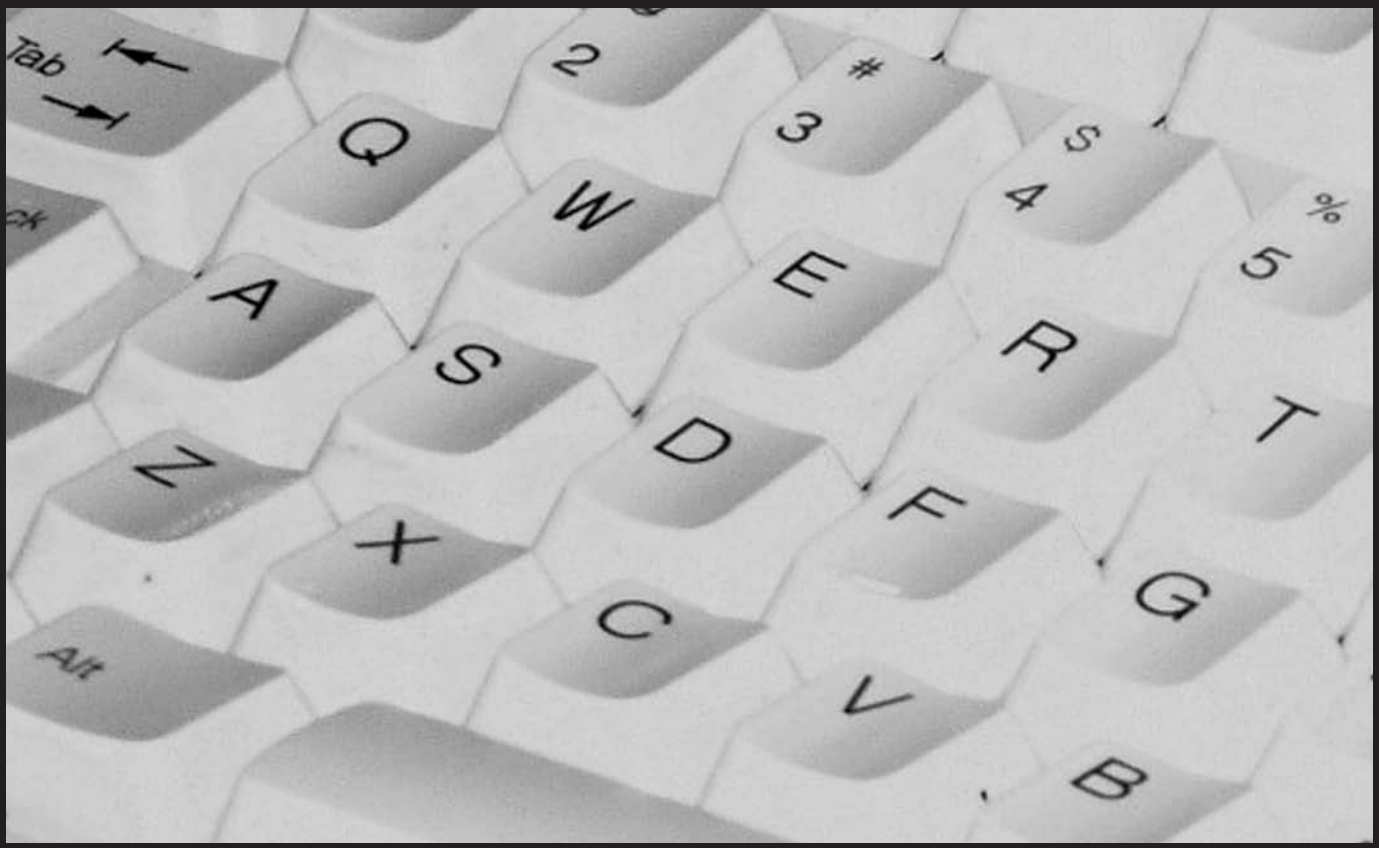
Online shopping and consumer protection
Discussion Paper

Standing Committee of Officials of Consumer Affairs

E-commerce Working Party

Consumer Affairs Victoria



Victoria
The Place To Be

May 2004

Disclaimer

Every effort has been made to ensure that the information presented in this discussion paper is accurate at the time of publication.

Published by Consumer Affairs Victoria,
452 Flinders Street, Melbourne, Victoria, 3000.

Authorised by the Victorian Government,
452 Flinders Street, Melbourne, Victoria, 3000.

Making a submission

All interested individuals and organisations are encouraged to provide comments on this discussion paper.

Comments in writing should be forwarded to:

The Convenor
E-commerce Working Party
Consumer Affairs Victoria
GPO Box 123A
MELBOURNE 3001

Email: onlineshopping@justice.vic.gov.au

Closing dates for submissions is 31 July 2004.

It should be noted that unless confidentiality for submissions is specifically requested, the contents of submissions may be made publicly available in any subsequent review process. Also, submissions may be subject to Freedom of Information and other laws and this should be taken into account when making submissions.

Further copies of this paper can be obtained by downloading it from the Ministerial Council on Consumer Affairs website **www.consumer.gov.au** or Consumer Affairs Victoria website at **www.consumer.vic.gov.au.**

Executive Summary

Consumer protection in online transactions is based on a mixture of existing legislation, in particular the *Trade Practices Act* 1974 (Commonwealth), State and Territory Fair Trading legislation, and voluntary, self-regulatory measures. Nationally, the most important of these voluntary measures is Building Consumer Sovereignty in Electronic Commerce: A best practice model for business (BPM) which sets standards for consumer protection in e-commerce.

E-commerce offers consumers many advantages in terms of choice and access to goods and services. Online transactions have increased significantly over the last few years with $4 billion spent in 2002 compared to $1.9 billion in 2001[1].

Despite the advantages of e-commerce, such as low-cost entry into new markets, it also presents consumers with a number of risks which are not apparent in the traditional retail environment. Some of these challenges are similar to those presented in other forms of distance selling, for example uncertainty about the location and identity of the seller, an inability to inspect goods prior to purchase, and uncertainty about delivery. Other risks are new or exacerbated in the online environment, for example whereas it is possible to pay for a mail order with a personal or bank cheque or cash on delivery, with online sales, goods need to be paid for in advance usually by releasing credit card and other personal information.

The Ministerial Council on Consumer Affairs (MCCA), which asked the E-commerce Working Party to prepare this paper, acknowledges that e-commerce issues require consideration by a range of organisations and individuals, and by state and national governments. However, in relation to fair trading and consumer protection matters for which it has responsibility, MCCA has asked the Working Party to consider and report to it on:

- Whether there should be a set of basic and uniform statutory measures to protect consumers engaging in online transactions and
- If so, to determine what those measures should be.

Three categories of consumer risk are examined in this Discussion Paper – security of payment information, privacy and fair trading matters. The paper canvasses some of the available national and international research into online shopping difficulties and presents data on consumer complaints relating to e-commerce.

The Working Party acknowledges that it is difficult to obtain conclusive, quantitative data about the nature and extent of consumer problems. It also acknowledges e-commerce is taking place in a rapidly changing marketplace where transaction and security technology platforms are still developing. It therefore makes no recommendations about future policy directions but rather asks a series of questions about the standards consumers might expect online. It notes current consumer protection measures and what has occurred in other jurisdictions.

[1] Source: E-commerce Today, LexixNexis Butterworths, 12 September 2003

There are various ways of achieving desired levels of consumer protection. The paper presents options ranging from retaining the current mix of consumer protection law, voluntary measures and information strategies to the development of new, mandatory disclosure requirements.

The E-commerce Working Party is not pre-disposed to a particular option. It invites and would welcome the views of interested individuals and organisations on the issues raised.

Contents

Section 1 Introduction

1

In 1999, the OECD released its *Guidelines for Consumer Protection in the Context of Electronic Commerce.* The Guidelines are designed to ensure that consumers are no less protected when shopping online than when purchasing from their local store.
By identifying core characteristics of effective consumer protection, the Guidelines intended to help eliminate some of the uncertainties faced by both consumers and businesses in the online world.

The Guidelines have served as the basis for the development of consumer education material, self-regulatory codes of conduct and law reform proposals among OECD member countries.
In Australia, for example, they served as the basis of *Building Consumer Sovereignty in Electronic Commerce – A Best Practice Model for Business* (BPM) and in New Zealand the *Model Code for Consumer Protection in Electronic Commerce*.

Three years after the release of the OECD Guidelines, the OECD's "report card"[2] on the Guidelines notes that much of the potential of business-to-consumer (B2C) e-commerce has yet to be realised. The OECD acknowledges that there are many reasons for this but notes that an important factor appears to be consumers' continued concerns about shopping online[3].

