a low probability that the novice consumer fully comprehends the advertising message. (Craik & Lockhart, 1978).

There are three types of consumer prior knowledge. The first type is the prior knowledge related to the traits of the product, especially the material and the non-material traits.

The second type is the prior knowledge related to benefits of the product, whether these be the functional features of the product or its psychological (Olson, 1988).

The third type is the value satisfaction derived from the product. Studies by Richard & Olson (1988) reached the conclusion that the certain meanings which the consumer understands through exposure to the advertising message, in the context of a certain environment of the product, depend on the level of the consumer's comprehension of the message.

In light of these previous studies in this field, two types of comprehension can be identified. The first type is the shallow comprehension, which is related to reaching material or tangible meanings.

The second type is the deep comprehension, which is related to reaching non-material and subjective meanings, which are more connected to certain symbols (Richard & Leven, 1985).

In light of the above, the comprehension process mediates the process of the consumer's awareness of advertising deception. Accordingly, the comprehension of the advertising message leads to the probability of the consumer's awareness of advertising deception (Preston & Richard, 1986).

Non-comprehension results when there is no accord between the level of comprehension and the type of the content of the advertising message. That is, the material content built upon tangible facts and which suits the comprehension process which leads to concrete meanings, and the evaluative content which is built upon the intangible aspects suitable and unsuitable to the process of comprehension which leads to abstract meanings. In this case, non-

comprehension becomes more probable and recognition of deception becomes less probable (Vermeersch & Swenerton, 1987).

Table 9.1 depicts the affective span of the comprehension process and prior knowledge as a cognitive variable mediating the process of recognising advertising deception.

Table 9.1: The affective span of the cognitive process in recognising deceptive advertising

Type of ad message	Ad message built upon tangible aspects (objective)	Ad message built upon intangible aspects (subjective)
Type of comprehension process		
The comprehension process which results in concrete meanings.	The comprehension process of the consumer accords with type of ad message where the probability of recognising the advertising deception is high.	The comprehension process of the consumer doesn't accord with type of message where the probability of recognising the advertising deception is low.
The comprehension process which results in theoretical meanings (abstract)	The comprehension process of the consumer is not in accord with the type of ad message where the probability of recognising the advertising deception is lowered.	The comprehensive process of the consumer is in accord with the type of the ad message where the probability to recognize the advertising deception is high.

9.2.4

Involve

ment

Involvement indicates the consumer's recognition of the extent of suitability between the product, the behaviour or the attitude to the consumer's personality (Mitchell, 1990). The consumer who recognises that the product being advertised is relevant becomes involved in it and shows interest in the message (Mitchell, 1990).

Studies (Mitchell, 1995; Stone, 1994) indicate that the consumer's involvement is accomplished with many factors, including traits of the product, its uses, results, its social value for the consumer, type of the ad message, characters presenting the visual presentation

(in the case of television advertising) and the source of the advertising message in the case of ads published in newspapers and magazines.

The level of consumer involvement with the product of the ad is determined in light of two factors. The first is the level of internal agreement between traits of the product and those of the consumer, referred to by Gardner (1985) as ‘intrinsic self-relevance’. The second is the role of the situational agreement between the traits of the product and those of the situation or the environment, referred to by Antil (1984) as self-relevance.

The above two factors assist in interpreting the content of the advertising, the effect on cognitive processes, attention and comprehension.

Figure 9.3 explains the framework of the consumer’s involvement with the product.

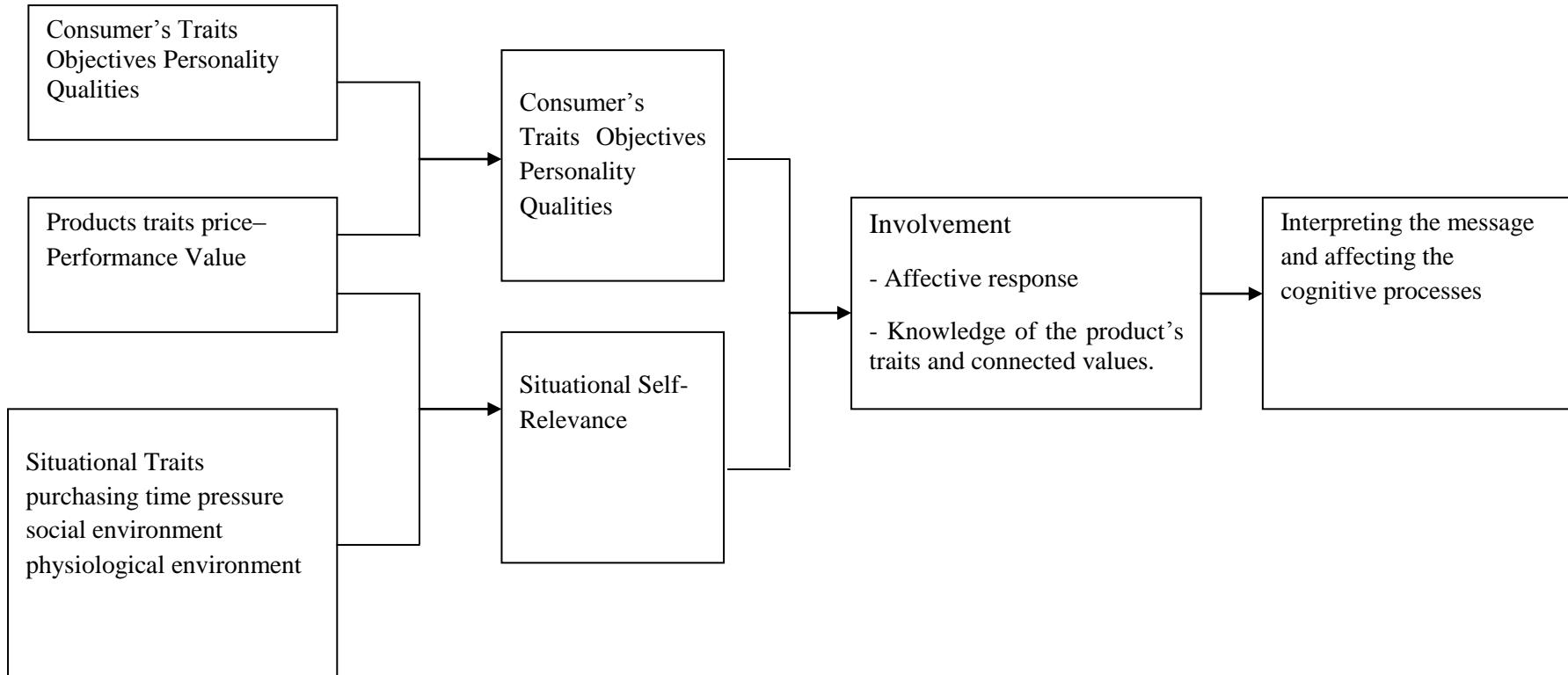


Figure 9.3: The framework of the consumer's involvement with the product

It is worth mentioning that the concept of involvement provokes disputes because it is considered to be an amorphous concept containing a plethora of meanings (Zaichowsky, 1995).

For the purpose of this research, and given its parameters, the involvement indicates the consumer's involvement with the product. Accordingly, the involvement is not related- to the advertising message itself, its technical components, those performing them, involvement related to the method or the source through which the advertising message is offered. Hence, here involvement is seen as the consumer's interest in a certain product (Laurent & Kapferer, 1995).

Gardner (1985) considers that the level of involvement determines the processes of employing the information contained in the advertising message in order to make a purchasing decision. He reached the conclusion that when the consumer's level of involvement is low, the information contained in the advertising message is used to a low degree, which is why, in those instances, the consumer is not duped by any deceptive advertising message.

Smith & Swinyard (1985) conclude that the price of the product advertised represents a critical factor in the process of involvement. For high involvement products, the consumer expects many benefits as a result of deciding to purchase them.

In the case of low involvement, they are mostly non-costly products. Accordingly, the customer does not pay attention to what is mentioned in the advertising message of the product. That is why the consumer's experience (trial) becomes the method available to the consumer.

The product's price is considered an affective factor as it uses logical information to persuade the consumer to make the decision to purchase, and ignoring the special products which the consumer deals with without the logical employment of information (Laurent & Kapferer, 1995).

In light of that, recognition of the advertising deception becomes connected to the product's cost. If the cost of the product is low, the consumer's interest is low, and accordingly, the consumer is expected to purchase the product while not being completely positive about the traits of the product as described in the advertising claims and contained in the advertising message.

Johar (1995) concludes that consumers who have a high level of involvement with traits of the product can be duped by deceptive ads which contain advertising claims in which incomplete comparisons are made between the traits of the advertised product and those of its rivals. This is a consequence of the fact that those consumers form deceptive beliefs when exposed to this DA message, where the effect of the DA message is more probable for the consumer who has a high level of exposure compared to consumers who have a low level of exposure, who in turn, try to make comparisons between the advertised product and rival products after exposure to DA messages. Therefore, for those consumers who have a low level of involvement, the recognition of DA is less probable.

Therefore, where the advertising message is related to products of high value, which are important to the consumer, and where the consumer manages to interpret the content of the advertising message during exposure to the ad, it is more probable that the advertising deception will be recognised.

Shimp (1979) determined what he called "social-psychological representation", in the sense that this representation means representing the evaluative claims which form deceptive claims. Being subjective and personal claims, the consumer has to reach certain meanings through those evaluative claims and those claims are subject to personal differences.

Shimp also concludes that when involvement is inconsistent with the type of advertising claims, recognition of advertising deception becomes more probable.

A study of 615 advertising messages, conducted by Pollay (1980), , found that 2 per cent of those messages contain evaluative (subjective) claims and that consumers interpreted them differently. This is as a result of the fact that involvements are inconsistent with the type of advertising claims.

Both Lord & Kim (1995) concluded that the framing of the consumer's involvement is consistent with those claims contained in the advertising message.

There are two types of consumer involvement framing. The first is affective framing, which concerns the subjective claims contained in the advertising message. The second is cognitive framing, which concerns the objective claims contained in the advertising message.

Recognition of advertising deception becomes more probable when there is consistency between the consumer's involvement framing and the type of advertising claims contained in the message. When consumers recognise this consistency, they become highly aware of the involvement, and therefore, it is more likely that they will recognise re advertising deception.

In light of the aforementioned, Table 9.2 clarifies the affective span of the involvement process as a behavioural variable mediating the process of recognising the advertising deception.

Table 9.2: The affective span of the involvement process in recognising deceptive advertising

Message Type	The advertising message built upon concrete aspects (objective)	The advertising message built upon non-concrete aspects (subjective)
Involvement Type		

Affective involvement framing	No consistency between message type and the consumer's involvement framing. Recognising advertising deception becomes more probable.	There is consistency between message type and the consumer's involvement framing. Recognising the advertising deception becomes less probable.
Cognitive involvement framing	No consistency between message type and the consumer's involvement framing. Recognising advertising deception becomes more probable.	There is a consistency between message type and the consumer's involvement framing. Recognising the advertising deception becomes less probable.

9.2.5 Beliefs

After undergoing the previous cognitive processes, the consumer might form a belief that the claims contained in the advertising message are connected to the traits of the product advertised. Should the advertising message be deceptive, the beliefs which are formed as a result of exposure to it will be deceptive (Armstrong & Russ, 1979).

In light of the behavioural trend to determine the advertising deception, those deceptive claims which were formed as a result of the deceptive message, are very important in the consumer's purchasing decisions.

Gardner (1975) uses beliefs as a measure to recognise advertising deception of the consumer based on the assumption that the normative beliefs, which experts identify in the span of the product, determine the level at which beliefs are about traits of the product for the consumer. When the consumer is exposed to the DA message, beliefs formed by the consumer are raised about the normative beliefs.

Armstrong (1979) also uses beliefs as a measure to recognise the advertising deception for the consumer based on the beliefs formed by the consumer after exposure to the DA message.

Dyer & Kuehl (1978) concluded that we must depend on the beliefs which the consumer formed, after exposure to the DA message, and that by the consumer's exposure to the corrective ad, belief about the traits of the product is still at a level higher than that before exposure to the DA message.

Beliefs express the reaction between the cognitive processes before the formation of those beliefs. Those processes are: recognition, attention, comprehension and prior knowledge.

If the prior processes cause advertising deception to the consumer, beliefs are considered a critical stage in the occurrence of the advertising deception; due to the fact that if the consumer does not believe in the presence of traits connected to the product in the advertising claims which are included in the advertising message, it is not probable that the advertising message would alter the purchasing decisions made by the consumer.

Due to the important role that beliefs play in the recognition of DA, some researchers maintain that pufferies are considered non-deceptive claims, due to the assumption that the consumer does not accept the credibility of those claims. This is dependent upon the nature of the advertised products and the consumer's prior knowledge of traits of the advertised products (Preston, 1976).

If beliefs are considered a critical stage in recognising the advertising deception, those beliefs must be important or relevant to the consumer in order that they can depend on them to recognise the advertising deception (Armstrong, 1979).

In light of the aforementioned, Figure 9.4 depicts the affective span of beliefs as a cognitive variable mediating the process of recognising the advertising deception as a cognitive determinant of the advertising deception.