This paper examines the key risks to consumers, both perceived and actual when engaging in online transactions. It considers the current regulatory framework and asks whether there is a need for further consumer protection measures and what those measures might be.

The Working Party acknowledges from the outset that many issues which effect consumers online go beyond the jurisdiction of the Ministerial Council on Consumer Affairs (MCCA) which has requested the preparation of this Discussion Paper. Addressing some of the issues of concern to consumers will require the co-ordinated effort of government and the private sector and will rely on a mix of self-regulation, technological responses and government regulation.

The purpose of this Discussion Paper therefore is to consider those issues for which MCCA does have particular responsibility – business-to-consumer transactions – and to elicit views from others areas of government, industry and the community which will help inform future action with regard to e-commerce consumer protection.

The Working Party acknowledges that it is difficult to obtain conclusive, quantitative data about the nature and extent of consumer problems with online trading. It therefore does not make any recommendations about the future direction of consumer protection and electronic commerce. It presents a range of possible options, both regulatory and non-regulatory and would be very interested in the views of industry and the community about desirable future directions.

[2] *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/2003doc.nsf/LinkTo/dsti-cp(2002)4-final.

[3] A recent Australian Bureau of Statistics report 8146.0 Household Use of Information Technology, Australia September 2003 noted that while Australians had doubled their spending on the Internet to about $4 billion, only 15 percent of adults actually purchased something online. This is despite the fact that 58 percent of Australians accessed the Internet in 2002; 43 percent have access to the Web at home; 23 percent have paid bills or used Internet banking. The survey showed that travel and accommodation is now the most common Internet purchase.

Section 2 SCOCA E-Commerce Working Party

2

In August 2002, the Ministerial Council on Consumer Affairs (MCCA) agreed to include a consideration of the need for a set of basic, uniform statutory measures to protect consumers engaging in online transactions on its strategic agenda and asked the E-commerce Working Party to give further consideration to the issue.

The E-commerce Working Party comprises representatives from the following agencies:

- Consumer Affairs Victoria (Project Convenor)
- Department of Consumer and Employment Protection, Western Australia
- Competition and Consumer Policy Division, Department of the Treasury, Commonwealth
- Office of Fair Trading, Department of Commerce, NSW
- Office of Consumer Affairs & Fair Trading, Tasmania
- Office of Consumer and Business Affairs, South Australia
- Australian Competition and Consumer Commission
- Department of Tourism, Racing and Fair Trading, Queensland
- Department of Justice & Community Safety, ACT
- Consumer and Business Affairs, Department of Justice, Northern Territory
- Ministry of Consumer Affairs, New Zealand.

This study is one project under consideration by the Working Party. Other areas subject to consideration by the E-commerce Working Party are:

- M-commerce
- The need for a common extra-territorial regime for State/Territory Fair Trading legislation and
- Web seals of approval.

"Section 3 Terms of Reference"

3

The Working Party has been asked to consider and report to MCCA on:

- whether there should be a set of basic and uniform statutory measures to protect consumers engaging in on-line transactions and
- if so, to determine what those measures should be.

"Section 4 Scope"

4

Direct marketing and distance selling involves the marketing of goods and services to consumers using a means of communication at a distance. Contracts of sale are also negotiated at a distance.

Distance marketing and selling includes mail order and catalogue sales, telemarketing and Internet sales. Distance selling has many characteristics which make it different from shop front retailing. These differences include uncertainty about the identity and address of the seller, inability to inspect goods prior to purchase, payment in advance of receipt of goods, uncertain delivery, and redress difficulties where purchases are made across borders.

Governments have recognised that these differences present risks to consumers and so have developed rules and best practice guidance for businesses operating direct marketing. Examples include the Direct Marketing Model Code of Practice, new rules for direct commerce made pursuant to the *Fair Trading Amendment Act* 2003 (NSW) and new telemarketing provisions within the *Victorian Fair Trading Act* 1999.

Online sales is a form of distance selling which gives rise to the risks already noted. However, there is evidence to suggest that consumers see online sales as more risky than traditional distance selling. The United Kingdom National Consumer Council [4] (UK NCC) in its consideration of consumer needs in a virtual world noted the following perceptions of risk when shopping:

SHOPPING TYPE	SAFEST – %	RISKIEST – %
High Street/shopping centre	86	3
Mail order from catalogue	6	5
Mail order from adverts	–	15
Catalogue agent visiting	–	2
Ordering and paying over telephone	2	22
Internet	1	35
Digital TV	1	4

Base 1,950 consumers

[4] UK National Consumer Council *E-commerce and Consumer protection, Consumers – real needs in a virtual world,* 2000 page 3

Perceptions of risk relate particularly to the need to pay for goods in advance by releasing credit card and other personal details. Traditional forms of distance selling such as mail order gave consumers the option of paying by personal or bank cheque, money order or sometimes, cash on delivery. While new forms of payment options are being developed in relation to Internet sales, for example Internet payment providers like PayPal and smart cards, most Internet sales now rely on the supply of credit card details.

The Victorian Drugs and Crime Prevention Committee[5] in its *Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses* noted that the particular features of e-commerce which exacerbate risk are the lack of physical presence of people in transactions, the ability of people to disguise or manipulate identity and the speed with which online transactions take place often denying parties an opportunity to "cool-off" and reflect upon a transaction, verify evidence about the subject matter or identify the other contracting party.

If online sales pose unique risks to consumers, then specially crafted rules may be needed to ensure consumers buying online are not disadvantaged *vis-à-vis* shoppers using more traditional forms of commerce, including other methods of distance selling.

The focus of this paper is online sales[6].

Question 1

Do online sales present a unique and perhaps greater risk of economic loss to consumers than other forms of direct sales?

[5] Parliament of Victoria Drugs and Crime Prevention Committee *Inquiry into Fraud and Electronic Commerce: Emerging Trends and Best Practice Responses* Discussion Paper, October 2002.

[6] The Ministerial Council on Consumer Affairs has recently reviewed the Direct Marketing Model Code of Practice. While issues relating to e-commerce were noted, the review did not analyse the adequacy of current regulatory arrangements relating to online transactions. The review report is expected to be released by the end of the year.

"Section 5 National and International Research into Online Shopping Difficulties"

5

E-commerce has the potential to benefit businesses and consumers and the economy generally. Despite the benefits of convenience and greater choice, the UK NCC noted that "shopping is one of the least popular online activities".[7]

This picture is repeated in Australia and New Zealand – only 14 percent of Australians and New Zealanders with Internet access bought something online in the six months to September 2001[8]. Indeed, Australia is ranked 13th and has a below average proportion of Internet users who are online shoppers compared with other nations surveyed for Taylor Nelson Sofres Interactive's third annual global e-commerce report.

Online shopping ranks well below other e-commerce activities – Internet banking, subscription gaming and searching for a job[9].

Several international and Australian opinion surveys and research studies have sought to explain what is preventing online shopping taking off. Examples of these studies include the following.

The UK NCC research into consumer needs in the virtual world[10]. This research, which was conducted in 2000, was conducted in three phases, a qualitative stage based on group discussions, a structured questionnaire asked of a cross section of the population and additional 'booster' interviews conducted in Scotland and Wales.

Key findings from the research indicated that consumers felt there was a lack of respect for their rights and safety online. They are asked to pay for goods before having seen them, to hand over personal and financial information to companies they often know nothing about and all this against a back-drop of constant warnings about online fraud.

The main disadvantages of shopping online were listed as:

- inability to touch or examine the goods
- releasing credit card details
- fraudulent suppliers
- releasing personal information
- no personal contact
- unknown supplier
- not everyone has access
- hidden charges
- delivery problems, and
- dislike shopping with a credit card.

[7] UK NCC op cit page 1.

[8] NOIE *Current State of Play.* Seven percent of all Australians bought something online during June 2002, Taylor Nelson Sofres Interactive's third annual global e-commerce report.

[9] In the three months prior to 2 July 2003, 36 percent of New Zealand Internet users banked online, 26 percent played online games, 23 percent visited an online job site and 17 percent visited a New Zealand online store, InternetNZ Usage Report 2 July 2003

[10] UK NCC op cit.

In November 2000[11], online shoppers in Australia named the following factors as inhibiting online shopping. The factors included:

- personal size, fitting is important (48 percent of respondents)
- shipping costs too high (40 percent)
- concerns that credit card data will be stolen (36 percent)
- want to see/feel item before buying (28 percent), and
- item is too expensive (22 percent).

In May 2000, NOIE found that the responses given by online shoppers as inhibiting online shopping included:

- credit card security (79 percent)
- disclose personal information (77 percent)
- cannot see or feel merchandise (65 percent)
- shipping and handling charges (55 percent)
- lack of trust in online merchants (48 percent), and
- unfamiliar with online shopping sites (40 percent).

A study by Ernst and Young into online retailing in Australia[12]. Identified the following issues as discouraging online purchasing:

- security of transactions and whether they are conducted by authenticated parties
- disclosure of personal information, and
- levels of service.

Service levels are expected to be at least as good as in the off-line world and preferably with better prices. The main service issues discouraging Australians from buying online seem to be high shipping costs and personal sizing or fit.

Consumers International (CI) *Should I buy? Shopping online: An international comparative study of electronic commerce* (September 2001) reported that many sites failed to:

- give a clear total cost
- give consumers information about key terms and conditions of the contract, and
- state which countries they do business with.

Having placed orders, CI found that six percent of goods did not arrive, nine percent of retailers failed to send a refund for goods returned and in some cases charges were levied for goods that were unavailable. CI noted that there had been improvements since its previous survey but that sites had a long way to go in improving information given on the site and in fulfilling orders reliably.

The Introduction to the OECD's *Report on Consumer Protections for Payments Cardholders*[13] summarises several other opinion surveys and research which document consumers' concern about paying for goods and services online. Examples cited include a survey by Jupiter Media Metrix which found consumers were "overwhelmingly" fearful about theft of credit card data online with 81 percent of US consumers afraid their card number would be intercepted online.

A Pulse survey conducted by Consumer Affairs Victoria (CAV)[14] in January 2003 found that less than half of the respondents surveyed[15] said that they had purchased goods online. Almost half of those who had purchased goods reported that they had experienced problems when doing so. The most common problems experienced related to:

- conversion rates or high delivery costs
- delays in the delivery of goods
- non-delivery of goods, and
- goods received being different from what was expected.

When asked what their main concerns would be if buying goods on the Internet, 66 percent of the respondents identified security issues. Other concerns nominated were:

- privacy issues
- delivery costs and conversion costs
- not knowing who you are dealing with
- lack of confidence in the quality of the goods
- delivery issues such as delays or non-delivery, and
- not knowing what to do if things go wrong.

---

[11] NOIE op cit.

[12] *Online Retailing in Australia, State of Play and Outlook for the Industry,* Ernst & Young, January 2001.

[13] *Report on Consumer Protections for Payment Cardholders,* OECD Directorate for Science, Technology and Industry, Committee on Consumer Policy, 14 June 2002, page 4.

[14] This was not a representative survey, the results cannot be generalised across the population. However, the results are indicative of consumer concerns and attitudes.

[15] 259 consumers were surveyed in face-to-face interviews conducted in the Melbourne Central Business District and in Wangaratta, a Victorian regional city.

The most persistent and serious consumer concerns related to online shopping can be summarised under the following headings.

Security of payment information

Consumers are still unsure whether it is safe to provide their credit card details online[16]. High-profile reports of hackers accessing databases containing credit card details exacerbate these fears. The problem is compounded by scammers who trick Internet users into providing credit card information using e-mail messages or fake websites[17] and unscrupulous online merchants who debit credit card accounts without authorisation. While online fraud is a very real problem, for many consumers lack of information about the extent or likelihood of online fraud and what they can do to protect themselves is also a significant issue.

Privacy

Consumers have doubts about the privacy of personal information supplied to e-traders. New technologies, for example cookies and Web bugs, allow greater tracking of preferences and data collection online than is possible offline. Consumers are concerned about unsolicited commercial e-mail (spam), from online marketers and others.

Fair trading

When there is no personal contact with the retailer and the consumer is paying for goods before delivery there are increased concerns about the quality and suitability of the goods, whether they will be delivered on time (or ever), what procedures are in place for refunds and complaints and how the consumer can get in contact with the merchant. These concerns and uncertainties may be magnified when traders are located in other jurisdictions.

Intrinsic issues

Many consumers enjoy the traditional shopping experience where they can touch, inspect or try on goods they are interested in. Such consumers are not so much concerned about online shopping as uninterested in the medium.

Question 2

Is the above an appropriate summary of risks and consumer concerns regarding online shopping?

Question 3

Are there other concerns which have not been identified?

[16] As a further example, an American Express survey in 2001 indicated that nearly 20 percent of all New Zealanders are worried about the security of shopping online. Thirty-six percent of non-purchasers in Australia said they have not purchased goods or services online because they do not want to disclose their credit card details. Taylor Nelson Sofres Interactive's third annual global e-commerce report, June 2002.

[17] In Australia recently, consumers have been tricked by scams involving fake Australian bank websites.

Section 6 Consumer Complaints

6

Complaints to government agencies nationally and internationally present a diverse picture.

The Drugs and Crime Prevention Committee[18] provided the following data on electronic commerce consumer complaints.

- During 2001, the Internet Fraud Complaint Centre (a joint initiative of the Federal Bureau of Investigation and US Department of Justice) received 49,711 complaints relating to Internet fraud of which 16,775 were referred to authorities for action. Of the referred complaints, 43 percent related to online auctions, approximately 20 percent related to undelivered merchandise and 10 percent to credit/debit card fraud. 2001 was the first year in which the data was reported. Australia accounted for 0.5 percent of complaints registered by the Internet Fraud Complaint Centre in 2001, behind the US (93.4 percent), Canada (2.2 percent), and the United Kingdom (1.0 percent).
- The US Federal Trade Commission's Consumer Sentinel recorded over 200,000 complaints in 2001 as compared with 18,600 in 1999 and 8,000 in 1998. In 2002, 47 percent of the 218,284 complaints lodged on the Sentinel database were Internet related. Internet related complaints represented 47 percent of all fraud related complaints up from 42 percent in 2001 and 31 percent in 2000. Where consumers reported the method of initial contact, 54 percent said the fraudster contacted them using either the Web site advertising, Internet software or e-mail. Only 23 percent were contacted by telephone and 13 percent by mail.
- In a telephone survey of online consumers conducted for the National Consumers League in the US between April and May 1999, 24 percent said they had purchased goods and services online but 7 percent which represented six million people, said they had experienced fraud or unauthorised use of credit card or personal information online.
- The top 10 types of Internet fraud recorded by the US Internet Fraud Watch between 1999 and 2001 were:
  - online auctions
  - general merchandise sales
  - Nigerian money offers
  - computer equipment and software
  - internet access services
  - information adult services
  - work-at-home schemes
  - advance fee loans
  - credit card offers, and
  - business opportunities/franchises.

[18] Parliament of Victoria Drugs and Crime Prevention Committee, op.cit.

- In 2002 the total amount reported lost to Internet-related fraud in the US was $122.36 million. That figure is based on 94,502 complainants who reported an amount lost. The top complaint categories in 2002 were Internet auctions (50 percent), shop-at-home/catalogue sales (13 percent), Internet access services (11 percent), foreign money offers (5 percent), Internet information services (including adult services) (5 percent).

Econsumer.gov, a joint service of consumer protection agencies in 17 nations, listed complaints filed from 27 April 2001 to 30 June 2002. The site has received more than 2,500 complaints since its launch in April 2001. The data showed that the top complaint was "Merchandise or service never received", followed by "Other misrepresentations", "Cannot contact merchant", "Failure to honour refund policy" and "Billed for unordered merchandise or service." Fifteen percent of consumer complaints are now about Internet auction services.

During the 01/02 financial year, the Australian Competition and Consumer Commission received 3,317 complaints relating to online trading. Of these, there were 638 consumer complaints dealing directly with online shopping issues such as misleading advertising, warranty and refund problems, receiving unsolicited goods or services, unauthorised billing and failure to receive purchased goods.

In the financial year ending June 2003, 2,899 complaints related to online conduct. This represented 5.4 percent of total complaints received. The seven most common issues complained about were as follows:

Issue	% of complaints
Misleading advertising or prices	23
Domain name renewals	20
Pyramid selling and other scams	7
Unsolicited goods or services	4
Warranty matters	4
Anticompetitive arrangements	2
Unconscionable conduct	1

At the State and Territory level e-commerce, including Internet sales complaints are not always recorded separately, for example, if a product purchased online is faulty, it will be recorded as a faulty product. Where complaints are captured, they are generally a very small percentage of total complaints received. For example during 2002, Consumer Affairs Victoria received 183 e-commerce complaints – up on the 57 received the previous year. Of these, 41 percent related to Internet sales – mainly the purchase of computers, computer accessories and software; 35 related to domain name services and 24 percent to Internet Service Providers.

The NSW Office of Fair Trading currently receives approximately 250 e-commerce-related complaints per year. This is a very small proportion of the total number received by the Office.