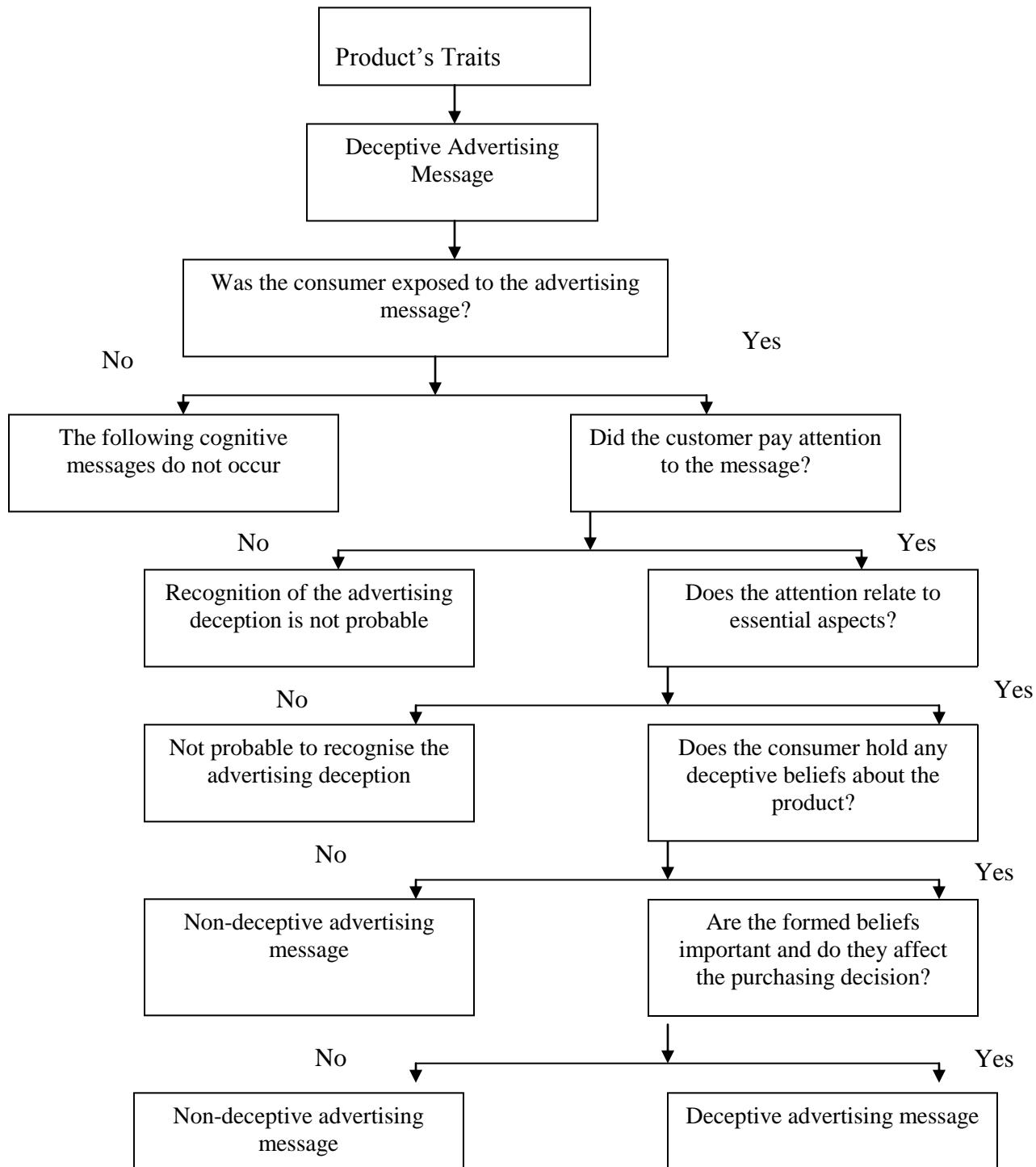


Figure 9.4: The affective span of beliefs in recognising deceptive advertising

9.3 Cyber-consumer protection inspired cognitive process

It seems entirely appropriate to have cyber-consumer protection law or cyber law that can be applied worldwide and across nation states to define and correct the imbalances between consumers and suppliers resulting from consumers' lack of or different levels of product knowledge. Cyberspace is in urgent need of a legal system that protects cyber-consumers across the nation and worldwide that is quite distinct from the laws applied for consumer protection, as these apply only to local consumers in realspace. Previous chapters established redress methods and potential guidelines or solutions for consumer protection from online deceptiveness and online fraud. Below is a suggested framework which is intended to strengthen consumer protection law and apply cyber law.

9.3.1 Online foreign lawyers

Because cyber-consumer protection involves international transactions or purchases, the online foreign lawyers redress method may be an effective solution for cyber-consumers. Usually, consumers making online international transactions are unaware of the consumer protection guidelines and consumer rights in foreign countries. The benefit of using an online foreign lawyer is that a consumer can investigate the vendor or website for any scams or previous fraud offences before making a purchase. Additionally, if a consumer has been caught in any sort of scam or fraudulent act, the online foreign lawyer may know what the rights of a foreign consumer and take action from there. The use of online foreign lawyers may therefore reduce the number of deceived consumers.

9.3.2 Online foreign public consumer protection authorities

Public consumer protection agencies available online allow cyber-consumers to seek help from online foreign public consumer protection authorities, and lodge complaints related to any deceptive or fraudulent behaviour.

9.3.3 Arbitration

This means that foreign consumers have access to an arbitration system that determines disputes by a private tribunal constituted for that purpose by the agreement of the disputants.

9.3.4 Online industry-based consumer dispute resolution schemes

Online industry-based consumer dispute resolution schemes are a form of tribunal that have been established specifically for an industry or sector such as banking, finance, insurance, telecommunications, etc.

9.3.5 Industry codes of conduct

Also known as voluntary codes of practice, industry codes of practice are bodies of rules and guidelines which purport to regulate industries from within in the sense that an industry establishes its own rules rather than having them imposed by the government, which also is used as the content of the law.

9.3.6 Escrow services

Escrow services refer to situations where a consumer makes an online purchase and the payment to the vendor is withheld by a third party to ensure the consumers receive their goods as promised by the vendor to the consumer's approval.

9.3.7 Online transaction insurance

Theoretically, online insurance is a type of traditional insurance for cyber-consumers to protect against any risks related to fraud and CCTs. The online coverage is analogous to the purchase cover insurance provided by visa credit card providers as an extended feature for cyber-consumers.

9.3.8 Trustmark

A trustmark, broadly speaking known as a web seal, is a sign or symbol displayed by a website to certify that the party granting use of the mark is notifying the general public that the website that displays the trustmark is one that complies with minimum standards.

9.3.9 Consumer education programs

Consumer education programs educate cyber-consumers to recognise fraudulent or deceptive behaviour, what the particular scams are and how they are practised.

9.3.10 Cyber-consumer complaints bulletin boards

Bulletin boards are websites that allows online consumers to share their online experience with other consumers and post complaints related to any online fraud or deception.

9.3.11 National deregistration

National deregistration is a government scheme by which only ‘accredited’ websites are allowed to operate within national boundaries, and others may be denied.

9.4 Conclusion

This chapter discussed the determinants of advertising deception recognition. In addition, this chapter examined the cognitive determinants as discussed in previous studies. Furthermore, it concluded that the cognitive processes which mediate the process of recognising advertising deception as cognitive determinants of the cognitive deception are determined in recognition (exposure to the DA message), attention, comprehension, prior knowledge, involvement and belief formation.

This chapter also discussed the affective span for each of those determinants. It concluded that the previous studies dealt with some variables which mediate the process of recognising advertising deception without coming up with a certain framing of the cognitive processes which mediate the recognition of the advertising deception.

As a result of the above, a framework was proposed for the cognitive processes which mediate the process of recognising advertising deception.

This chapter concluded that the more the consumer is repeatedly exposed to the DA message, the less chance there is to recognise the message as deceptive. Furthermore, the more experience or knowledge the consumer has about the product, the higher the chances of recognising advertising deception.

If the consumer has an interest in the product, the less chance there is of recognising advertising deception. Thus, when certain beliefs are formed by the consumer about the inclusion of certain traits in the product, the less are the chances of recognising advertising deception.

In the following chapter, the effect of the advertising deception on the purchasing decision taken by the consumer after exposure to the DA message is discussed.

CHAPTER TEN

NEW CYBER SOLUTIONS TO PREVENT LOSSES, FINANCIAL DAMAGES AND PSYCHOLOGICAL HARM TO CYBER-CONSUMERS

10.1 Introduction

The previous chapter established that redress for online fraudulent behaviour and deception in CCTs by means of litigation is not effective and explained why that was the case. This chapter considers whether redress for CCTs by means other than through litigation are effective and, as will be seen, finds that such redress methods as they currently exist are generally ineffective.

‘Redress’ here includes both reactive and proactive redress methods, for example, ADR and transaction insurance, respectively.

Redress for CCTs by means other than litigation includes online chargeback, online transaction insurance, and pressure applied through foreign lawyers or cyber-consumer protection bodies, and ADR. Such methods could also be classified according to whether they fall into the online protection-through-trust or an online protection-through-technology category. For example, a trustmark falls into the former, while cyber-consumer complaints bulletin boards or a ‘cybercourt’ (basing automated judgements upon decisional heuristics) would fall into the latter.

This will not be pursued further in this thesis other than noting the following. Trust measures are a form of online proactive consumer redress. Generally, they are effective as redress for CCTs only to the extent that they may prevent the failure of CCTs, and are of no assistance in any particular instance of CCT online fraud and online deception.

As noted in Chapter One, the major concern of this thesis is the measurement of consumer awareness and cognitive processes, financial costs, emotional and psychological effects of DA, and how the cyber-consumer can be protected from fraudulent behaviour and DA. The broader issues of consumer protection law for CCTs, and a comprehensive solution to the problems of failed CCTs, will inevitably involve laws beyond those merely provided for access to justice.

As CCTs involve contracts formed between consumers in different countries through cyberspace, the full context involves at least four areas of law. Thus there are links between redress, consumer protection, private international law, contract law and cyber law and they collectively make up the general context of a discussion of redress for CCTs.

10.2 Potential cyber solutions

The two criteria used to evaluate the various CCT redress methods (enforceability and simplicity) do not include ‘effectiveness’ as such, since methods 2 to 8 (current non-litigation-based redress — see Chapter Seven) were on the list of redress methods because they were already potentially effective to a minor extent but needed to be evaluated for their degree of effectiveness. However, the following methods, such as transaction insurance, are considered here because they are either not currently effective at all but could become effective, or they could be possible remedies but in fact will never be capable of assisting with cyberspace, online fraud and online deceptiveness problems with CCTs. They are considered here merely to explain what they are, and to clarify possible misconceptions with respect to their potential as remedies. The term ‘potential’, in the heading of this section, is thus used broadly, and as indicated in

Chapter Eight, the overall conclusions reached in Chapter Eleven are based upon the findings in respect of methods 2 to 8 only.

10.2.1 Online transaction insurance to support loss recovery

10.2.1.1 Description

In theory, this solution involves a type of online traditional insurance coverage for protection against risks associated with fraud and CCTs for individual online transactions or any number of online transactions over a given time period for a single online policy holder. The online coverage would be analogous to the purchase cover insurance provided by the Visa credit card (underwritten in Australia by Zurich Australian Insurance Limited), but would be sold directly to online consumers as an online insurance industry product and not as a credit card industry product. In fact, this solution could also be provided at present by being sold as an extended feature of credit card products for online consumers.

In 2010, the following insurers were approached in regard to this question through telephone conversations with manager or assistant-manager level officers: Allianz, AAMI, Australian Better Business Insurers, Zurich, QBE Mercantile Mutual, ING and East West Insurance Brokers. Not one provided coverage for so-called CCTs or knew of anyone who did. Zurich was aware of its connection with Visa, but advised that it did not provide such coverage directly to individual online consumers.

There may be a distinct segment in the insurance market waiting to be filled. There has been no previous solution here for cyber-consumers. In any event, if there is to be an CCT insurance provider in the marketplace, the degree of difficulty in finding them is surely not a problem for

online consumers in itself, as the majority of individuals are involved with insurance brokers to some extent, whether it is for motor, health, property or travel insurance, so online transaction insurance may be a potential solution.

10.2.1.2 Assessment

In regard to the enforceability criterion, online transaction insurance would not involve or require coercive power. The cyber-consumer would not compel the online vendor in any way as the remedy is provided by a third party. Insurers, however, pay on insurance claims at their discretion, and they could be compelled to do so through litigation.

In terms of the complexity criterion, the online transaction insurance redress method is comparatively uncomplicated, as compared with litigation. It would be fairly straightforward for cyber-consumers to engage insurers to protect their intended CCTs if suitable insurers become available.

10.2.1.3 Conclusion

Online transaction insurance does not involve or require coercive power over the vendor but insurers might be coerced, therefore its result for difficulty of enforcement is ‘low’. Finally, the method achieves a ‘low’ for complexity. It is likely then that online transaction insurance, if any were available, would probably be effective as a means of solving problems with low-value CCTs. Tabulated, the overall result for transaction insurance is as follows.

Table 10.1: Online transaction insurance

Method	Difficulty of enforcement	Complexity
9. Online Transaction Insurance	Low	Low

This method deserves a final observation when we consider how easily credit card online transaction security terms could be extended to better cover online fraud and online deceptiveness problems with CCTs. If online transaction insurance became available, it may be seen as a complete, permanent or fully satisfactory solution.

10.2.2 Trustmarks to prevent cyber losses

10.2.1.1 Description

Trustmarks are also known as “web seals”. Broadly speaking, there are two types of trustmark (or web seal). There is the ‘merchant credibility endorsement’ (ida.gov.sg, 2002), and there are trustmarks which relate to the trustworthiness of data being communicated via digital transmission channels. It is the trustmark of the former variety that is examined here.

A trustmark is a mark, sign or symbol displayed by a website to certify that the party granting use of the mark is notifying the public that the website that displays the trustmark is one that complies with minimum standards, such as conformity with specified privacy principles or conformity with specified dispute resolution procedures. Thus, as noted previously, it is a merchant credibility endorsement, and visitors to the website can verify whether or not the website is so certified by contacting the purported granter of the trustmark.

The website thus bears the ‘seal of approval’ of the party granting use of the mark, hence, in the relevant attribute, the website may be trusted by the cyber-consumer as being reliable. Examples of trustmarks are those issued by TrustE (truste.org, 2005), CPAWebTrust (cpawebtrust.org, 2005) and PricewaterhouseCooper’s ‘BetterWeb’ (pwcglobal.com, 2002).

These types of marks can be distinguished from the second type of mark issued by bodies such as VeriSign (verisign.com, 2005), which are concerned more with encryption, communications security or data security. The ‘TrustE’ trademark however, is limited to providing an endorsement concerning a website’s privacy policies only. Digital Enterprise (digitalenterprise.org, 2005), and is therefore of limited interest here.

The CPAWebTrust seal claims that any site displaying its WebTrust seal has “been certified by a specially trained and licensed public accounting firm, has disclosed its business practices, has been audited to prove the site actually follows those practices, and has met international WebTrust Standards for e-Commerce” (cpawebtrust.org, 2005). Examples of websites that bear the WebTrust seal are those of Ammbit.com, Comodogroup.com, and Ariba.com.

The BetterWeb seal was launched in 1999, and claims to be a Web standards program that addresses the areas where consumers perceive the most risk in online transactions: sales terms, privacy, security and customer complaint policies. Through a simple but rigorous process, online organisations such as retailers and service providers can obtain a licence to display the seal.

The general nature of a trustmark is that of an endorsement from a specialist, independent third party whose continued existence depends itself on being a source of reliability. Thus trustmark issuers are displaced ‘vertically’ from those receiving marks, and these issuers may be further distinguished from ‘horizontal’ endorsement that can be found in such systems as that employed

by eBay (ebay.com, 2005), where trustworthiness is conferred by consumers themselves by the process of consumers rating the trading system or the sellers of goods for trustworthiness (ida.gov.sg, 2002).

In respect of trustmarks awarded vertically, the sub-variety of trustmark of interest here, industry commentators have noted that “these top-down accreditation systems have done their job very well, it must be said”, while of the horizontal variety it was noted that “the peer accreditation system works well on the internet because there is in existence a loose and highly democratic community of people who have the same interests.” In respect of such comments such as ‘done their job very well’ and ‘works well’, which are undoubtedly true in some sense, it should be noted that these were not only subjective assessments made without supportive or explanatory data, but were probably also relativistic, in that they were made as comments on a phenomenon evaluated in comparison to a situation where trustmarks did not exist at all (ida.gov.sg, 2002).

Furthermore, the results of this thesis’ research convinced the researcher that trustmarks are advantageous to cyber-consumers and online vendors alike. The cyber-consumer’s protection is undoubtedly enhanced and it is also likely that a certified online vendor will experience an increase in sales. With a suitable incorporation of the e-commerce trustmark into legislation, B2C e-commerce could find a firm foundation for further development (bileta.ac.uk, 2002).

In other words, the method needs the coercive force of law as yet not applicable to it.

10.2.1.2 Assessment

The emphasis added in respect of the previous statement also suggests that the problem with trustmarks as they currently stand, of either vertical or horizontal variety and irrespective of how

many practical examples of the use of trustmarks that may be considered, is the same. While the chances of cyber-consumer satisfaction is increased by dealing with endorsed vendors, the mere possession of a trustmark does not preclude the possibility of a cyber-consumer experiencing fraud and deception problems. Furthermore, there is no inbuilt adjudication and enforcement mechanism in relation to the possession of a trustmark, and while the trustmark undoubtedly improves the situation for cyber-consumers, the bottom line is that the cyber-consumer is still ultimately at the mercy of the online vendor's hostility in the event of dispute.

A question for the future, then, is whether developments in trademark technology could improve problems with the kind of online transaction security offered by trustmarks.

Assessed against the enforceability criterion however, the method may be to some extent effective in relation to problems with CCTs; the method is exclusively concerned with pre-contractual representations and thus has no coercive force at all unless an online deceived consumer was willing to sue the online vendor or the trademark issuer for negligent misrepresentation or similar deception.

According to the complexity criterion, the method is very simple as it involves nothing more than the display of the trademark issuer's seal on the vendor's website.

10.2.1.3 Conclusion

Regarding difficulty of enforcement, the trademark method does not have any significant post-transaction coercive power beyond the possibility of suing for misrepresentation. Its result for difficulty of enforcement is therefore 'low'. Finally, the method achieves a 'very low' for

complexity. Trustmarks might be to some level effective as a means of solving problems with CCTs. Tabulated, the overall result is represented in Table 10.2.

Table 10.2: Trustmarks

Method	Difficulty of enforcement	Complexity
10. Trustmarks	Low	Very Low

10.2.3 Consumer education programs to prevent deception

10.2.3.1 Description

Cyber consumers can be educated to recognise fraudulent or deceptive advertisements, what particular scams there are and how they work. They can be educated on specific issues regarding the online purchasing of goods such as online privacy issues; applicable law; properly identifying the online vendor and the contractual subject-matter; keeping records of online transactions; vendor refund online policies and online warranties; delivery time, costs and currencies; risks inherent to cross-border purchases; what cyber-consumers can do if difficulties arise; and cyber-consumer information sources available on the Internet itself. Cyber-consumer education websites already exist to assist with these issues (accc.gov.au, 2005) and cyber-consumers can be referred to them by vendors' websites, which could be required to be linked to such websites.

10.2.3.2 Assessment

As a means of online protection, cyber-consumer education is very important to ensure that the consumer is aware of any fraudulent behaviour or deception in order to avoid the above mentioned procedures. Hence, it is important that it be recommended and promoted. Consumer education is a means of preventing the failure of a CCT; however, it is of no use after the event in pursuing redress when a CCT has failed.

Therefore, cyber-consumer education is essential. As previously mentioned in Chapter Five, a suggested framework for the cyber-consumer to determine online DA is recognition (exposure), attention, comprehension and prior knowledge, involvement and beliefs.

However, when assessed according to the enforceability criterion, while the method of cyber-consumer education may possibly be very effective in respect of pre-transaction problems with CCTs, the method is concerned exclusively with pre-contractual cyber-consumer advice and has no coercive force at all.

Assessed by the complexity criterion, the method is very simple. The method involves nothing more than the offering of cyber-consumer advice, typically through various websites and perhaps school educational programs.

10.2.3.3 Conclusion

Consumer education achieves an overall result as follows. The method does not involve either coercive or persuasive power; its result for difficulty of enforcement is therefore ‘low’ and the method achieves a result of ‘very low’ for complexity.

Therefore, cyber-consumer education is possibly very highly effective as a means of solving online fraudulent abuse, online deception, and problems related to CCTs. The overall results are presented in the table below.

Table 10.3: Consumer education

Method	Difficulty of enforcement	Complexity
11. Consumer Education	Low	Very low

10.2.4 Cyber-consumer complaints bulletin boards

10.2.4.1 Description

A cyber-consumer complaints bulletin board is a website that allows for the posting of online consumer complaints noticed by anyone, for access by others, via the Internet. They are analogous to physical notice boards to which online complaints, online warnings or other notices may be attached regarding online deception and fraudulent behaviour. For example, by posting their complaints on the Internet through a cyber-consumer complaints bulletin board, deceived online consumers can publicise their grievances to thousands of other cyber-consumers. This lawful and simple method affords cyber-consumers increased leverage in resolving disputes.

A typical cyber-consumer complaints bulletin board works as follows.

On a weekly basis, the proposed website publishes the ‘Top 10’ list of complaints received on its site. The complaints chosen reflect the seriousness of all complaints, the ludicrousness of the processes involved and, in many cases, the simplicity of the fix. Companies are then contacted,

and an official detailed complaint is forwarded directly to the company. This speeds up the resolution process. When the Top 10 list is published, the company responses are also included. ‘No Reply at Time of Press’ is published if a company chooses not to respond.

The method is one way by which a cyber-consumer complaints bulletin board exposes offenders.

10.2.4.2 Assessment

The usefulness of a cyber-consumer complaints bulletin board is limited to only having increased leverage through the public notification of a cyber-consumer’s complaints. Certainly an online vendor will not appreciate negative public commentary, may be deeply embarrassed or shamed by it, and may even provide the answer the cyber-consumer is looking for as a result, but that remains a long way from the situation an online vendor would face following an unfavourable judgment from a court with effective enforcement powers. A shamed online vendor would still be acting voluntarily if they provide the solution the cyber-consumer is seeking.

Furthermore, a cyber-consumer complaints bulletin board user “cannot determine from those cyber-consumer complaints bulletin board websites the likelihood of a future negative interaction with a particular trader. They can only discover prior to the existence of such an interaction”, (Gillette, 2002). Thus, cyber-consumer complaints bulletin boards are merely indicators of how online vendors might behave in the future, and make another contribution to cyber-consumer education.

Therefore, as with other potential solutions examined in relation to the failure of CCTs, there is no complete solution here, as there are no legal sanctions involved. Furthermore, an unfair vendor, if things get really bad, can simply close up and re-open elsewhere under a different

name. This method is helpful, however, by adding to the range of options cyber-consumers have as an effective remedy.

Assessed against the enforceability criterion, the method is completely effective in respect of post-transaction problems with ICTs — the method is exclusively concerned with pre-contractual consumer commentary, has no coercive force at all but may have some premature force.

According to the complexity criterion, the method is extremely simple. The method provides nothing more than consumer commentary.

10.2.4.3 Conclusion

Consumer complaints bulletin boards achieve an overall result as follows. This method does not involve any coercive power but it may produce a result. There may be a small amount of persuasive power in the threat of the consumer shaming rogue vendors. Its result for enforcement power is therefore ‘very low’. The method results in a ‘low’ for complexity (but not a ‘very low’) as there may be some degree of difficulty learning how to access and post complaints to cyber-consumer complaints bulletin boards.

Cyber-consumer complaints bulletin boards are possibly effective as a means of preventing online fraud and deception problems with CCTs. Tabulated, the overall result is as follows.

Table 10.4: Consumer complaints bulletin boards

Method	Difficulty of enforcement	Complexity
12. Consumer Complaints Bulletin Boards	Very low	Low

10.2.5 National deregistration for fraudulent behaviour

10.2.5.1 Description

‘National deregistration’ refers to the possibility of some sort of scheme by which ‘accredited’ websites could be allowed to operate within national boundaries, and by which all others are denied the right to do so.

10.2.5.2 Assessment

In terms of government regulation in this area, while concerned with online content regulation (e.g. pornography), an example of how effective this could be can be seen in the *Broadcasting Services Amendment (Online Services) Act 1999* (Cwlth). This attempt at government cyberspace regulation was described in August 1999, by Professor Nadine Strossen, then President of the American Civil Liberties Union as making Australia a “global village idiot” (exn.ca, 2002). Apart from the censorship issues, Strossen (1999) argues this because of the alleged technical impossibility of regulating cyberspace in this way, when website operators could simply relocate sites wherever they wanted.

Thus, the idea of deregistration would have limited effect where unscrupulous vendors can play a cyberspace version of the ‘shell game’ (now you see me, now you don’t) and the issue is really whether or not effective redress can be obtained after the fact (i.e. after online fraud and deceptiveness related to CCTs). Deregistration is, in fact, just a form of pre-emptive consumer education, and provides no remedy *of itself* for problems with CCTs, which could still be caused by accredited online vendors.

In terms of the cost criterion, the national deregistration redress method is likely to be free of charge to the consumer but may involve some cost in submitting evidence to authorities in support of a request to deregister an offending website.

Assessed against the enforceability criterion, the method is not effective as it does not involve actual coercive power in respect of obtaining a remedy for a breached CCT, but it may have some prospective deterrent power if enough deceiving websites are deregistered for such offences. Regarding its complexity, the method is comparatively simple; all that would be involved would be the submission of a request for deregistration with supporting documentation.

10.2.5.3 Conclusion

The overall result for the national deregistration redress method is as follows. This method may to some extent involve actual coercive power in respect of obtaining a remedy for a breached CCT and may also have some prospective deterrent power; its result for ease of enforcement is therefore ‘very low’. Finally, the national deregistration method of redress result for complexity is ‘low’. National deregistration then, may possibly be more effective as a means of solving problems with CCTs. Tabulated, the overall result for national deregistration is as follows.

Table 10.5: National deregistration

Method	Difficulty of enforcement	Complexity
13. National deregistration	Very low	Low

10.3 Conclusion

This chapter commenced by noting a concern with practical issues and alternative scenarios associated with CCTs. It further noted the concern with scenarios which result specifically in online fraud and deception related to CCTs in the context of existing methods.

In terms of the methods or potential solutions and redresses established in Chapter Eight, the methods expressed as a table were assigned to the forms of redress for CCTs considered in this chapter in Table 10.6. As a preliminary, however, note that there is a difference between ‘current’ methods (2 to 8) and ‘potential’ methods (9 to 13).

Methods 2 to 8 were on the list of redress methods because they are already effective to some extent but needed to be evaluated for their degree of effectiveness. Methods 9 to 13 were either not currently effective at all but could become effective (transaction insurance), or they (the remaining methods) might be thought of as being possible remedies assisting with online fraud and deceptiveness problems with CCTs.

Table 10.6 Evaluation of cyber-consumer protection and CCT redress methods

Method	Difficulty of enforcement	Complexity
--------	---------------------------	------------

Table 10.6.1 Current methods redress

2 Foreign lawyers	High	Acceptable
3 Foreign public consumer protection authorities	Very High	Acceptable
4 Alternative dispute resolution/online dispute resolution	High	High
5 Arbitration	Acceptable	High
6 Online industry-based consumer dispute resolution schemes	High	High
7 Industry codes of conduct	Very High	Acceptable
8 Escrow services	Low	High

Table 10.6.2 Potential solutions and redresses

9 Transaction insurance	Low	Low
10 Trustmarks	Low	Very Low
11 Consumer education	Low	Very Low
12 Consumer complaints bulletin boards	Very Low	Low
13– National deregistration of vendor websites	Very Low	Low

In examining these issues, current and potential remedies for these problems in the form of cyber-consumers and CCT have been considered, ranging from the appointment of lawyers and

appeal to cyber-consumer agencies in the country of the unfair vendor, to the potential of ADR, escrow and trustmarks, to the potential benefits of cyber-consumer education schemes and cyber-consumer complaints bulletin board systems, and to the potential benefits of industry codes of conduct and national schemes of registration and de-registration of websites. All were considered and, in every case, were found at some point to be either effective or non-effective as a remedy for online fraud and deception related to CCTs.

Given the ineffectiveness of current methods then, perhaps answers may be sought in hypothetical legal remedies: perhaps the only source of effective remedies for CCTs may be either of two possibilities. First, problems associated with national private international law rules might be reduced or eliminated so that jurisdiction issues become irrelevant.

A second approach could be to side-step such problems altogether, through the creation of a cyber-consumer redress/protection solution to provide some sort of globally-harmonious and accepted scheme of litigation for CCTs. A cyber-jurisdiction is perhaps one means by which such a convention could be administered to provide access to justice that is adequate enough for CCTs.

For our purposes, a ‘cyber-jurisdiction’ is a general term for a court whose processes and powers are available to litigants via the Internet, and implies the use of at least some of the following features: technology that allows litigants and related parties, and their representation, to be connected to the court via the Internet without their physical presence in any particular place, at any relevant time (pre-trial through to post-trial) in the processing of a matter before the court; the conduct of related court proceedings electronically; monitors for judges, counsellors, jurors

and witnesses; video conferencing; and digital evidence presentations—in other words, advanced ODR but with enforcement powers.

CHAPTER ELEVEN

EVALUATION OF THE PROPOSED CYBER-CONSUMER PROTECTION FRAMEWORK

11.1 Introduction

The previous chapter proposes and evaluates several cyber-consumer protection methods or potential solutions to prevent deception in online advertising. This chapter identifies the DA from behavioural and legal perspectives. Consumer awareness of DA differs from one consumer to another; therefore in this section, the consumer's awareness is measured using a framework that measures DA from both the legal and behavioural perspectives. Also, this chapter uses a framework to determine ad effectiveness and DA.

11.2 Identifying deceptive advertising: a behavioural perspective

As a result of criticisms of identifying DA by applying legal criteria, and criticisms against legislation for monitoring ads and the prohibition of deceptive advertisements, researchers have attempted to define DA in terms of the behavioural aspects or cognitive processes which mediate the way in which the consumer receives the advertising message. The following is an elaboration and discussion of those contributions.

Howard and Herbert define DA as arising when an ad contains a group of symbols that have different interpretations to that of the consumers and that one of those interpretations is false (Gardner, 1975). It is clear that this definition has identified one aspect of deception — that one of the symbols might be false — but DA does not result from symbols only. Thus, the definition does not include all possible sources of deception.

Aaker (1974) defined DA in terms of the cognitive processes through which the message is received. He sees that deception takes place when the ad enters the consumer's cognitive process, leading to a cognitive process about a product characterised as being either different from the fact of the matter, or influencing purchasing behaviour, which then leads to harm to the consumer.

This is the first definition which includes the cognitive processes, but it does not identify the components of the cognitive process. Nor does the definition identify sources and characteristics of the deceptive claims mentioned in the ad, or the so-called deceptive action. The definition does not treat DA as something which might harm the consumer; rather, it determined the actual harm as a condition of DA.

Gardner (1976)'s definition seeks to encompass both the 'operational' and 'behavioural' aspects: deception in the ad exists if the ad leads to the creation of impression(s) or belief(s) which are false or deceptive to the consumer. They are different from those he expects to be present when reasonable knowledge is available for the consumer about the subject (product) of the ad.