It is difficult to draw conclusions from complaints data. First, it is indicative of the range of issues experienced by consumers in relation to the Internet including those which would be handled by consumer affairs agencies, some which would go to the Police and some which would go to regulators like the Privacy Commissioner. Second, while the level of complaints represents a very small percentage of online transactions[19], the data is likely to underestimate particular problem areas, for example non-delivery of low cost goods, where consumers may decide to "put it down to experience". One of the particular findings of the Parliament of Victoria Drugs and Crime Prevention Committee in its Final Report into Fraud and Electronic Commerce[20] is that people are very reluctant to report electronic fraud. Third, it is not clear that consumers who experience online difficulties will know who to turn for assistance – the Pulse survey cited earlier noted that of the people surveyed, at least half said they were unsure where to go with online shopping issues.

Question 4

Are complaints a good gauge of issues faced by consumers buying goods and services online?

[19] ABS report op.cit.

[20] Parliament of Victoria Drugs and Crime Prevention Committee, *Inquiry into Fraud and Electronic Commerce – Final Report (2004).*

"Section 7 Issues"

7

In section 5, consumer issues were summarised under four categories, security of payment, privacy, fair trading matters and issues intrinsic to the online medium. Of these, only security of payment, privacy and fair trading issues give rise to potential consumer detriment and are considered further in this section.

7.1 Payment Security and Cardholder Protections

Payment cards including credit cards are currently the main method of paying for goods and services online. Like most forms of distance selling, payment is in advance of receipt of the goods or services. The OECD Report on *Consumer Protections for Payment Cardholders*[21] provides a useful summary of the types of problems consumers encounter paying for online transactions. It divides the problems into three groups:

- ***I didn't do it*** – unauthorised transactions which are the result either of fraud or error. The OECD Report suggests that the incidence of payment card fraud online is higher than other forms of commerce and is growing[22]. The National Office for the Information Economy has suggested however, that consumer concerns about online payment security are disproportionate to the actual risks[23].
- ***I didn't receive it*** – where the consumer has not received goods or services paid for after a reasonable time. The OECD report also suggests that this includes complaints where goods do match the description of what was ordered though such complaints may equally be included in the following and final category.
- ***I don't want it*** – includes goods which are not fit for purpose or are defective, or where a trader does not honour a cooling off right which has been exercised by a consumer.

Various organisations and mechanisms are involved in addressing the consumer risks arising from online payments. In Australia, key protections arise primarily from voluntary arrangements rather than statutory protections. They include:

Payment card networks' chargeback mechanism, simply referred to as "chargebacks". The OECD Report[24] describes in some detail how these processes work. In general, where goods or services ordered do not arrive, are defective or transactions are unauthorised, the cost of the transaction is charged back against the merchant. The merchant can dispute the claim but ultimately the matter is decided between the card issuing company and the merchant's bank.

[21] OECD Report op. cit., page 11.

[22] OECD Report op. cit., page 6.

[23] *Setting the record straight about online credit card fraud for consumers,* National Office for the Information Economy, 2001.

[22] OECD Report op. cit., pages 8-10.

While chargeback arrangements provide quite effective consumer protection, it is arguable whether consumers are aware of them or have any understanding of their operation.

The Review of the Code of Banking Practice (CBP) considered the issue of chargebacks in both its Issues Paper and Final Report. As a result, the Australian Bankers Association has agreed to include a clause on chargeback disclosure in the revised CBP[26]. This will require all subscribers to the Code to provide general information on chargeback rights, the timeframe for disputing a transaction and a warning that the ability to dispute a transaction may be lost outside the applicable timeframe. The revised CPB will also require subscribers to exercise chargeback rights if available and not to accept a refusal of a chargeback by a merchant's financial institution unless it complies with the card's scheme rules.

The *Electronic Funds Transfer Code of Conduct,* developed under Australian Securities and Investments Commission (ASIC) auspices, is a voluntary code which also provides consumers some protection in the case of unauthorised transactions where there is no contributory negligence on behalf of the consumer, for example disclosing a PIN to another party. Most, if not all banks are signatories to the Code.

While payment by credit cards is currently the most popular means of paying for goods and services online, alternative online payment methods are growing in popularity. Online payment service providers, such as PayPal, manage payments between buyers and sellers.

Buyers typically open a PayPal account linked to a standard bank account or a credit card account. An electronic funds transfer can top up the PayPal account, which is used to pay sellers when a purchase is made.

This type of online payment is particularly common between buyers and sellers engaged in online auctions, especially where the seller is not able or does not want to accept credit card payments.

More recently, this payment mechanism has gained popularity at standalone online stores[27], possibly because services like PayPal market themselves as offering reduced liability for chargebacks.

At the same time as offering sellers protection from chargebacks, PayPal does not guarantee refunds for buyers whose goods are not delivered. Furthermore, PayPal will not entertain buyer claims for not-as-described goods.

Accordingly, the consumer protections provided by credit card chargebacks are diluted, or non-existent, in some online payment transactions unless they are directly linked to the credit card.

Question 5

Are existing chargeback rights an effective means of consumer protection?

Question 6

Are consumers generally aware of chargeback rights?

Question 7

a. Will the growth of alternative online payment processes reduce the consumer protection currently provided to consumers through chargeback mechanisms?

b. Are there other measures which could be adopted to protect consumers if other online payment methods become common?

[26] As at 15 August 2003, the following banks have adopted the revised Code of Banking Practice – Adelaide Bank Ltd; Australia & New Zealand Banking Group Ltd; BankSA (A division of St George Bank Ltd); Commonwealth Bank of Australia; St George Ltd.

[27] PayPal reports over 42,000 websites accept PayPal (Aug 2003).

While the control of liability arising from unauthorised use of credit cards is governed by non-legislative and contractual means[28], the OECD Report[29] notes that some OECD members have regulatory regimes protecting consumers against unauthorised use of cards, non-delivery of goods and services and non-conforming goods and services. For example, the UK Distance Selling Regulations[30] provide that if fraudulent use is made of a consumer's credit, debit or stored value card for distance selling, the consumer is entitled to cancel payment and be reimbursed in full by the card issuer. Under the Distance Selling Regulations, the onus to show that a debit was authorised is placed on the card issuer.

The Canadian fair trading legislation requires a card issuer to cancel or reverse any credit card payment (and associated interest or charges) on request by the consumer if the consumer has exercised a cancellation right and the trader has not refunded the consideration within the 30 days.

Other responses to the risks posed by online payments include:

Technological Responses

There has been significant investment by both the government and non-government sectors in developing and enhancing the security of payment systems in use online. Examples include the development of Secure Sockets Layer (SSL) technology, the development of Public Key Infrastructure (PKI),[31] VeriSign's Trusted Commerce program[32] and various credit card and banking initiatives[33].

Education and Information

Consumer affairs and other government agencies[34] provide a range of information fact sheets and other tools to assist consumers make informed decisions about the level of risk involved in online transactions and steps to take to lessen risk. For example, in 2002, Consumer Affairs Victoria developed ShopSafe™, an interactive tool that teaches consumers what they should be looking for at each stage of a web purchase. This tool is aimed at people with little online shopping experience.

---

[28] The terms and conditions of most common credit cards specify that consumers will not be held liable for unauthorised transactions (apart from the first $50 - $100) as long as the transactions are reported immediately.

[29] OECD Report op.cit pages 13-16.

[30] *Consumer Protection (Distance Selling) Regulations 2000.*

[31] Based around public key infrastructure (PKI) authentication, certification authorities and digital certificates, this is an attempt to bolster security online. However, digital certificates have not yet taken off in the B2C market and PKI has found most of its applications in B2B e-commerce and in e-government (as in the Commonwealth's Gatekeeper strategy). Its future take-up will depend in part on reduced costs and whether digital certificates can become more interoperable across computing platforms and different applications. PKI cannot guarantee the business is trustworthy or that the consumers' information will be kept private and secure once received.

[32] Launched in July 2002, Trusted Commerce is a marketing program that is primarily concerned with security, verifying identity during online transactions and the authentication of web servers. Verisign provides the software, often to large web hosting providers who have many small businesses online. This is one commercial solution that addresses the problem of consumers abandoning online credit card purchases during payment because they do not feel safe online.

[33] Internet users with VISA credit cards are provided with a password for credit card use at online stores, protecting against losses through theft or hacking of card number databases. This program is aimed at reducing credit card fraud online by confirming or denying the identity of the consumer to the merchant and reducing the use of stolen cards and numbers.
MasterCard has also announced that it will introduce a new PIN authorisation system, SecureCode. The system is intended to ease consumer concerns about online shopping and also provide online merchants with greater assurance about the identity of the person completing the transaction.
A Fraud Taskforce convened by the Australian Bankers Association has commenced work on three major projects aimed at improving fraud prevention in all banking transactions both electronic and face-to-face banking transactions. The three projects are
- The development of voluntary industry standards on security and fraud prevention.
- An analytical study of identity documents.
- The development of a fraud education program for banking customers.