Gardner's (1976) definition is important and might be reliable in developing a comprehensive definition of DA, while Aaker's (1974) definition does not mention the possible effect of DA on the consumer's purchasing decision.

Armstrong and Russ (1975) conclude that DA takes place when the consumer perceives or believes in the existence of certain traits in the advertised product as a result of exposure to the DA message, by virtue of the explicit and implicit claims it makes, provided that this claim is relevant to the consumer. This definition ignores the possible effect of the ad's deception on the

consumer's purchasing decision; it depends on product experts and is not suitable for detecting DA.

Olson and Dover (1978) define DA as being an ad which leads to the formation of false beliefs, provided that the following conditions are present: it is possible to identify those false beliefs and that those false beliefs were formed as a result of the exposure to the deceptive ad, and not as a result of any other reason.

It is worth noting that Olson and Dover's (1978) definition, instead of relying on the beliefs which the consumer forms as a result of watching, listening to or reading the ad, do not identify the possible effects of false ads, which are formed as a result of deception in the ad, and inform the consumer's purchasing decision.

Gaeth and Heath (1987) define DA as that gap between the real performance of a product and the consumer's beliefs about the product's performance formed as a result of exposure to DA. It is clear that this definition is not suitable since it does not include the deceptive action or the characteristics of the DA message. It also connects the advertising deception with the product's performance, since the product's performance is identified by functionality only. This definition implies that DA probably has no effect on the consumer's purchasing behaviour. This means that the occurrence of DA is connected with the performance of the product (which is dependent on many factors), and not connected to characteristics of the product. Thus, the advertising message might be credible (not deceptive), but the consumer might have formed a belief, as a result of the product's non-performance, that the advertising message is not credible (deceptive).

A review of these definitions indicates the following:

- The definitions which depend on experts to determine deception in the ad cannot be reliable in developing a comprehensive behavioural definition of DA.
- Some definitions focus on the deceptive action performed by the advertiser to deceive the consumer. Other definitions focus on the effect of DA on the cognitive processes of the consumer when receiving the advertising message.
- All of the definitions, except Aaker's (1974), include the effect of deception as represented in the actual harm done, or the consumer's assessment of the product after trying it. Hence, they are not considering the ad and its effect on the purchasing decision as a probable instance of DA.
- The definitions which include the cognitive processes which mediate DA use different cognitive components such as perception, belief, impressions etc.
- None of the definitions presents a comprehensive definition of DA which includes the cognitive processes performed by the consumer to understand and perceive the advertising message and the effect of deception on the consumer's behaviours and purchasing decisions.

Table 11.1 presents a summary of the definitions of DA, including that of the FTC.

Table 11.1: Summary of definitions of deceptive advertising

Components definition	Source of deceptive advertising	Causes of deceptive advertising	Cognitive Processes				Purchasing behaviour	
			Comprehension impression awareness	Belief	Importance of the claim in affecting the consumer	Comparing the claim with reality	Probable effect	Actual effect
1 FTC Definition (1974)	Revealing information or non-real deceptive revelation				Claims are important for the consumer.		They affect the purchasing behaviour	
2 Haefner (1972)	Deceptive ad						Credible evaluation of the ad depending on experts in the product's field	
3-Webster (1974)	Deceptive ad	Misrepresentation of facts (deception)						
4 Aaker (1974)	Deceptive ad		Cognitive processes happen as a result of exposure to the ad				Evaluation of cognitive processes is different than the truth.	Affecting the purchasing behaviour and causing harm.
5 Gardner (1975)	Deceptive ad		Formation of impressions or beliefs					
6 Armstrong & Russ (1975)	Explicit or implicit claims in deceptive ad		Beliefs or awareness are formed about ad claims		Ad claims suitable for the consumer.	False ad claims		
7 Jacoby & Small (1975)	Deceptive ad	Contents, components them, context in the field of medications	Impressions or beliefs are formed among some doctors.	Affecting a certain percentage of doctors.	Impressions criticism are false or unsatisfying			
8 Olson & Dover (1978).	Deceptive ad		The consumer forms impressions			Beliefs formed about the ad are different than reality.		
9 Gaeth & Heath (1987)	Deceptive ad		Beliefs are formed among consumers.			Beliefs formed will differ as a result of advertising the truth		

11.3 Identifying deceptive advertising: the legal perspective

The efforts of the FTC in drawing attention toward practices of DA have led to direct studies of DA, finding that the efforts and special resolutions of the FTC go some way to preventing advertisements from being deceptive. Hence, the FTC's methods do contribute to reducing the amount of DA in advertisements generally.

However, advertisers under the pressure of legislation issued against DA turned from blatant deception to more subtle deception, which is difficult to identify, in order not to avoid facing legal action or decisions issued by the FTC, and, accordingly, the power of legislation to prevent deceptive practices in ads has decreased over time.

The methods used by the FTC (affirmative disclosure and corrective advertising, discussed below) contribute to its limited effectiveness. It is worth noting that there is another method, counter-advertising, whereby the FTC allows anyone to publish an advertisement countering the ad deemed by the FTC as being deceptive. This method is not used on a large scale.

11.3.1 Affirmative disclosure

This method provides that if the advertisement, from the perspective of FTC experts, is not providing enough information to allow the consumer to take a sound decision concerning the product subject of the ad, the FTC issues a decision obligating the company to make an 'affirmative disclosure', which takes the form of an ad which contains unambiguous terms and additional information relative to the advantages and limitations of the product.

Cohen (1985) criticises this method, accusing it of being ineffective, since the consumer can ignore exposure to that information in full. It is also probable that the mental mismatch

between the consumer and the content of the affirmative disclosure might lead to not understanding the information in full.

11.3.2 Corrective advertising

If affirmative disclosure implies more information being made available for the consumer by offering information which was not in the previous ad, the corrective ad includes deleting or removing the consequences of exposure to the information included in the previous advertisement.

Dyer and Kuehl (1975) conclude that the beliefs connected to the advantages of a product remain at a high level as a result of the deceptive ad, despite the corrective ad being used; the corrective ad is not successful in removing the effects of DA.

Among the most important challenges of the legal trend in facing DA is the determination made by Gardner (1975) that the FTC does not have an understanding of the deception from the behavioural perspective. Its decisions reflect its preoccupation with the act of deception rather than the effect of the advertised message on the consumer.

Gardner (1975) also criticises the legislative method used by the FTC, which is dependent on case-by-case rulings. This has led to a rise in the number of laws related to cases of DA so that the legal basis became ‘prescriptive’, so it is difficult to prove neutrality.

Preston criticised the fact that ‘puffery’ was not subject to FTC monitoring since, although those pufferies are not facts, they still express the seller’s opinion, without indicating as much to the consumer. It is probable that the consumer receives the opinions as facts which subsequently influences purchasing behaviour.

Horton (1994) also criticises FTC policy because it focuses on the ability of an advertisement to deceive the consumer more than on the effect the ad claims have on the consumer; that is, the FTC focuses more on the actual advertisement rather than the consequences of DA. The DA is connected to the advertisement's ability to deceive while the deceptive ad depends on the consumer's awareness or non-awareness of DA.

We can see that the legal dimension has some aspects which can be dependable in coining a definition of DA, which takes into consideration the behavioural aspects of the consumer on the one hand, and the deceptive action performed by the advertiser via the advertising on the other. It also includes a definition of DA.

The FTC has an understanding, albeit implicit, of a certain type of cognitive process performed by the consumer when exposed to the advertised message.

Figure 11.1 illustrates the steps used in assessing advertising claims in a legal sense.

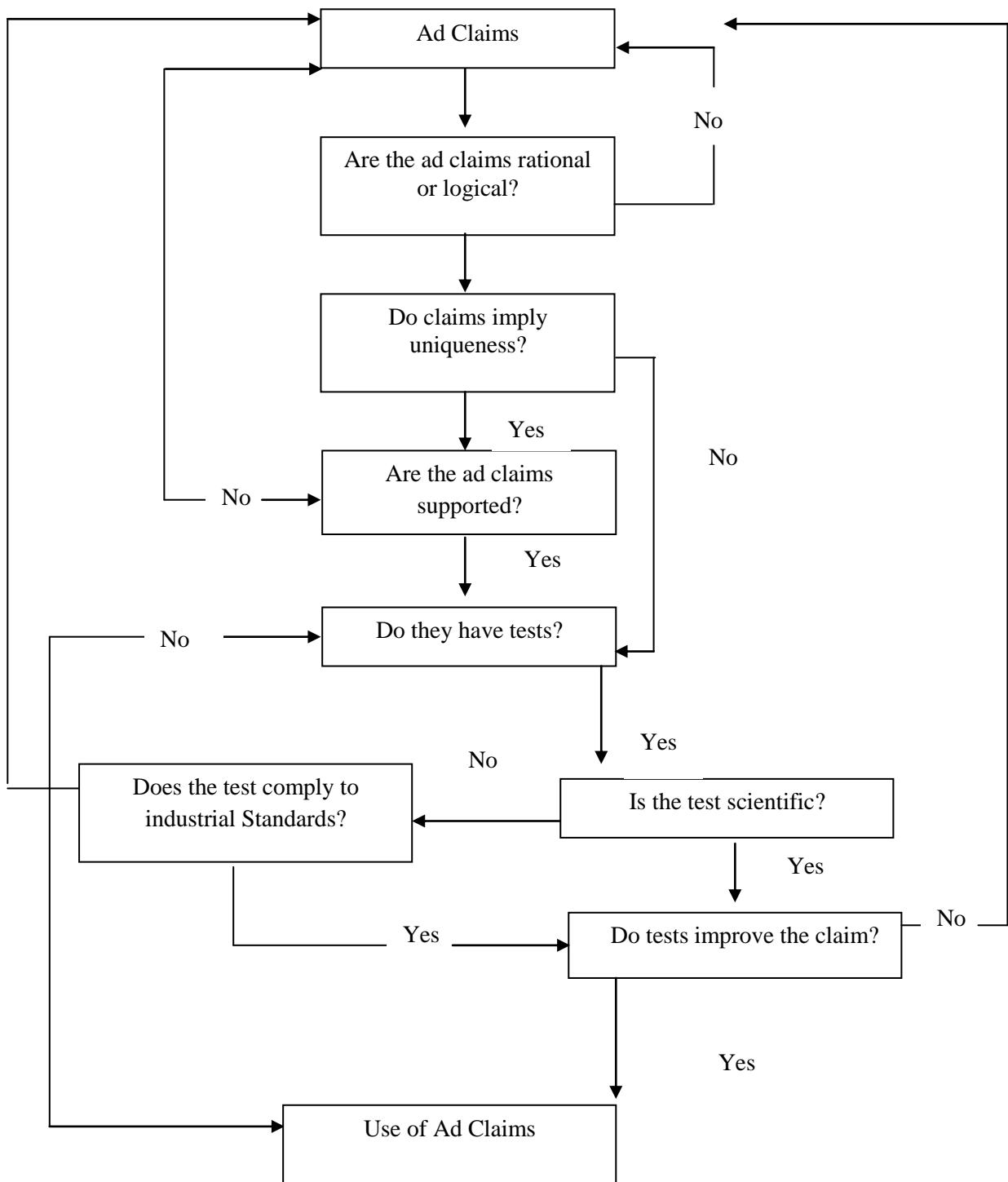


Figure 11.1: The steps of assessing advertisement claims using legal trends

11.4 Measuring deceptive advertising

Many methods can be used to determine DA. The nature of measuring the concept of DA is dependent on the method used.

11.4.1 Measuring deceptive advertising: the legal dimension

In order to determine whether an ad contains deception and in order take subsequent action, the FTC applies a set of standards to the advertised claims, whether these be explicit or implicit. The FTC focuses on determining the deceptive advertisement, and ‘False advertising’ occurs when the explicit claims of the advertisement about the characteristics of the product are different from the reality.

For example, if the advertisement mentions that a product is made of solid gold when it is gold-plated only, the claim indicates that one characteristic of the product— being made of solid gold— could be proved false by means of examining the product (Preston, 1986, 1987).

The FTC depends on product experts to measure DA instead of standards which could determine the deception in an advertisement. The determination of DA by experts provoked huge disputes between researchers in the behavioural sciences. It was also opposed by the advertising companies whose advertisements were determined as being deceptive, where decisions issued by the FTC concerning the applications of those standards to advertisements were different.

According to the FTC method, the advertisement is judged as being deceptive in light of the context or the environment in which it is publicised. Hence, despite the same advertising claims being made, whether or not deception exists depends on the context in which that

claim is used, which indicates that a certain advertisement may be deceptive in one context and not deceptive in another (Preston, 1986).

In light of these criticisms of the dependence on product experts to determine deceptiveness in advertising, the FTC conducted a consumer opinion survey to complement the opinion of experts and not as a substitute. The survey scales used by FTC were very biased; they conformed to the opinion of FTC experts regarding the deceptiveness of an advertisement. The FTC prepares a list including a number of questions and gives it to one company to collect answers from consumers. It uses closed questions requiring only a ‘yes’ or ‘no’ answer. This, in turn leads to the consumer’s bias by answering ‘yes’ for DA (‘yes-saying bias’) (Preston, 1986).

It is worth mentioning that the legal methodology for determining DA by means of dependence on false advertising as a basis for the probable advertising deception is not sufficient to determine DA.

There are three sources of advertising deception:

- false advertising, which could be determined by product experts
- the consumer does not understand the advertisement’s message because the claims mentioned in the ad imply meanings different than those understood by the consumer
- the consumer forms beliefs related to the characteristics of the product which are different than the actual ones characteristics.

DA might be the result of at least one of the following:

- false claims about the product’s characteristics;
- the consumer conceives claims about the product in a different manner than that presented in the advertising message, indicating misunderstanding of the advertising message by the consumer (the receiver of the

advertising message) or the miscomprehension of the message; - the consumer forms beliefs about characteristics of the product different from the reality.

Dependence on the legal method for determining DA leads to a generalised judgment that includes other ads, although this is not the case from the consumer's viewpoint. False advertising does not necessarily involve a deceptive ad—the relationship between the false advertising message and the extent to which the consumer is deceived take different shapes.

Table 11.2 clarifies the differences between the deceptive advertisement and the false advertisement.

Table 11.2: The differences between a false advertisement and a deceptive advertisement

The Ad Message	False	Truthful
Consumer's Comprehension		
Deceptive	Claims made in the message are false (leading to false beliefs by the consumer)	Claims made in the message are truthful literally and technically (leading to false beliefs of the consumer)
Non-Deceptive	Claims made in the message are false and the consumer identifies the ad via cognitive processes as providing a false advertising message.	Claims made in the message are truthful and the consumer identifies the ad via the cognitive processes as providing a truthful advertising message.

In light of the above, we cannot depend on legal methodology to determine DA independently or separately from the study of the cognitive processes performed by the consumer as a result of exposure to the advertising message.

11.4.2 Measuring advertising deception: the behavioural dimension

In light of the shortcomings of legal methodology in measuring advertising deception, researchers have offered some contributions which focus on measuring DA from the consumer's perspective.

The behavioural dimension used to measure DA uses the normative belief technique. Gardner (1975) was the first to present this method. It was also used by Dyer and Kuehl (1978) in studying the effect of the corrective ad on consumers' beliefs.

To determine DA, the normative belief technique uses the following steps:

1. Determining the functional characteristics which are connected to the product by means of a group of experts.
2. Measuring the extent to which beliefs are connected to the functional characteristics of the product (normative beliefs) by extracting the opinions of a sample of consumers.
3. Examining some deceptive advertisements determined as being deceptive through applying agreed-upon standards.
4. Measuring the beliefs of a sample of customers about the functional characteristics of the product after exposure to the predetermined deceptive advertisements.
5. Comparing the normative beliefs with the beliefs formed after exposure to the deceptive advertisement (comparing steps 2 and 4).
6. Deeming the advertisement deceptive if there is a fundamental difference between the belief formed as a result of exposure to the deceptive advertisement and the normative belief.

The normative belief technique implies that there is a natural misunderstanding accompanying the communication process connected to the ad; therefore a comparison between the beliefs connected to the product's characteristics, which were formed as a result of exposure to the deceptive ad, with the normative beliefs connected to the characteristics of the product, are required.

Thus, the normative belief technique is accurate in measuring deception in an advertisement, as illustrated in Figure 11.2.

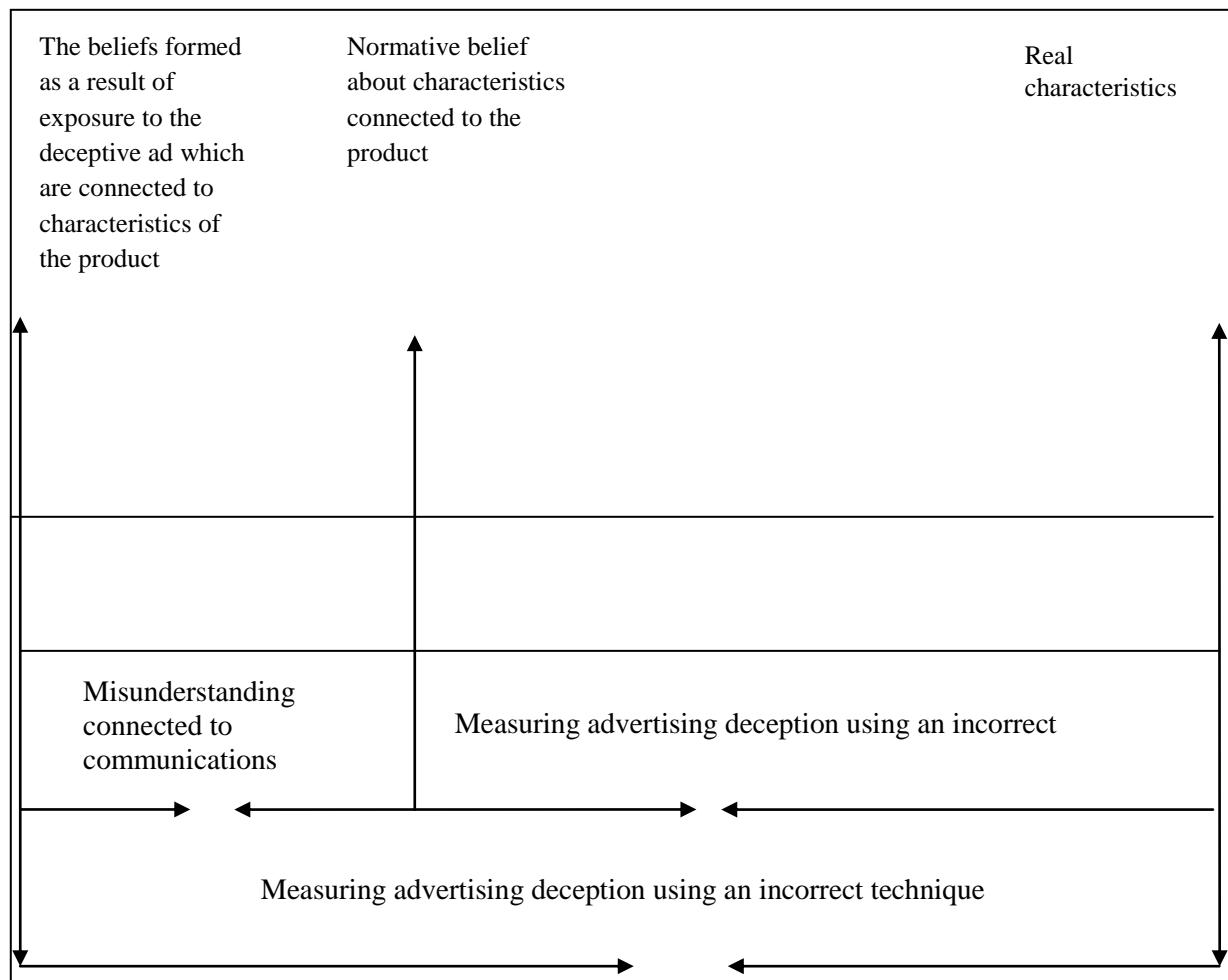


Figure 11.2: Normative belief technique

The normative belief technique is not without criticism. In measuring DA, it focuses on functional characteristics—the material and objective characteristics of the product. DA, on the other hand, can occur as a result of the beliefs which are shaped by the product's

evaluative characteristics—the non-material and personal characteristics connected to the consumer.

The normative belief technique does not consider the extent of the importance of the beliefs which take shape as a result of the consumer's exposure to the deceptive ad prior to making the purchasing decision.

The normative belief technique depends on specific product experts to determine the functional features. Although these are not sufficient to determine deception in the ad, opinions of product experts are different from the opinions of consumers.

11.5 Determining advertising effectiveness and deceptive advertising

The advertiser using DA, either through explicit or implicit ad claims, tries to realise the goal of the advertised message—raising sales—and accordingly, from the advertiser's perspective, the deceptive advertisement is linked to the effectiveness of the message.

From another perspective, the advertiser tries to convince the consumer to buy the product by means of affective and cognitive processes. Accordingly, the advertised message, which depends on persuasion, tries to find a way by which the consumer will become more interested in the product. As the consumer becomes interested in the content of the message, purchasing decisions are affected (Darley & Smith, 1993).

Petty (1983) determines the affective and cognitive processes of persuasion as being central or peripheral, as described below:

- The persuasive process can occur in the central route of persuasion in the human mind.

The persuasive processes occur in the central route of persuasion in the human mind. They are the processes which take place when the consumer has enough “attention” for the exposure of the ad message- which includes ad claims- be they explicit or implicit ad claims. Those processes occur when the consumer is at a high level of involvement in the information included in the ad’s message about the product.

Accordingly, the meanings implied in the ad message lead to certain beliefs connected to characteristics of the advertised product. Those beliefs, then, transform to inclinations toward the product where the purchasing intentions become higher.

- The persuasion process can also occur in the peripheral route of persuasion in the human mind. In this case, the consumer has a lower level of involvement with the information included in the advertising message.

Accordingly, the content of the message does not lead to the formation of certain beliefs or inclinations toward the product, or any purchasing intentions; instead the process leads to the formation of orientations toward the ad itself by virtue of the effects produced by what is implied in the message.

Advertisers resort to the use of sound effects or the use of certain figures in an effort to persuade the consumer to form positive orientations, or inclinations, toward the ad itself, which later on affect the formation of orientations toward the product.

Studies indicate that the persuasion processes, which occur in the central route of persuasion in the human mind, take place when the advertising message has factual content and when it is related to the tangible or objective facts about the product.

This message is noticed more than that which is built on emotional content. The advertising message which is built on facts leads to the formation of powerful and positive beliefs connected to the product and influences the consumer's purchasing decision.

This, in turn, leads to the realisation of the objectives of the advertised message.

If the deceptive advertisement message is heavily dependent on the evaluative characteristics and the intangible characteristics, dependence on the deceptive message to realise the goals of the ad is uncertain, and this effect can be realised without using DA. The advertiser depends on DA by relying on the evaluative process since it is difficult to prove false, and on the absence of legal mentoring in the countries which has legislations to monitor the ads.

Figure 11.3 bellow illustrates the ad's effectiveness and its relationship to DA.

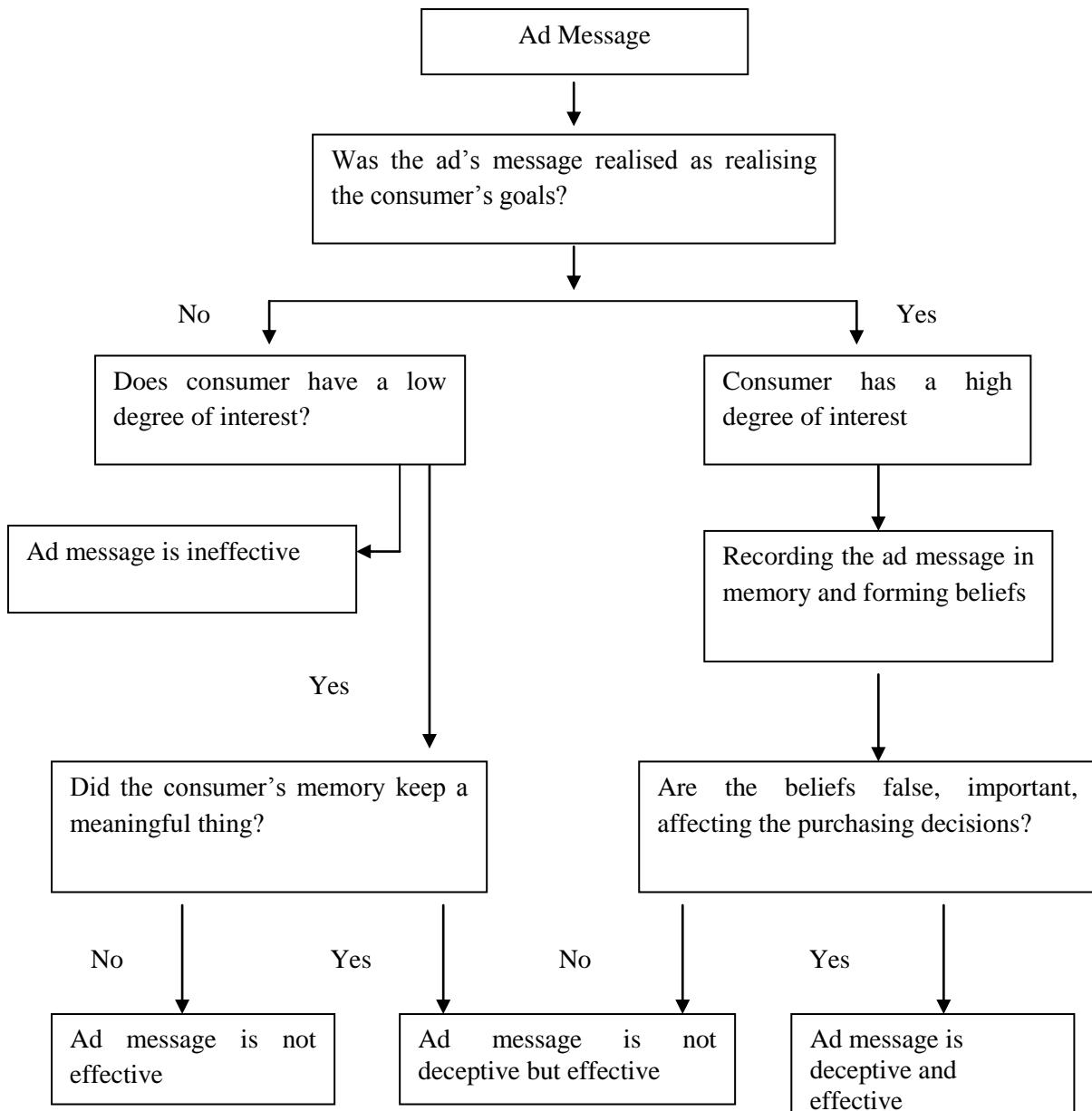


Figure 11.3: The ad's effectiveness and relationship to DA

From Fig 11.3 we can see the following:

- The consumer's interest in the advertised message is initially determined by the extent to which the message realises the consumer's goals. After that, the level of interest the consumer pays to the ad results in effects to the consumer from exposure to the advertising.

- A high level of involvement makes the process of making a purchasing decision go through several stages, starting with the interpretation of the advertising to reach meanings, and form concepts and beliefs connected to the advertised product. This reflects the involvement of the law if they are false. The process of making a purchasing decision, in such a case, is limited since the intentions to purchase are not frequent.
- The realisation of the goals of advertising and the realisation of advertising effectiveness are not always connected to advertising deception. DA is connected to the formation of false or deceptive beliefs by consumers. It is also effective, but for a short time period.

Dependence on non-deceptive advertising assures the effectiveness of advertising in both the short term and the long term, since the effectiveness of DA is confined to a short period. In the long term, the consumer can identify the deception in an advertisement.

11.6 The framework evaluation summary

Previous research has proved that deception in online advertising is a major problem for cyber-consumers who are still being affected psychologically and financially. In this research, a framework has been proposed which is intended to enhance cyber-consumers' online experiences by preventing psychological harm and financial losses. This framework covers cyber-consumer protection from a legal perspective by addressing potential solutions such as cyber-consumer protection laws and guidelines to help improve cyber-consumer experiences.

11.7 Conclusion

This chapter discussed the concept of deceptive advertising from both the legal and behavioural perspectives, concluding that the behavioural dimension of DA, rather than the

legal dimension, is preferable for studying DA, as it works on the correspondence between the agreed-upon standards of ad deception and the consumer's opinion of the ads.

The chapter discussed the means of measuring DA, they are: normative belief and explicit belief. The researcher concluded that the explicit belief method is the most reliable in this field if applied in a manner reflecting the nature of the scale applied to the advertisement.

This chapter also discussed the relationship between advertising effectiveness and DA, concluding that it is not necessary for advertising to include deceptive aspects in order to be effective. The effectiveness of the advertising can be realised via non-deceptive advertising and this effectiveness is for both the short and long term; while the effectiveness of the deceptive advertising is confined to the short term.

The following chapter discusses the determinants of the consumer's recognition of DA.

CHAPTER TWELVE

ENCAPSULATION AND FUTURE WORK

12.1 Introduction

This chapter reviews and draws together the development of the various themes examined in previous chapters in addressing the basic research issue: whether effective redress for online deception in advertising and any outcomes related to online fraudulent behaviour in addition to CCT is, or can, be made available by litigation or by any other legitimate non-litigation-based method, whether current or potential. The chapter then states the overall conclusions reached by this research project. The chapter closes by evaluating the relevance and importance of this thesis to the development of the law of international cyber-consumer protection, and suggests what further research might be done to extend the study.