The prevention of identity fraud will be the focus of this year's work. Skimming and Internet security have been identified as other areas of high priority.

[34] A great deal of information about online security is available, for example at:
http://www.ecommerce.treasury.gov.au
http://consumer.vic.gov.au
http://www.accc.gov.au/ecomm.access1b.htm
http://www.noie.gov.au/publications/NOIE/trust/index.htm

Other Voluntary Measures

In relation to payment security, the BPM advocates that businesses should:

- provide:
  - easy to use payment mechanisms;
  - security that is appropriate to the transaction;
  - access to information on the security of payment and authentication mechanisms; and
- not contract out of responsibility for losses arising from the misuse or failure of authentication mechanisms.

The Australian Direct Marketing Association (ADMA) Code of Practice, which is based on the Direct Marketing: A Model Code of Practice, contains provisions relating to online sales and unauthorised transactions. For example, clause 29 of the ADMA Code states: "Limitations of liability for unauthorised transactions or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of the electronic commerce".

The effectiveness of these voluntary codes depends on the extent to which they have been adopted by business. The Commonwealth Government is currently reviewing the effectiveness of the BPM[35]. The ADMA Code, also, is to be considered by the ACCC in the context of a revocation and substitution of authorisation process.

Redress

The Australian Banking Industry Ombudsman scheme will handle complaints relating to chargebacks. The Ombudsman takes the view[36] that exercising a chargeback where there is a right is good banking practice. Accordingly, where a bank fails to chargeback correctly, the consumer should be compensated for any loss without being required to attempt to recover against the merchant.

Question 8

Is the current mix of measures adequate to address consumer online payment risks?

Question 9

Should payment cardholders have a right to cancel unauthorised card debits, with the onus on the card issuer to show that the debit was authorised?

7.2 Privacy

The OECD's *Privacy Online: Policy and Practical Guidance*[37] summarised the privacy issues relating to the online world as follows:

> In the digital economy, individuals may leave behind electronic "footprints" or records of where they have been, what they spent time looking at, the thoughts they have aired, the messages they sent, and the goods and services they purchased. The related privacy issues arise from the fact that all this computer-processable personal information, whether automatically generated or not, can potentially be collected, stored, detailed, individualised, linked and put to a variety of uses in places geographically dispersed all around the world, possibly without user knowledge or consent[38].

The *Privacy Act* 1988 (Cth) and the *Privacy Amendment (Private Sector) Act* 2000,[39] which extended coverage of the Act to the private sector, are the major mechanisms through which information privacy concerns are addressed in Australia. The Act contains the National Privacy Principles (NPPs) which set out how organisations should collect, use and disclose, keep secure and provide access to personal information. The principles give individuals a right to know what information an organisation holds about them and a right to correct information.

[35] Senator the Hon Ian Campbell Parliamentary Secretary to the Treasurer, Media Release dated 3 July 2003.

[36] Noted in the *Review of the Code of Banking Practice*, Issues Paper February 200, page 83 and following.

[37] OECD Directorate for Science, Technology and Industry Committee for Information, *Privacy Online: Policy and Practical Guidance*, Computer and Communications Policy, 21 January 2003.

[38] ibid, page 5.

[39] The website of the Office of the Federal Privacy Commissioner at http://www.privacy.gov.au provides extensive information about Australia's privacy laws

The Privacy Act sets base line standards which apply equally online and offline. However, the regulatory model established is essentially co-regulatory[40] with organisations encouraged to develop their own response to the NPP through codes of conduct. These codes can then be approved by the Privacy Commissioner. The Working Party notes that the Internet Industry Privacy Code is currently one of the few codes under consideration by the Privacy Commissioner[41].

In addition to legislation and codes, the Privacy Commissioner provides detailed consumer information about online privacy issues and ways to enhance information privacy online, for example *5 steps to better on-line privacy*[42].

Responsibility for regulation of information privacy particularly as regards the private sector rests with the Federal Attorney-General and the independent Office of the Federal Privacy Commissioner. The Working Party understands that the effectiveness of the *Privacy Amendment (Private Sector) Act* 2000 will be reviewed in 2004.

At this time, the Working Party makes the following observations:

- The scope of Australia's privacy legislation is limited by the exemption of many Australian businesses from its application. Under section 6D of the Act, Small Business Operators are exempt from the application of the Privacy Act. An organisation is deemed to be a Small Business Operator if during a financial year its annual turnover for the previous financial year was $3 million or less. Small Business Operators which trade in personal information or are associated with a larger organisation or providing health services are not exempt. Arguably, many online traders would be exempt from the Privacy Act.
- Many Australian websites do not publish privacy policies. An 'Internet Sweep' was conducted by the Australian Competition and Consumer Commission on 14 and 15 February 2001. The sweep of 250 Australian sites was part of a wider, international 48-hour sweep by 48 agencies in conjunction with the International Consumer Protection and Enforcement Network. Twenty-seven per cent of Australian e-tailers had posted privacy notices[43]. In May 2003, a Consumer Affairs Victoria survey of 380 Australian websites found that 27 percent had posted a privacy policy.
- The BPM states businesses should provide consumers with clear and easily accessible information about the way in which they handle personal information.
- In the US, legislation improved disclosure of data collection practices. The US Federal Trade Commission's April 2001 Children's Online Privacy Protection Act (COPPA)[44] compliance survey found that the vast majority – nearly 90 percent – of 144 sites that collected personal information from children had privacy policies as opposed to only 24 percent in 1998, before passage of the legislation[45].
- It is also important that privacy policies are accessible[46]. Some e-traders have been criticised for designing privacy policies that are almost inaccessible to everyday site users through lengthy policies with no summary and no plain English[47].

[40] According to a news report, Privacy complaints soar in Australian IT on 2 September 2003, the Office of the Privacy Commissioner has been "deluged" by complaints about business misuse of personal information. While businesses were expected to self-regulate by establishing and administering industry specific codes, self-regulation has yet to emerge. Mr Crompton is quoted as saying "In the end, the office is the primary enforcer of privacy law in the private sector, as compared with expectations that many more Australian businesses would have put up their own codes". See http://australianit.news.com.au/articles/0,7204,7136833^15306^^nbv^,00.html

[41] See http://www.privacy.gov.au/business/codes/index.html#2

[42] See http://www.privacy.gov.au/internet/tools/index.html

[43] http://www.accc.gov.au/

[44] The Children's Online Privacy Protection Act 1998 (COPPA) came into effect in April 2000. It requires websites to meet certain criteria to safeguard the privacy of young Internet users. COPPA requires websites that are targeted at, or collect information from children aged 13 and under to post a privacy policy that is linked to from the site's home page and on every page in which personal information is collected from children. The privacy policy must explain:• The type of information the site is seeking • How that information will be used • Whether the information will be shared with any other business or advertisers; and • How the child or his/her parent can contact the site.
Sites must obtain parental consent before such information is collected. Consent may be given to only one part of a request. Parents must also be given the opportunity to review their child's information as collected by the site and may delete or change it at any time.

[45] http://www.ftc.gov/opa/2002/04/coppaanniv.htm

[46] A survey of 2,000 online shoppers found consumers report a high level of difficulty in understanding privacy polices, Harris Interactive (December 2001).

[47] At one time, Amazon.com's privacy policy was over 50 pages when printed, US Federal Trade Commissioner Sheila F. Anthony, The Case for Standardization of Privacy Policy Formats, http://www.ftc.gov/speeches/anthony/standardppf.htm

7.3 Fair trading

Many of the concerns expressed by consumers about online transactions – complaints about non-delivery of goods, length of time for delivery, non-disclosure of costs and charges, product quality[48] and concerns about redress – are issues which consumers face generally with regard to distance selling. Together with privacy concerns and payment security concerns, they can undermine consumer confidence in online transactions. The difference between privacy and payment security concerns and fair trading concerns is that the MCCA is in the "driver's seat" in determining whether reforms are needed in relation to fair trading issues and if so, the nature of those reforms.

7.3.1 Information

An important element of an effective market is the provision of full and accurate information to enable consumers to make rational decisions about whether to buy, what to buy, how to buy and from whom to buy. Information is necessary for the effective exercise of consumer choice and also empowers consumers to understand and exercise their rights.

Adequate information is particularly significant online because consumers cannot go into the retail outlet, talk to the merchant or inspect the goods on offer. They are reliant on the information provided on the merchant's website.

To make informed purchasing decisions consumers need clear and accurate information about the business they are dealing with, the product or service they are buying and the terms and conditions of the purchase. They also need advice about what to do if something goes wrong.