12.2 The impact of the research

The impact of this research, in general terms, is that from a theoretical perspective, it describes online deception and fraudulent behaviour in relation to CCTs and determines cyber-consumers' cognitive processes and awareness of deception. Laws and litigation, specifically in consumer protection law, cyber law, and the law of international consumer redress currently exist, and this thesis evaluates the effectiveness of those laws as a regime, and proposes improvements based on evidence and reason. Thus, the research presents a comprehensive synthesis of an important single issue including CCTs and prevention of online deceptive and fraudulent behaviour, conducted broadly and in detail.

More specifically, this study suggests potential solutions to problems with online fraud/deceptiveness and CCTs. A solution would give cyber-consumers increased confidence to purchase goods from foreign and domestic vendors without having to face any financial or physical harm. A major advantage of this would be the potentially enormous economic benefits to be derived from a workable international consumerism. Cyber-consumers would benefit because they could shop safely, at any time, in a global market, using intelligent and efficient search tools. Vendors would benefit because they would have online customers who are more trusting and therefore more willing to engage with them, and they would be able to establish online business operations within a legally regulated environment.

Obtaining these benefits depends upon recognising the existing deficiencies in the present circumstances. This thesis has documented and demonstrated those deficiencies in terms of theory and practice .

Also, in order to realize any benefits, a solution must be based on good theoretical foundations, workable established precedent, and realistic expectations. In the first case, consumers have a good theoretical foundation in the various justifications for social/legal intervention in online practices and CCTs considered in this thesis. In the second case, a combination of existing consumer protection law and online law models and the relevant directives of the EU do indeed provide precedents which are demonstrably workable.

Furthermore, a negotiated assembly from the appropriate substantive and procedural provisions of such laws and perhaps other laws would result in a solution which would certainly be workable. As for expectations, it is evident that expectations of the success of a proposed solution based on solid precedent, in terms of both existing law and existing technology, is realistic.

Finally, this research can be further extended in two ways. The study could be extended by empirical testing of the recommendations mentioned above to prevent online deceptiveness and fraudulent behaviour to provide a safer cyber space for CCTs. Also, research could be conducted into the potential links between such information technology fields as Artificial Intelligence and expert systems, and judicial decision-making processes, in order to ascertain whether such processes could be automated and used by an electronic court for the purpose of reducing the amount of online fraud and deception for cyber-consumers and CCTs, also to resolve difficulties associated with trans-border consumer disputes.

Artificial Intelligence is defined as “intelligence exhibited by an artificial entity. Such a system is generally assumed to be a computer” (nationmaster.com 2006), and “the use of computers to model the behavioural aspects of human reasoning and learning” (bartleby, 2006).

Artificial Intelligence can be built into expert systems software. An ‘expert system’ is an interactive system that responds to questions, asks for clarification, makes recommendations, and generally helps and can replace the user in the decision-making process; the system mirrors the human thought process. It even uses information supplied by real experts in a particular field such as law. Expert systems are particularly good at making critical decisions that we might not otherwise make because of expense. In many ways, expert systems recreate the decision process better than humans do. We tend to miss important considerations or alternatives that expert systems do not.

There is no apparent reason why an expert system in the form of an electronic court could not be made permanently available online and accessible through the Internet to make low-cost judgements based upon facts supplied by the parties to a disputed CCT, and rules of laws supplied by an international consumer redress/protection convention. Such a system could

even handle issues without precedent, based upon certain pre-determined and up-dateable reasoning rules, and the system generally could be subject to appeals, at a price, just like the decisions of normal courts.

Artificial Intelligence and expert systems are issues to be explored in further research. In any event, it is important that the protection of consumers engaging in CCTs remain a topic of both academic and government concern.

While in most cases CCTs will probably provide rewarding experiences for all concerned, the fact is that some disputes regarding CCTs are inevitable; the law intervenes to regulate international events in other areas such as crime, telecommunications and B2B commerce, and there is much to be gained from the provision of effective remedies for online fraud and deception in CCTs. Some of the advantages of globalisation are still waiting to be realised.

12.3 Encapsulation

Chapter Two presented the history of DA from a theoretical and legal perspective, including the stages of its development, with previous research and studies showing that the laws need to be updated and improved in order to effectively keep up to date with technology and prevent Internet-based fraud and crime. Such laws would help to establish a safer and more reliable cyber environment. Also, this chapter described the relationship between the current not-so-effective laws and CCTs. This chapter showed that several areas of law need to be considered for the purposes of this thesis; they include those pertaining to: Australian consumer protection law, private international law, cyber crime, and e-commerce.

Chapter Three discussed the concepts of DA in the context of the legal dimension as it involves consumer protection and redress, and the behavioural dimension as it determines the

consumer's cognitive process—to what level the consumer is aware of noticing the deceiving message when exposed to it. As the main concern of this thesis is online-related fraud and deception related to CCT, this chapter focused mainly on online-fraud-related issues and online DA strategies. Furthermore, this chapter described the indicators that signalled the presence of DA, and pointed out that the term 'deceptive' can refer to both explicit and implicit claims.

Chapter Four considered DA in terms of behavioural and legal trends. Previous studies indicated that the consumer's cognitive process to some extent determines the purchasing decision when the consumer is exposed to deception. This chapter also discussed DA in terms of the legal dimension in order to identify where the laws and legislation lack cyber-consumer protection for CCTs, and found that legislation that provides cyber-consumer protection barely exists for low-value (less than \$40,000) purchases made, whether local or international.

Chapter Five examined the consumer's cognitive process and behaviour and the determinants of the cognitive effects of DA, finding that the more the consumer is repeatedly exposed to the deceptive advertising message, the less the chances are that the consumer will recognise the deception. This chapter also suggested a framework for the determinants of the DA process. Through this chapter, we find that the advertising messages which are built on subjective aspects have consistency between message type and the consumer's involvement framing, which makes the recognition of the advertising deception less probable. The advertising message which is built upon objective aspects, however, shows no consistency between message type and the consumer's involvement framing, making recognition of the advertising deception more probable.

Chapter Six considered the effect of the DA on purchasing decisions from legal and behavioural perspectives. It concluded that consideration of only the behavioural aspect of the effect of DA on purchasing decisions is inadequate because it does not provide an integrated framework that accounts for the effects that advertising deception has on cognitive processes, and consequently, the effect of these cognitive processes on the purchasing decision.

Chapter Seven described and analysed the academic scholarship regarding the justifications for consumer protection—including protection for CCTs conducted in cyberspace—and described the conflict between libertarianism and interventionism. The chapter also described and summarised the academic scholarship concerning four legal perspectives directly or indirectly relating to protection for consumer transactions: consumer protection law, contract law, private international law and cyber law.

Chapter Seven concluded that, for the purposes of regulation of CCTs, the most effective remedy is likely to be interventionist—one associated with state-backed sanctions. An interventionist approach was demonstrated as inevitable since there are likely to be limitations to the effectiveness and legal certainty of cyberspace self-ordering, especially where some aspects of the performance of CCTs necessarily occur in realspace, and since libertarian remedies are ultimately unenforceable.

Chapter Seven also disclosed the beginnings of a convergence between the separate debates about interventionism and private international law. In Boss's “universal system – developed cooperatively by different countries”, in Hardy's “statutory or judicial solution”, in Post's “promotion of the common welfare”, in Goldring's “multi-lateral international agreements” and “broadly-based effort to establish international consumer protection norms”, and in

Tokeley's "cyber-jurisdiction which would regulate the internet independent of national laws", a possible single unified resolution to both debates was noted.

Chapter Eight established the theoretical and legal contexts for problems associated with redress for CCTs, especially, but not exclusively, those conducted in cyberspace, since most CCTs are transacted, to some extent, within cyberspace.

Chapter Eight concluded with a general regulatory theory of CCTs reduced to a simple formulation: in the case of online fraud and deception in a valid and binding CCT, concluded via the Internet or otherwise and where interventionist protection for the consumer party is justifiable, no form of redress should be acceptable unless that form of redress is at least effective.

The chapter also described the methodology used in evaluating the cost-effectiveness of the redress methods considered by this thesis.

Chapter Nine considered redress for online fraud and deceptiveness in CCTs by means other than litigation. It demonstrated that such means, at least as they currently exist, are generally not effective.

The chapter concluded that, given the ineffectiveness of potential solutions, the only source of effective remedies for online fraud and deceptiveness in CCTs will be one of two possibilities. The first is the reduction or elimination of the problems associated with national private international law rules so that jurisdiction issues become irrelevant. The second is the side-stepping of such problems altogether through the creation of an international cyber-consumer protection regime to provide an effective scheme of internationally-recognised and enforceable court-based litigation for CCTs. It was noted that a cyber-jurisdiction, as defined,

was perhaps one means by which such a convention could be administered to provide access to justice effectively enough for CCTs.

Chapter Ten considered various commentaries from academic and judicial sources concerning the specific redress and enforcement provisions of a range of model consumer protection-related laws proposed by Australia, the UN, the OECD, the EU and the US, especially in respect of transnational enforcement. These law models were considered in both descriptive and prescriptive terms, looking at the objective characteristics of the models, and how those characteristics might be used, if at all, in the formulation of a solution to the problems of CCTs. The chapter also considered commentary relevant to the possible process of uniting the general content of those law models.

It was found that each of the models examined in the chapter is beset by the problems of discrepant consumer protection standards and non-united private international laws, leading to a lack of consumer confidence in entering CCTs, and in the enforcement of judgements regarding failed CCTs. It was conceded that it might not be easy to create an international cyber-consumer redress/protection law, but successful examples of such a process were noted.

Finally, the chapter noted that in a world of increasing geographic neutrality, and with so many stakeholders having so much to gain, it is possible that efforts to create a regime for CCTs may be near at hand. It was hoped that the key objectives of such a regime would include the creation of effective CCTs remedies, ease of use by consumers, and a balancing of the interests of consumers and online vendors.

12.4 Overall conclusion

In terms of the methodology established in Chapters Seven and Eight— expressed as a table—the various results for cyber-consumer protection and CCT redress methods numbered 2 to 13 can now be collectively tabulated as indicated in Table 12.1.

Table 12.1: Evaluation of cyber-consumer transaction redress methods

Method	Difficulty enforcement	of Complexity
---------------	-------------------------------	----------------------

Table 12.1.1: Current redress methods

2. Foreign lawyers	High	Acceptable
3. Foreign public consumer protection authorities	Very High	Acceptable
4. Alternative dispute resolution/online dispute resolution	High	High
5. Arbitration	Acceptable	High
6. Online industry-based consumer dispute resolution schemes	High	High
7. Industry codes of conduct	Very High	Acceptable
8. Escrow services	Low	High

Table 12.1.2: Potential solutions and redresses for cyber-consumer protection

9. Transaction insurance	Low	Low
10. Trustmarks	Low	Very Low
11. Consumer education	Low	Very Low
12.Cyber-consumer bulletin boards	Very Low	Low
13.National deregistration of vendor websites	Very Low	Low

From this final version of the table, it is clear that there is no current method that provides redress for CCTs. This conclusion should be understood in the context of the point made in Chapters Seven and Eight that the overall conclusion regarding the effectiveness of the various redress methods is based upon the findings presented in Chapter Nine only. The findings in Chapter Ten, however, are useful as indicators of the general nature of a potential solution —even if such indications are predominantly in negative terms, as problems to be avoided.

Having examined a variety of actual current redress methods and alternative hypothetical solutions—such as international agreement on uniform conflicts rules—in relation to the problem of CCTs, this thesis does not conclude simplistically that any one particular solution is *the* ‘correct’ solution and that all other possibilities are ‘incorrect’ or ‘ineffective’. On the contrary, the conclusion is that all current methods, law models and hypothetical solutions are part of an array of potential solutions for any particular problematic CCT. However, the solution which is explicitly recommended as having the greatest probability of achieving effectiveness in redress for CCTs, is the development of an international consumer protection convention or, at least, a redress convention.

It would be instructive, at this point, to draw this thesis to a close by linking these conclusions to the theoretical framework established in Chapters Seven and Eight.

The two fundamental conclusions of this thesis are that no effective redress for online fraud and deception in CCTs is provided by any current redress method and that an international and cyber-consumer law, in the form of an international convention, would provide the greatest probability of solving this problem.

The theoretical framework described in Chapters Seven and Eight consists of a range of elements. In summarised form, those elements established that state-provided protection for

CCTs is justified on the grounds of information asymmetry, inequality of bargaining power and, arguably, a general right to a remedy for actual abuses.

A single proposition can now be derived from all of that the foregoing: consumers are entitled to be protected when they engage in CCTs but in fact, they are not; and this is a social/legal anomaly which, on various grounds, is in urgent need of correction.

From the debate, presented in Chapter Seven, between the interventionist and libertarian schools of thought, it appears that only an interventionist solution could provide a remedy with the geographical reach and enforcement power required to address this problem.

Chapter Seven concluded by considering a new regulatory theory to serve as a guiding principle for steering a path towards a clear and workable solution for problematic CCTs. The theory was expressed in a simple formulation as follows: in the case of any online fraudulent behaviour and deception in a valid and binding CCT, where interventionist protection, for the consumer party, is justifiable, no form of redress will be acceptable generally unless that form of redress is at least effective. The question now is whether this thesis has achieved the goal of providing a solution which is clear and workable to make Internet use a safer environment for cyber-consumers and general users.

REFERENCES

- Aaker, D., (1974). *Deceptive Advertising advertising*. In D. Aaker & G. Day (Ed.).
Consumerism.
- Alavi, M., & Carlson, P. (1992). A review of MISresearch and disciplinary development.
Journal of Management Information Systems, vol. 8(4) 45–62.
- Alexander, M., (1997). Net Security: Your Digital Doberman (1997)
- Australian Competition and Consumer Commission. (2005). *What does econsumer.gov do?*
<http://www.accc.gov.au/content/index.phtml/itemId/255387/fromItemId/8135>.
- Australian Competition and Consumer Commission. (2005). *Internet shopping.*
<http://www.accc.gov.au/content/index.phtml/itemId/8135/fromItemId/3667>.
- American Express. (2003). *Online fraud guarantee*
http://www10.americanexpress.com/sif/cda/page/0,1641,7021,00.asp#more_info.
- American Express. (2002). American Express Credit Card Conditions.
- Asia-Pacific Economic Cooperation. (n.d.) Approaches to consumer protection within the
APEC region - report of the electronic. Retrieved
- Commerce Steering Group (2002).
<http://elib.fda.moph.go.th/kmfda/KmDoc/ApproachesToConsumerProtection.pdf>.
- Armstrong, G. (1979). Detecting and correcting deceptive advertising. *Journal of Consumer Research*, 6.

Armstrong, G. (1975). Applications of consumer information research to public issues.

Communication Research, 2(3), (1975).

Armstrong, G. & Russ, F. (1975). Detecting deception in advertising.

AskOxford. (2005). http://www.Askoxford.Com/Concise_Oed/Consumer?View=Uk.

Averitt, N. (1981). The meaning of ‘unfair act or practices’ in Section 5 of the Federal Trade Commission Act. *Georgetown Law Journal*, 70, 225–296.

Ayres, I. & Braithwaite, J. (1992) *Responsive Regulation*

Azzouni, A. (2002). The adoption of the 1980 convention on the international sale of goods by the United Kingdom. <http://www.cisg.law.pace.edu/cisg/biblio/azzouni.html>.

Bailey, P. & Pertschuk, M. (1984). The law of deception: the past as prologue. *American University Law Review*, 33, 849–897.

Baldwin, J. et.al.,(2004). The crisis in enforcement of civil judgments in England and Wales. *Public Law*, 305–328.

Barnes, A. Dworkin, T. & Richards, E. (2005) Uniform commercial code.

<http://highered.mcgraw-.>

Bartleby. (2006) Artificial intelligence. <http://www.bartleby.com/65/ar/artifInt.html>.

Bell, A. (2003). Forum shopping and venue in transnational litigation

Bell, A. (1994). Responses to forum shopping in transnational litigation: recent developments and new directions. Paper presented at the Continuing Legal Education.

Berinato, S. (2005). *You sue, you lose: the high cost of litigation.*

<http://www.cio.com/archive/020104/vendor.html>.

British and Irish Law Education and Technology Society. (2002). *Trusting the Trustmark?*

<http://www.bileta.ac.uk/02/papers/nordquist.html>

Black, V. (1997). Consumer protection in the conflict of laws: Canada, the United States and

Europe. *Consumer Law in the Global Economy - National and International Dimensions*

Bogdanor, V. (2003). *Federalism and the nature of the European Union.*

http://www.riia.org/pdf/research/europe/Bogdanor_Final.pdf.

Bonnie, R. & Robert, C. (1987). Deception in brand names. *Journal of Public Policy and Marketing*, 6, 93–103.

Boss, A. (1992). The Emerging Law of International Electronic Commerce *Temple International & Comparative Law Journal*, 6, 293–309.

Brandt, M. & Preston, I. (1997). The Federal Trade Commission's use of evidence to determine deception. *Journal of Marketing*, 54–62.

Brookfield Communications v West Coast Entertainment Corp (1999) 174 1036.

Brown v the Butchers and Drovers' Bank (1884) 41, 755.

Burke, J. *Standard Form Contracts* (2004), <http://www.lex2k.org/sfc/discussion.html> at 6 January 2007.

Burnett, R. (2004). Law of international business transactions. (3rd ed)

Butterworths, (2002). Business and law dictionary (2nd ed.)

Butterworths, (1997). Butterworths encyclopedic Australian legal dictionary.

Butterworths, (1998) Concise Australian legal dictionary.

Cairns, B (2005) Australian Civil Procedure.

CarBuyingTips.com consumer guide to avoiding ebay fraud, escrow internet fraud, check fraud, auto fraud, and Nigerian scams (2005).www.carbuyingtips.com/fraud.htm.

Carney, J.A. (1972). Section 5 of the Federal Trade Commission Act: unfairness to consumer. *Wisconsin Law Review*, 1(4) 1071–1076.

Carnival Cruise Lines Inc. v Shute (1991) 499: 585.

Carolyn, T. et, al. (1994). The effects of multiple product endorsements by celebrities on consumer attitudes and intentions. *Journal of Consumer Research*, (20,) 535–547.

Citibank. (2000). Citibank's full security guarantee. Clarke, R and Dempsey, G, The Feasibility of Regulating Gambling on the Internet.

Clarke, R. (2000). Appropriate research methods for electronic commerce.
<http://www.anu.edu.au/people/Roger.Clarke/EC/ResMeth.html>.

CNN. (2005). *Three jailed in global ebay scam*.
<http://edition.cnn.com/2005/WORLD/europe/10/28/ebay.scam.ap/index.html>.

Cohen, D. (1972). Surrogate indicators and deception in advertising. *Journal of Marketing*, 36, 11.

Cohen, D. (n.d.). The concept of unfairness as it relates to advertising legislation, Op. Cit., P 11.

Cohen, D. (1980). The FTC's advertising substantiation program. *Journal of Marketing*, 44 26–35.

Columbia Encyclopaedia. (2005). Laissez Faire. <http://www.bartleby.com/65/la/laissezf.html>.

Commercial Bank of Australia V Amadio, 151 CLR (1983).

Conde, J. (2005). Credit card chargeback primer.

Cook, V. (1998). CISG: from the perspective of the practitioner *Journal of Law and Commerce*, 17, 343–353.

Cordera, M. (2001). E-consumer protection: a comparative analysis of EU and US consumer protection on the internet. *Rutgers Computer & Technology Law Journal*, 27 231–264.

Coteanu, C. (2005). Cyber Consumer Law and Unfair Trading Practices, Council Regulation (EC) No 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters (the Brussels Regulation).

County of Santa Cruz (2005). *Long Arm Statute* (2005)

http://www.santacruzdcss.org/html/long_arm_statute.html.

CPAWebTrust. (2005). <http://www.cpawebtrust.org/consumer.htm>

New South Wales Government Department of Commerce: Office of Fair Trading. (2007).

Crackdown on illegal advertising,

http://www.fairtrading.nsw.gov.au/About_us/News_and_events/Media_releases/2007_media_releases/20070505illegaladvertising.html.

- Craswell, R. (1981). The identification of unfair acts and practices by the Federal Trade Commission. *Wisconsin Law Review*, 1, 107–153.
- Dann, S. Dann, S. Belch, G., & Belch, M (2004). *An integrated marketing communications perspectives*, Advertising and promotion. 2nd ed.
- Debussere, F. (2004). International jurisdiction over e-consumer contracts in the European Union: Quid Novi Sub Sole? (2002) *International Journal of Law and Information Technology*, 10, 344–366.
- Dicarlo, V. (2005). *How to reduce the high cost of litigation*
<http://www.dicarlolaw.com/NetscapeHTRHCL.htm>.
- Dicey, A. & Morris, J. (1993). The Conflict of Laws
- Dickie, J. (1999). Internet and electronic commerce law in the European Union
- Dictionary.com, *Cost* (2005) <<http://dictionary.reference.com/search?q=cost>>
- Dictionary.com, *Cyberspace* (2005) <<http://dictionary.reference.com/search?q=consumer>>
- Dictionary.com, *Effective* (2005) <<http://dictionary.reference.com/search?q=effective>>
- Dictionary.com, *Enforceability* (2005)
<<http://dictionary.reference.com/search?q=enforceability>>
- Dictionary.com, *Simplicity* (2005) <<http://dictionary.reference.com/search?q=simplicity>>
- Diedrich, F. (2000). A law of the internet? Attempts to regulate electronic commerce.
- Digital Enterprise. (2005) *Case Study: TrustE*. <http://digitalenterprise.org/cases/truste.html>.

Diners Club. (2003). *Diners Club Electronic Access Conditions of Use*.

http://www.dinersclub.com.au/s02_personal/default.asp?whichfile=p26_terms_and_condition.s.asp

DTI. (2005). Cross border consumer contractual disputes within the European Union: which country has jurisdiction? http://www.dti.gov.uk/ccp/topics1/guide/jurisdiction_brussels.htm.

DTI. (2005). *Jurisdiction – FAQ*.

http://www.consumer.gov.uk/ccp/topics1/guide/jurisdiction_faq.htm.

EBay.com (2005) <www.ebay.com>

Institute of Economic Affairs. (2005). *What is meant by 'free-market'?*

<http://www.iea.org.uk/record.jsp?type=page&ID=23>.

Welcome to Econsumer.Gov! (2005). <http://www.econsumer.gov/english/index.html>

Eisengraeber, J. (2004). Lis Alibi Pendens under the Brussels I Regulation *Exeter Papers in European Law 1 of 63, 16.*

Encarta Online Dictionary, *Enforce* (2005)

<<http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?refid=1861608465>>

Encarta World English Dictionary, *Simplicity* (2005)

<<http://encarta.msn.com/encnet/features/dictionary/DictionaryResults.aspx?refid=1861732764>>

Why Use Escrow? (2005). <https://www.escrow.com/index.asp>.

Etienne-Cummings, S. (1997). Vanishing boundaries: extending the long-arm statute into cyberspace. *Southern Illinois University Law Journal*, 22, 217–241.

European Union (1968). Convention on jurisdiction and the enforcement of judgments in civil and commercial matters Brussels of 26/01/98, OJ C 027 (498y0126(01))
<http://www.curia.eu.int/common/recdoc/convention/en/c-textes/brux-idx.htm>.

European Union. (1980) Convention on the law applicable to contractual obligations, OJ C 027 (498y0126(03)) of 26/01/98, http://www.rome-convention.org/instruments/i_conv_cons_en.htm.

European Union. (2001). Council regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters,

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32001R0044&model=guichett&lg=en.

European Union. (2000). Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce

http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf.

European Union. (1997). *Directive 97/7/EC on protection of consumers in respect of distance contracts*,

http://europa.eu.int/ISPO/ecommerce/legal/documents/31997L0007/31997L0007_en.html.

Exkhardt, R. (1970). Consumer class actions. *Notre Dame Law Review*, 45, 663–670.

ACLU president's internet remarks insulted Australia (1999).

<http://exn.ca/Stories/1999/08/24/04.asp>.

Findlaw. (2004). *New system of endorsement for industry codes of conduct* (2004).

<http://www.findlaw.com.au/news/default.asp?task=read&id=16079>.

Findlaw. (2005). *US constitution: first amendment* (2005).

<http://caselaw.lp.findlaw.com/data/constitution/amendment01>.

Findlaw. (2005). *US constitution: fourteenth amendment*.

<http://caselaw.lp.findlaw.com/data/constitution/amendment14/>.

Fitzgerald, B., Middleton, G. & Fitzgerald, A. (2004). *Jurisdiction and the internet*.

Forder, J., & Quirk, P. (2001). *Electronic commerce and the law*.

Foreign Judgments Act 1991 (Australia).

What was the napster case about and what does it mean? (2005).

http://law.freeadvice.com/intellectual_property/copyright_law/napster.htm.

Basic uses of computer bulletin boards (2003).

<http://www.freewell.com/freereports/business/63.html>.

French, W.A., & Borks, H.C. (1977). Food labeling regulation: efforts towards full disclosure. *Journal of Marketing*, 38, 14–19.

Fullerton, J. (1997). *Uniform commercial code*. <http://www.fullertonlaw.com/chapt12.htm>.

Galliers, R.D. (1992). Choosing information systems research approaches in RD.

Galliers (Ed.). Information Systems Research: Issues, Methods and Practical Guidelines, Great Britain, Blackwell Scientific Publications.

Gamertsfelder, L. 'Cross Border Litigation: Exploring the Difficulties Associated with Enforcing Australian Money Judgements in Japan' (1998) 2 *Australian Bar Review*

Gardner, D. (1975). Deception in advertising: a conceptual approach. *Journal of Marketing*, 39.

Gardner, D. (1985). Low involvement strategies for processing advertisement. *Journal of Advertising*, 14.

Gellhorn, E. (1969). Proof of consumer deception before the Federal Trade Commission. *Kansas Law Review*, 17, 559–572.

Gillette, C. (2002). Reputation and intermediaries in electronic commerce. *Louisiana Law Review*, 62, 1165–1197.

Goldring, J. (1998). Globalization, national sovereignty and the harmonisation of laws. *Uniform Law Review*, 3, 435–451.

Goldring, J., Maher, L., & McKeough, J. (1993). *Consumer Protection Law* (4th ed.).

Goldring, J., Maher, L., & McKeough, J. (1996). Consumer protection, the nation-state, globalisation, and democracy. *Journal of computer-mediated communication*, 2.

Gordon, B. (1998). The legal challenge of regulating the internet. Fact or fallacy?

Haefner, J. (1972). The perception of deception in television advertising, an exploratory investigation, Ph. D. abstract, (p. 26). University of Minnesota

A convention aimed producing a new international convention on jurisdiction and foreign judgments in civil and commercial matters (2003).

[http://www.cptech.org/ecom/jurisdiction/Prel_Doc08\(e\).doc](http://www.cptech.org/ecom/jurisdiction/Prel_Doc08(e).doc).

Halpern, M., & Mehrotra, A. (2000). From international treaties to internet norms: the evolution of international trademark disputes in the internet age. *University of Pennsylvania Journal of International Economic Law*, 21, 523–561.

Hanks, M. (2005). *The five limits of litigation*.

<http://library.findlaw.com/2000/Aug/1/126087.html>

Hardy, I. (1994). The proper legal regime for ‘cyberspace’ u.pitt.l.rev.993 *Stanford Law Review*, 55, 993–1055.

Harland, D. (1991). Implementing the principles of the United Nations guidelines for consumer protection (1991) *Journal of the Indian Law Institute*, 33, 189–245.

Harland, D. (1997). The United Nations guidelines for consumer protection: their impact in the first decade in Iain Ramsay (Ed,) *Consumer Law in the Global Economy*.

Harris, W. (1993). Consumer disputes and alternative dispute resolution. *Australian Dispute Resolution Journal*, 239–252.

Developments in the law - the law of cyberspace. (1999). *Harvard Law Review*, 112, p. 1574.

Helper, L., & Slaughter, A. (1997). Toward a theory of effective supranational adjudication. *Yale Law Journal*, 107, p. 273.

Henderson, D.(2005). *Anti-Liberalism 2000*.

<http://www1.worldbank.org/economicpolicy/globalization/documents/wincott.pdf>.

Hill V Gateway 2000 Inc, 105 F.3d 1147 (1997).

hill.com/sites/0072488263/student_view0/uniform_commercial_code.html.

- Hoegle, R., & Boam, C. (2000). The internet and jurisdiction - international principles emerge but confrontation looms. *The Journal of World Intellectual Property*, 3.
- Honnold, J. (1998). The sales convention: from idea to practice. *Journal of Law and Commerce*, 17, 181–186.
- Horning, R. (1997). The enforceability of contracts negotiated in cyberspace. *International Journal of Law and Information Technology*, 5, 109–157.
- Horton, R.L. (1984). Buyer behavior: a decision making approach. Charles E. Nerrill (p. 125). Publishing Co.
- International Communications Round Table. *Brussels regulation: international debate* (2000) http://www.icrt.org/pos_papers/2000/001025_EC.pdf.
- IDA Singapore. (2002). *Building user confidence in electronic commerce transactions via trust marks*. [http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/457df2836309e02fc82569660010f4ae/\\$FILE/DeepKnowledge.pdf](http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/457df2836309e02fc82569660010f4ae/$FILE/DeepKnowledge.pdf).
- Jacoby, J., & Hoyer, D. (1982). Consumer miscomprehension of television communication. *Journal of Marketing*.
- Jacoby, J., & Small, C. (1975). The FDA approach to defining misleading advertising. *Journal of Marketing*, 39.
- Jardine, E. (1996). An agreement between Australia and the European Union on trade practices: a proposal. *Trade Practices Law Journal*, 4, 67–76.

Jew, B. (1998). *Cyberjurisdiction - emerging issues and conflicts of law when overseas courts challenge your web.*

<http://www.gtlaw.com.au/gt/site/articleIDs/37713994BFA233DBCA256D1F00042F58?open&ui=dom&template=domGT>.