The results of the international Internet Sweep Day held in September 1999 showed that at that time most e-commerce sites failed to provide even basic consumer information[49].

The Consumers International 2001 study[50] also revealed that too few sites gave consumers information about total costs, key terms and conditions of the contract or details of the countries in which they carried out business.

Current Regulatory Measures

The *Trade Practices Act* 1974 (Cth) and State and Territory Fair Trading legislation prohibit misleading and deceptive conduct including false and misleading representations and omissions of information which misleads or deceives consumers.

In Victoria, legislative protections go further[51] and require disclosure of the supplier's full business address or telephone number, the total price, postal/delivery charges and the availability of any cooling off rights. Where such cooling off rights exist, they are deemed to be 10 days.

While current legislation contains comprehensive prohibitions against misleading representations[52], and arguably requires total cost disclosure if it is represented as or implied to be a total cost[53], it does not contain provisions as to what information must be provided to consumers.

Guidance as to what information should be included in websites[54] is contained in the BPM, which, as has been noted, is a voluntary, model code. There is no requirement for compliance with this code and no active monitoring of compliance where businesses have elected to become signatories.

As noted earlier, the BPM is currently subject to review.

---

[48] These concerns were among those noted by Industry Canada at a December 2000 Hague Conference - see *OECD Report on Consumer Protections for Payment Cardholders*, op. cit page 6.

[49] ACCC news release *E-commerce fails the Test: International Sweep Day Results Show Most Sites Don't Provide Basic Consumer Information* at http://www.accc.gov.au/media/mr-197-99.htm

[50] Consumers International, op.cit.

[51] Fair Trading Act 1999 (Victoria) Div. 3, Part 4.

[52] The TPA has been used effectively to prosecute traders against misleading online conduct. For example, in April 2002, Bikes Direct entered into an enforceable undertaking with the ACCC. Bikes Direct is an Internet trader based in Australia which had allegedly mislead consumers regarding warranties and refunds and had sold bikes that did not comply with mandatory Australian consumer product standards. In November 2002, the ACCC filed proceedings against the operator of a website purporting to be the official booking site of the Sydney Opera House. In this case, several consumers in the United Kingdom and Europe had sought to purchase tickets from the site. Their credit cards were charged for the tickets but no tickets were received.

[53] In ACCC v Dell Computer Pty Ltd, the Federal Court held that Dell Computer had published misleading advertisements by not stating that a compulsory delivery fee would also be charged.

[54] In relation to information disclosure, the BPM recommends businesses:
- identify themselves, including: ■ business name ■ physical and registration address ■ e-mail address and telephone number ■ ABN or CAN or other registration/licence number ■ contact details/links to bodies/codes of which the trader is a member.
- provide sufficient information about the transaction including: ■ itemisation of all costs collected by the trader (in the applicable currency, with currency exchange information or links to currency exchange sites), or the method of calculation ■ notice of delivery, postage, handling, insurance and other charges and taxes not collected by the trader ■ notice of ongoing costs, and method of notification of changes ■ period during which offer is valid ■ applicable restrictions, limitations or conditions ■ payment methods ■ terms of delivery ■ termination, return, exchange, cancellation, refund, or renewal terms ■ applicable warranties ■ applicable after-sales service ■ for Australian consumers, the Australian jurisdiction whose law governs the contract (and a statement that any dispute will be heard by an Australian court or tribunal) and, for other consumers, any stipulated governing law or forum. The BPM also suggests businesses disclose their privacy policies and procedures and the security and authentication mechanisms used.

Overseas

Some overseas jurisdictions have developed mandatory information disclosure requirements.

On 25 May 2001, Canadian Federal, Provincial and Territorial Ministers responsible for consumer affairs approved a new approach to harmonise consumer protection legislation in electronic commerce. A common template[55] was approved which covers contract formation, cancellation rights, credit card charge-backs and information disclosure.

Suppliers will be required to disclose the following information to consumers:

- The supplier's name and, if different, the name under which the supplier carries on business.
- The supplier's place of business, and if different, the supplier's mailing address.
- The supplier's telephone number and, if available, the supplier's e-mail address and facsimile number.
- A fair description of the goods or services being sold to the consumer, including any relevant technical or system specifications.
- An itemised list of the price of the goods or services being sold to the consumer, as well as any shipping charges, taxes, custom duties or broker fees payable by the consumer to the supplier.
- The total consideration payable by the consumer to the supplier under the contract and the currency in which it is payable.
- The terms, conditions and method of payment. The date when goods are to be delivered or the services are to be commenced.
- The supplier's delivery arrangements, including any delivery, postage and handling and insurance costs that are not included in the price of the goods or services.
- The supplier's cancellation restrictions, limitations or conditions of purchase that may apply.

The required information must be disclosed in a clear and comprehensible manner on one Web page and consumers are required to be supplied with the contract, either in writing or electronic form within 15 days after the contract is entered into.

The Internet Sales Contract Harmonisation Template has been adopted in Alberta, Ontario and Nova Scotia and is progressing in other provinces. Manitoba had an Internet Agreement Regulation (2000) which preceded the Template but which contains very similar rules.

Article 5(1) and 5(2) of the EU Directive 2000/31/EC on e-commerce requires Member States to ensure that service providers make certain information such as their name, geographic address, electronic mail address, details of any trade registration or professional affiliation available to the recipient of the service easily, directly and permanently accessible. Where there is a reference to price, these must be indicated clearly and unambiguously and shall indicate whether they include tax and delivery charges.

The EU Distance Selling Directive also contains requirements about information disclosure. According to this Directive, the supplier must provide the consumer with clear and comprehensive information concerning:

- the identity and address of the supplier
- the characteristics of the goods or services and their price
- delivery costs and delivery times
- details of terms for returning goods
- details of deadlines for returning goods
- general terms and conditions of business
- the arrangements for payment, delivery, or performance
- the existence of a right of withdrawal
- the period for which the offer or the price remains valid
- the cost of using the means of distance communication, and
- the minimum duration of the contract.

[55] http://strategis.gc.ca

[56] Eighty-one per cent of U.S. users polled said it is "very important" sites should list their e-mail address, street address or telephone number where they can be contacted, Consumer WebWatch Transparency Survey.

The United Kingdom has implemented this Directive on 31 October 2000 via the Consumer Protection (Distance Selling) Regulations 2000. The Regulations require traders to disclose:

- their identity and street address
- their 'commercial purpose'
- the main characteristics of the product
- the (tax inclusive) price
- any delivery costs
- the payment, delivery and performance arrangements
- the statutory cooling-off right and process
- any contractual right to cancel
- the period the offer remains valid
- any minimum duration of a contract for services
- any substitute for unavailable product
- any after-sales service
- any guarantees, and
- any inability to cancel after the commencement of services.

The BPM, the EU E-commerce and Distance Selling Directives all identify similar sorts of information which should be disclosed to consumers – see following. The question is, should disclosure be mandatory or be left, as is the case now, to voluntary instruments and market forces.

7.3.1.1 Identity of and ability to locate E-Traders

A common concern voiced by consumers is the difficulty determining who they are dealing with online[56]. When a consumer walks into a physical store, they automatically derive from their surroundings the store's trading name, its location or address, and a means by which to contact someone in case of any problems.

In the online world, that information is not obtained in the same way. It needs to be explicitly made available for the online consumer to have the same level of knowledge as the same customer in a physical store. Without that information, the online consumer is at a disadvantage

The key information relates to the identity of the business and a means to contact them either via mail, telephone or electronically in case of any problems.

These are positive disclosure requirements that place only a small or insignificant burden on the e-trader.

Clear disclosure of such information could provide consumers with a greater 'safety net' when problems arise with online traders, by enabling consumers to easily contact traders to resolve disputes. This may lead to more effective resolution of minor service difficulties and more serious contractual disputes.

It should be noted that the majority of Australian websites disclose this sort of information. It needs to be determined whether this information is important enough that it should be on every site.

Some identity information can currently be obtained through mechanisms like *WHOIS*. The public *WHOIS* service is a standard feature of Internet domain name systems around the world. It allows Internet users to query a website's domain name to find out the identity of the registrant.

For Australian domain names, the publicly available information is limited to the registrant's name and a contact e-mail address. The street or registered address of the trader and its telephone number is not disclosed[57], according to Australian *WHOIS* policy.

[56] Eighty-one per cent of U.S. users polled said it is "very important" sites should list their e-mail address, street address or telephone number where they can be contacted, Consumer WebWatch Transparency Survey.

[57] The full data record is only available to law enforcement in the event of an official investigation.

The data available to the public on *WHOIS* can, on occasions, provide some valuable information to consumers to help in their initial assessment of the trustworthiness of a particular website. However, the technical competence to look up publicly available WHOIS data is arguably limited to a very small proportion of Internet users. Without specific consumer education strategies, this is unlikely to change.

A requirement to disclose name, address, telephone number and e-mail address is contained in the Victorian[58], European, UK, US[59], and Canadian legislation, as well as in the BPM, the ADMA code and proposed Australian national anti-spam legislation.

Question 10

a. Are there potential or existing consumer problems related to the non-disclosure of an e-trader's legal name, address, telephone number, and e-mail address?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure?

7.3.1.2 Total costs in the applicable currency

Another complaint common in surveys of consumers' attitudes to online shopping is that purchasers may incur extra costs which they were not expecting. Those costs could include delivery charges, handling fees, taxes, customs duties, or broker fees.

This is a very serious issue for those consumers who can feel they have been misled when they receive higher bills than expected[60].

In a store, a label or tag usually states the total cost clearly. Online, the consumer may become confused when the total cost is not displayed clearly at the time of ordering. Having this information is even more important when paying before delivery and receipt of goods.

Costs should always be stated in the applicable currency. A standard format for disclosure of cost information could assist e-traders and reduce disputes with customers.

It should be noted that there are current prohibitions on false representations about price. Stating total cost, however, would constitute positive disclosure on the part of online traders and total price transparency.

A further issue that should be considered is in circumstances where full details of postal and delivery costs are not known at the time of the transaction. In these circumstances, the means of arriving at the total cost may need to be disclosed. A standard approach, when the price is not known at the time the contract is entered, is to state how the price will be determined[61].

Customs charges in international orders, may not be known by a particular online business. Further it may be too onerous to expect businesses to obtain this information. In this case, it may be adequate for the trader to state that the customer is responsible for any customs charges.

A requirement is present in the Victorian, UK, and Canadian legislation, as well as in the BPM and the ADMA code.

Question 11

a. Are there potential or existing consumer problems related to the non-disclosure of total costs in the applicable currency?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of total costs?

[58] The Victorian legislation only requires business name or contact telephone number.

[59] For all organisations subject to COPPA.

[60] When asked what information they thought websites should provide, 95 per cent of survey respondents said it is "very important" for e-commerce sites to specifically disclose all fees, Princeton Survey Research Associates (January 2002), A Matter of Trust: What Users Want from Web Sites, http://www.consumerwebwatch.org/news/1_abstract.htm.

[61] See for example, the Fair Trading Act 1999 (Vic) section 61.

7.3.1.3 Returns/Refunds/Exchange/ Cancellation Policies

Consumers should know what will happen if something goes wrong, such as the goods not arriving or arriving damaged. They are familiar with returning faulty goods to stores. Policies are usually posted or are available on demand and a customer service desk or manager can usually be located.

However, when traders are not close to the buyer or when they do not have a physical store that customers can visit, the process is complicated and uncertain. In these situations, consumers need clear information about return, refund, exchange, and cancellation policies in order to make an informed decision at the time of purchase and in the event of post-sales issues[62].

Most businesses already have these policies. They would be available to a customer in a store and they arguably should be available to a customer online. Such information is fairly easily provided and may reduce disputes and service calls from customers.

A requirement is present in the UK, European, and Canadian legislation, as well as in the BPM and the ADMA code.

Question 12

a. Are there potential or existing consumer problems related to the non-disclosure of returns/refunds/ exchange/cancellation policies?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of returns/refunds/exchange/cancellation policies?

7.3.1.4 Delivery arrangements/ timelines

Linked to concerns about identity and reliability are consumer fears about the delivery (or non-delivery) of their goods. These fears are exacerbated in distance sales such as B2C e-commerce when the consumer is not certain with whom they are dealing.

While the protection afforded consumers through chargebacks (see section 7.1) is significant, confidence could be improved by clear disclosure of when and how consumers could expect to receive the goods.

A requirement is present in the UK, and Canadian legislation, as well as in the BPM and the ADMA code.

Question 13

a. Are there potential or existing consumer problems related to the non-disclosure of delivery arrangements/timelines?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of delivery arrangements/timelines?

[62] Eighty-eight percent of U.S. Internet users polled said it is very important e-commerce sites have a statement of policies for returning unwanted items or cancelling reservations, Consumer WebWatch Transparency Survey.

7.3.1.5 Complaints/Dispute resolution processes

In the case of problems with a purchase form a local store, a consumer can talk face-to-face with someone who may be able to resolve their complaint.

Online, the process may not be so transparent and personal and consumers may feel more secure knowing how their complaint will be dealt with and what the process is should they have a problem. This information should also contain details of any dispute resolution service of which the e-trader is a member.

The May 2003 study of 380 Australian trader websites by CAV found 4 percent had clear information about complaints handling procedures. However, such disclosure may not provide to consumers any guidance on the standard of dispute resolution mechanisms to be provided.

A requirement is present in the BPM and the ADMA Code.

7.3.1.6 Product suitability

It may be desirable for an e-trader to give the consumer the opportunity to detail the purpose for which they are acquiring the product or the result desired. Offline consumers have the opportunity to see and examine products before purchase. They can also seek the advice of the merchant. In B2C e-commerce the consumer is often relying on standard or generic information provided by the e-trader.

Allowing consumers to indicate the purpose for which the goods are to be used would enable section 74B of the Trade Practices Act – 'Actions in respect of unsuitable goods' – to apply.

This may be a cumbersome approach, which will not assist inarticulate consumers. The Canadian and UK legislation address this problem from a different angle, instead requiring provision of: 'a fair and accurate description of the product, including any technical or system specifications'.

Question 14

a. Are there potential or existing consumer problems related to the non-disclosure of complaint handling procedures and any dispute resolution service?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of complaint handling procedures and any dispute resolution service?

Question 15

a. Are there potential or existing consumer problems related to the non-disclosure of information about the suitability of a product?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of information about the suitability of a product?

7.3.1.7 Privacy of personal information

Exemptions from the privacy regulatory regime and the general low level of disclosure of privacy policies were noted in section 7.2.

While it is appropriate that national privacy legislation set out the obligations of traders with respect to information privacy, disclosure of such policies would be within the scope of state and territory Fair Trading legislation.

Requirements are present in the Canadian and US legislation[63], elsewhere in European legislation, in the BPM and the ADMA code.

Question 16

a. Are there potential or existing consumer problems related to the non-disclosure of policies on the collection, storage, use and trade of consumers' personal information?

b. If so, given a range of self-regulatory or regulatory options, what is the best way to improve online disclosure of policies on the collection, storage, use and trade of consumers' personal information?"

7.3.2 Cooling-off rights

Cooling-off rights have traditionally been used where a consumer is likely to subjected to high pressure sales methods from which they can not easily walk away, for example door-to-door sales. A further rationale for cooling-off rights has been the consumer's inability to shop around and compare products and prices. The cooling-off gives the consumer time to re-consider and compare the purchase.

Legislative cooling-off rights in Australia currently generally only apply in the case of door-to-door selling. The non-contact sales provisions within the Victorian Fair Trading Act require an e-trader to disclose cooling-off (and other cancellation rights) where such rights are provided by the e-trader. Where a cooling-off right is provided as a condition of the contract, the Victorian legislation deems this to be 10 days[64].

The UK Distance Selling Regulations give the consumer the right to cancel a contract and obtain a refund (minus costs for delivery) for whatever reason within seven working days from the date that the consumer received the goods. There are exceptions for perishable goods, custom-made goods and dated goods such as magazines.

There are advantages and disadvantages regarding a cooling-off right in online sales. There is not the same rationale for applying cooling-off rights online as there are with door-to-door sales – consumers are not likely to be subject to high pressure selling, if they do not wish to proceed with a sale, they can stop and compare other possibilities. A cooling-off right might place an e-trader at a competitive and cost disadvantage vis-à-vis a local trader where a cooling-off right does not apply.

On the other hand, online shopping is qualitatively different from offline shopping and even from other forms of distance selling like mail order. The speed of transacting can often deny consumers time to appropriately reflect on their intended purchase.

The ADMA Code of Practice[65] provides for a cooling-off period of seven business days from the receipt of goods, or for services, on the date the contract to supply services is made. ADMA members must ensure this right to cancel a contract is specifically mentioned or prominently displayed in contractual documentation.

There are exclusions from the above cooling-off. For example, the cooling off does not apply to contracts for made-to-measure goods or personalised goods, for goods which can be easily copied like books, computer software, videos or compact discs or goods which deteriorate rapidly. As many of the goods Australian consumers have tended to purchase online have been books and CD's, the cooling-off under the ADMA Code would not have applied.