Johar, G.V. (1998). *Consumer behaviour: a quadrennium.*

<http://www.annualreviews.org/doi/abs/10.1146/annurev.psych.49.1.319?journalCode=psych>.

Johnson, D., & Post, D. (1996). Law and borders - the rise of law in cyberspace. *Stanford Law Review*, 1367–1402.

Jossey-Bass. (2005). *Alternatives to the high cost of litigation.*

<http://www.josseybass.com/WileyCDA/WileyTitle/productCd-ALT.html> at 14 CCTober 2005

Journal of Information, Law & Technology

Juenger, F. (1993). Choice of law and multistate justice.

Korobkin, R. (2003). Bounded rationality, standard form contracts and unconscionability. *UCLA School of Law*, 1203–1295.

Kristal, S. (2002). *Advertising assaulting women awaken from media.*

<http://www.feminists.com/resources/media/artspeech/advertisingassault.html>.

Latimer, P. (2003). *Australian Business Law*. (22nd ed.)

Lessig, L. (1995). The path of cyberlaw. *Yale Law Journal*, 104, 1743–1755.

Lessig, L. (1996). The zones of cyberspace. *Stanford Law Review*, 1403–1412.

Levey, S.J. (1968). Symbols for Sale. In Glenview & Scott (Eds.). *Perspectives in consumer behavior* (pp. 211–213. Foresman Co

Lim, Y. (2002). Cyberspace Law: Commentaries and Materials.

Long, L., & Long, N. (2002). Computers - information technology in perspective (9th ed).

Maggs, G. (1998). Internet solutions to consumer protection problems. *South Carolina Law Review*, 49, 887–902.

Mallesons, S.J. (2005). *Boilerplate clauses*.

http://www.mallesons.com/publications/Asian_Projects_and_Construction_Update/6781340W.htm.

Martin, M. (2002). Keep it online: the Hague convention and the need for online alternative dispute resolution in international business to consumer e-commerce. *Boston University International Law Journal*, 20, 125–159.

Martin, R. (2005). *The cost of litigation*.

http://www.divorcenet.com/states/arizona/the_cost_of_litigation.

McNamara, T. (2004). Graduating from obscurity: The U.N. international sale of goods convention. <http://www.dgslaw.com/articles/565324.pdf>.

McRobertson Miller Airline Services V Commissioner of State Taxation (WA), (1975). 133 CLR 125.

Mead, P. (1999). ADR agreements: good faith and enforceability. *Australian Dispute Resolution Journal*, 40–52.

Meltz, D (1996). The extraterritorial operation of the trade practices act. *Trade Practices Law Journal*, 4, p. 185.

Merriam-Webster Online Dictionary. (2005). <http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va>.

Methenitis, M. (2007). Deceptive advertising? Not quite. Law of the game. <http://lawofthegame.blogspot.com/2007/04/deceptive-advertising-not-quite.html>.

Mingers, J. (2003). The paucity of multimethod research: a review of the information systems literature. *Information Systems Journal*, 13, 233–249.

Mo, J. (1997). International Commercial Law.

Moore, R.L., Farrar, R.T., & Collins, E.L. (1998). *Advertising and public relations law*. Retrieved..., from <http://www.directessays.com/viewpaper/16330.html>.

Moore. C. (1969). Deceptive trade practices and the federal trade commission. *Georgia Law Review*, 28, 493–502.

Mortensen, R. (2001). Duty free forum shopping :disputing venue in the Pacific. *Victoria University of Wellington*, 32, 673–703.

National archives of Australia, appendix 10 - recordkeeping cost-benefit analysis (2005). http://www.naa.gov.au/recordkeeping/dirks/dirksman/dirks_A10_cost_benefit.html.

Artificial Intelligence (2006). <http://www.nationmaster.com/encyclopedia/Artificial-intelligence>.

Netanel, N. (2000). Cyberspace self-governance: a skeptical view from liberal democratic theory. *California Law Review*, 88, 395–498.

Not Good Enough, *Australia's Customer Complaints Website* (2002)

<<http://www.notgoodenough.org/?page=21>>

Nunamaker, J.F., Chen, J.M., & Purdin, T.D. (1990-91). System development in information systems research. *Journal of Management Information Systems*, 7,(3), 89–106.

Nygh, P., & Davies, M., (2002). *Conflict of laws in Australia* (7th ed.)

Nygh, P. talk on jurisdiction and the internet [Unpublished conference paper].

OECD. (2001). Consumers in the online marketplace OECD workshop on the guidelines - one year later - report of the workshop

http://www.oecd.org/document/19/0,2340,en_2649_201185_1864403_1_1_1_1,00.html.

OECD. (2003). Consumers in the online marketplace: the oecd guidelines three years later - report to the OECD council on the guidelines for consumer protection in the context of electronic commerce.

[http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/af6ec39d8631ca3ac1256cc2005c0edf/\\$FILE/JT00138646.PDF](http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/af6ec39d8631ca3ac1256cc2005c0edf/$FILE/JT00138646.PDF).

OECD. (2001). First report: government and private sector initiatives to promote and implement the OECD guidelines for consumer protection in the context of electronic commerce.

[http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256a010059d1e9/\\$FILE/JT00103514.PDF](http://www.olis.oecd.org/olis/2000doc.nsf/4f7adc214b91a685c12569fa005d0ee7/c125692700623b74c1256a010059d1e9/$FILE/JT00103514.PDF).

OECD. (1999). *News release - OECD governments agree on consumer protection guidelines for e-commerce*. <http://oecdpublications.gfi-nb.com/cgi-bin/OECDBookShop.storefront/EN/product/932000023P1>.

OECD (1999). Recommendation of the OECD council concerning guidelines for consumer protection in the context of electronic commerce.

http://www.oecd.org/document/51/0,2340,en_2649_34267_1824435_1_1_1,00.html.

OECD (2002). *Report on consumer protections for payment cardholders*.

[http://www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-cp\(2001\)3-final](http://www.olis.oecd.org/olis/2001doc.nsf/linkto/dsti-cp(2001)3-final).

OECD (2002). *Resolving e-commerce disputes online: asking the right questions about ADR*.

[http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/7f89b52192b7f8d5c1256bce00389cc6/\\$FILE/JT00127493.PDF](http://www.olis.oecd.org/olis/2002doc.nsf/43bb6130e5e86e5fc12569fa005d004c/7f89b52192b7f8d5c1256bce00389cc6/$FILE/JT00127493.PDF).

OECD (2002). *Update of official statistics on internet consumer transactions*.

<http://www.oecd.org/EN/home/0,,EN-home-29-nodirectorate-no-no-no-29,00.htm>.

Oughton, D (1991). Consumer law - cases and materials.

Concise Oxford Dictionary English of Current English (1980). Oxford University, Pace Law School, *CISG: Table of Contracting States* (2005)

<http://www.cisg.law.pace.edu/cisg/countries/cntries.html>.

Parish, R. (1980). In A. Duggan et al. (Eds.) *Consumer protection law and theory*.

Parkdale Custom Built Furniture Pty Ltd v Puxu Pty Ltd (1982) 40 ATPR 307.

Pearce, G., & Platten, N. (2000). Promoting the information society: the EU directive on electronic commerce. *European Law Journal*, 6, 363–378.

Perritt, H. (2000). *Testimony by Henry H. Perritt, Jr. Dean, Chicago-Kent College of Law*.

<http://www.kentlaw.edu/cyberlaw/perritthtest.html>.

Peter R., Dark, & Robin J.B., Ritchie, (2007). The defensive consumer, advertising deception, defensive processing, and distrust.

http://www.websitepublisher.net/scripts/article_print.php?ArtID=89.

Peterson v Young (1964) 110 CLR 162 at 170.

Peterson, E. (1987). The case against 'the case against the UN guidelines for consumer protection". *Journal of Consumer Policy*, 10, 425–432.

Piper Aircraft Co v Reyno, 454 US 235 (1981).

Positive solutions (2005). <http://www.positivesolutions.com.au/>.

Post, D. (2002). What Larry doesn't get: code, law, and liberty in cyberspace. *Stanford Law Review*, 52, 1439–1459 PWC.

<http://www.pwcglobal.com/extweb/ncpressrelease.nsf/DocID/44CA2D3D42CB0A0E8525685E006F3889>.

Preston, I., & Richards, J. Consumer miscomprehension as a challenge to ETC.

Prosecutions of deceptive advertising. (1986). *Journal of Marshall Law Review*, 19, 605–609.

Preston, I. (1987). Extrinsic evidence in Federal Trade Commission deceptiveness cases. *Columbia Business Law Review*, 633–637.

Preston, I. (1989). The Federal Trade Commission's identification of implications as constituting deceptive advertising. *Cincinnati Law Review*, 57, 1243–1247.

Pyati, A. (2005). *Whose vision of an information society?*

http://www.firstmonday.org/issues/issue10_5/pyati/.

Quirk, P., & Forder, J. (2003). *Electronic commerce and the law* (2nd ed.)

Reich, N. (2000). Consumerism and citizenship in the information society - the case of electronic contracting. *Competition and Consumer Law Journal*, 7, 185–200.

Rice, D. Jurisdiction in cyberspace: which law and forum apply to securities.

Richards, J.L. (1990). Deceptive advertising: behavioral study of a legal concept. New Jersey:

Lawrence Erlbaum Associates. <http://www.questia.com/library/book/deceptive-advertising-behavioral-study-of-a-legal-concept-by-jef-l-richards.jsp>.

Richards, J., & Zakia, R. (1981). Pictures: an advertiser expressway through FTC regulation. *Georgia Law Review*, 16, 77–80.

Rickett, C. et. al., (2003). International perspectives on consumers' access to justice.

Ritter, J. (1992). Defining international electronic commerce. *North Western Journal of Law and Business*, 13 3–30.

Rosner, N. (2005). International jurisdiction in European Union e-commerce contracts. http://www.llrx.com/features/eu_ecom.htm#b3.

Ross, P. (1996). The law of misleading advertising: an examination of the difference between common and civil law countries. *International Journal of Advertising*, 15, 33–47.

Rothchild, J. (1999). Protecting the digital consumer: the limits of cyberspace utopianism. *Indiana Law Journal*, 74, 893–989.

Rousseau C/ Commerzbank (1998). 11-98-000244 1998, July 1 Revue de jurisprudence de droit des affaires 1999 464.

Rubin, S. (2005). *Lack of courtroom experience due to high costs of litigation.*

[http://www.zsa.ca/En/Articles/article.php?aid=739.](http://www.zsa.ca/En/Articles/article.php?aid=739)

Rule, C. (2002). Online dispute resolution for business - b2b, e-commerce, consumer, employment, insurance, and other commercial conflicts.

Schu, R. (1997). The applicable law to consumer contracts made over the internet: consumer protection through private international law? *International Journal of Law and Information Technology*, 5.

192–229. <http://www.johnstonbuchan.com/pubs/trade/UNConventionFebruary2004.pdf>.

Trade Practices Bill, Second Reading Speech. vol 57.

Smith, J. (1993). Can the advantages of ADR procedures be transposed to a judicial forum? *Australian Dispute Resolution Journal*, 299–306

Smith, L. (2004). Global online shopping: how well protected is the Australian consumer? *Competition and Consumer Law Journal*, 12, 163–190.

Stanford University. (2007). *Libertarianism*. Stanford University Encyclopedia of Philosophy. <http://plato.stanford.edu/entries/libertarianism/>.

State Department of USA. (2001). *Australian practice - note from the Australian delegation in relation to forum non conveniens*.

http://www.state.gov/www/global/legal_affairs/australian_annex-a.html.

Steinwall, R. (2000). Annotated Trade Practices Act 1974.

Sullivan, J (2005). *Lawmakers should help businesses combat litigation costs.*

http://www.legalreforminthene.ws.com/Op-Ed/Op-Ed_John-Sullivan_8-18-05.html.

Sykes, E., & Pryles, M.(1991). *Australian private international law* (3rd ed.).

Taperell, G., Vermeesch, R., & Harland, D. (1974). *Trade practices and consumer protection.*

Adhesion Contract (2005). <http://legal-dictionary.thefreedictionary.com/Standard+form+contract?p>.

Forum Non Conveniens (2005).

<http://encyclopedia.thefreedictionary.com/Forum+non+conveniens?p>.

Forum Non Conveniens (2005). <http://legal-dictionary.thefreedictionary.com/forum+non+conveniens?p>.

Standard Form Contract (2005).

<http://encyclopedia.thefreedictionary.com/Standard+form+contract?p>.

Transactions on the Internet? (2000). University of Pennsylvania Journal of International Economic Law, 21, 585–657.

Australian Government. (2005). *The internet and b2c e-commerce*.

http://www.ecommerce.treasury.gov.au/bpmreview/content/discussionpaper/03_chapter2.asp.

TrustE Security Guidelines (2005). <http://www.truste.org/>

UNCITRAL. (1958). Convention on the recognition and enforcement of foreign arbitral awards.

<<http://www.jus.uio.no/lm/un.arbitration.recognition.and.enforcement.convention.new.york.1958/doc.html>>

UNCITRAL (1980). United Nations convention on contracts for the international sale of goods. <http://www.uncitral.org/english/texts/sales/CISG.htm>.

Union Des Etudiants Juifs De France C Yahoo! Inc, (2000).

United Nations. (1999). *Guidelines for consumer protection*.
<http://www.un.org/documents/ecosoc/res/1999/eres1999-7.htm>

University of North Carolina School of Law (2005). *Personal jurisdiction and the internet*.
<http://www.unc.edu/courses/pre2000fall/law357c/cyberprojects/spring01/Jurisdiction/pj/PersonalJurisdiction.html>.

Vaughan, M. (2000). Business or consumer e-commerce - what's the difference?
Telecommunications Journal of Australia, 50, 1–2.

VeriSign (2005). *SSL certificates*. <http://www.verisign.com/products-services/security-services/ssl/index.html>.

Vishal P.R. (2006) *Articles and information on smart advertising information*. Advertising-101, <http://www.advertisingsmart.net/Advertising-101/16>.

Vogel, D. (1995). Trading up - consumer and environmental regulation in a global economy.

Webster, F.E. (1974). *Social aspects of marketing*. Englewood Cliffs, J., Prentice Hall p. 33.

Weidenbaum, M. (1987). The case against the UN guidelines for consumer protection.
Journal of Consumer Policy, 10, 425–432.

Weirsma, W. (1996). *Research methods in education: an introduction*. (4th ed.). Boston. Allyn and Bacon.

Economic Interventionism (2005). In *Wikipedia*.

http://en.wikipedia.org/wiki/Economic_interventionism.

Wilkes, W.A., & Wilcox, J.B. (1974). Recent FTC actions: implication for the advertising strategies. *Journal of Marketing*, 38, 55–69.

William H.D. Jr. (1998). Managing: legal issues, PJM. Archives / magazines articles.

<http://www.professionaljeweler.com/archives/articles/1998/aug98/0898man1.html>.