Question 17

Should there be a mandatory cooling-off right in relation to online consumer contracts?

Question 18

If so, how long should the cooling-off be and what exemptions should apply?

[63] The 1998 Children's Online Privacy Protection Act (COPPA).

[64] Section 71 FTA (Vic) operative as of 1 October 2003.

[65] ADMA Code of Practice, section 20 onwards.

7.3.3 Delivery of goods

Section 7.3.1 discussed disclosure of when products purchased online would be delivered. This section discusses specific delivery targets. Delays in delivery of goods ordered and paid for in advance is recognised as a particular issue besetting distance selling including Internet sales.

The BPM does not specify delivery targets in regard to the delivery of goods. It suggests e-traders disclose their own delivery arrangements. By contrast, both the Direct Marketing Model Code of Practice and the ADMA Code of Practice suggest goods be delivered within 30 days. Where this target cannot be met, the trader is to advise the consumer of the reason for the delay and offer the consumer the opportunity to cancel the order and receive a full refund of any money paid.

The UK Distance Selling Regulations also require delivery within 30 days unless the parties have agreed an alternative delivery date. If delivery is not made within 30 days, the consumer has grounds for a refund.

An alternative has been voiced by some consumer groups: that traders not be allowed to debit the consumer's credit card until delivery has been made. Another issue is whether services should be subject to the same regime as delivery of goods.

Question 19

a. Are there potential or existing consumer problems that could be addressed through specific delivery targets?"

b. If so, given a range of self-regulatory or regulatory options, what is the best way to set delivery targets?

7.3.4 Redress

Effective redress has been identified as a fundamental consumer right in the United Nations Guidelines for Consumer Protection. In addition to the courts, consumers in most Australian jurisdictions have recourse to small claims jurisdictions which provide speedy and cost effective redress.

The need for effective dispute resolution mechanisms in e-commerce is noted in the 2001 Treasury Discussion Paper *Dispute Resolution in Electronic Commerce*[66].

Effective redress depends on both legal rights and mechanisms through which to obtain redress. To date, there is significant international uncertainty about which court has jurisdiction to hear a cross-border dispute and which country's law will govern the resolution of a dispute.

The Canadian Consumer Measures Committee (CMC) at the request of Federal, Provincial and Territorial Ministers for Consumer Affairs have produced a useful consultation paper on this issue[67]. The paper notes that there have been a number of international initiatives that have considered the following approaches to consumer contracts:

1. Country-of-destination approach. This allows the consumer always to sue in their home jurisdiction and allows consumers to rely on the protection of their own laws. Consumer advocates have promoted this approach but businesses have expressed concern that they would then have to defend themselves against a multitude of jurisdictions.
2. Country-of-origin approach. Under this approach, jurisdiction rests with the seller. While this approach provides business with a predictable environment, consumer groups contend it provides an incentive for businesses to operate from jurisdictions with lax consumer protection laws ultimately undermining consumer confidence in e-commerce.
3. Prescribed seller approach. This involves businesses being subject to the laws or courts as prescribed in the contract. The difficulty of this approach is that it would allow the seller to dictate the choice of law and forum possibly overriding consumer protection law in the consumer's home country.
4. Targeting approach. This approach assumes that if a vendor specifically targets a purchaser in a particular jurisdiction, then the courts of that jurisdiction should exercise jurisdiction.

[66] The Treasury, Dispute Resolution in Electronic Commerce, October 2001.

[67] Canadian Measures Committee, The Determination of Jurisdiction in Cross-border Business-to-Consumer Transactions, A consultation Paper 2002.

The CMC has proposed the following rules to deal with choice of forum in consumer contracts:

1. In circumstances where:
   - the consumer contract resulted from a solicitation of business in the consumer's jurisdiction by or on behalf of the vendor and the consumer took all necessary steps for the formation of the contract in the consumer's jurisdiction, or
   - the consumer's order was received by the vendor in the consumer's jurisdiction, or
   - the consumer was induced by the vendor to travel to a foreign jurisdiction for the purpose of forming the contract and the consumer's travel was assisted by the vendor,
   - the consumer has the option of proceeding against the vendor in either the consumer or the vendor's jurisdiction.
2. If a vendor took reasonable steps to avoid concluding contracts with consumers in a particular jurisdiction, it is deemed not to have solicited business in that jurisdiction.
3. A vendor may bring proceedings against the consumer only in the courts of the consumer's jurisdiction.
4. The provisions in paragraph 1 may be varied by agreement only if the agreement is entered into before a dispute or it allows proceedings to be brought in courts other than those provided for in paragraph 1.

The following rules have been proposed with regard to choice of law.

1. The parties to a contract may agree that the law of a particular jurisdiction will apply to the consumer contract.
2. No agreement will deprive a consumer of the protection he/she is entitled to provided that:
   - the consumer contract resulted from a solicitation of business in the consumer's jurisdiction by or on behalf of the vendor and the consumer took all necessary steps for the formation of the contract in the consumer's jurisdiction, or
   - the consumer's order was received by the vendor in the consumer's jurisdiction, or
   - the consumer was induced by the vendor to travel to a foreign jurisdiction for the purpose of forming the contract and the consumer's travel was assisted by the vendor.
3. No If there is no agreement as to applicable law, the law of the consumer's jurisdiction shall apply provided that one of the conditions above is met.
4. If the vendor demonstrates that it took steps to avoid concluding contracts with consumers resident in a particular jurisdiction, it is deemed not to have solicited in that jurisdiction.

The European Union has adopted new rules relating to jurisdictional issues in the context of e-commerce. The basic rule set out in the Brussels Regulation is that the defendant shall be sued in the state it is domiciled. However, special rules are provided in the case of consumer contracts. Where an online trader directs activities in the consumer's home state, the consumer is entitled to sue in the consumer's home state unless the consumer chooses to sue in the vendor's state.

The Brussels Regulation has been criticised by business groups that have contended the Regulation will result in online vendors being involved in disputes with countries in which the laws are more onerous. However, the European Parliament and Commission have noted that the mere fact that an Internet site is accessible in a country will not be sufficient for the Regulation to apply.

The Hague Conference on Private International Law is also currently working on a draft convention on jurisdiction and enforcement of judgements in civil and commercial matters. It is understood, however that the current focus of its work is B2B contracts.

In the US, the American Bar Association (ABA) has also made recommendations on jurisdictional issues. In regard to business-to-consumer contracts, it has said that the courts should enforce mandatory, non binding arbitration clauses and that jurisdictional choices should be enforced where the consumer has demonstrably bargained with the seller. It is interesting to note that in response to the ABA report, the Federal Trade Commission (FTC) has said that it is concerned that the proposals would erode consumer protection in the global marketplace[68].

International legal uncertainty together with the need to develop new mechanisms to handle often low cost, cross-border complaints has lead to the development of various online alternative dispute resolution (ADR) facilities.

[68] See Consultation Paper above, page 19.

A comprehensive review of online ADR mechanisms was undertaken by the International Conflict Resolution Centre at the University of Melbourne on behalf of the Victorian Department of Justice[69]. The review, which is part of a broader project focusing on strengthening ADR, comprised a literature review of online ADR including 128 books, articles and online resources; analysis of 76 past and current online ADR sites; an analysis of five illustrative cases and liaison with researches and experts in online ADR.

Notwithstanding the effort both locally and internationally in investigating and promoting the use of online ADR, and the current uncertainty surrounding questions of the applicable fora and law, several questions arise:

Question 20

Where a business specifies an applicable law or jurisdiction to govern a contractual dispute, should it be required to clearly disclose this information "at the earliest possible stage of the consumer's interaction with the business"?[70]

Question 21

Should businesses located in Australia which enter a contract with a resident of Australia be required to spell out which jurisdiction's law will govern the contract and where the dispute will be heard.

Question 22

Going further, would there be any value in providing over-riding statutory recourse to an Australian forum for dispute resolution in a B2C contract involving a foreign retailer?

[69] See the Department of Justice website at: http://www.justice.vic.gov.au/CA256902000FE154/Lookup/Online_ADR/$file/Reseach_ADR_Exploration_Report_03.pdf

[70] BPM section 50.

"Section 8 Options"

8

The previous sections of this paper have looked at the issues and risks that face consumers making online purchases. Some of these like privacy concerns, and to a lesser extent, security of payment issues fall outside the jurisdiction of the Ministerial Council on Consumer Affairs. While the Council may have input into developments in these areas, it cannot set the agenda.

8.1 Status Quo

This envisages retention of the existing regulatory mix of consumer protection law – including enforcement; the voluntary BPM; education and information strategies.

Advantages

Current consumer protection legislation at the Commonwealth, State and Territory level applies equally online as offline. Rigorously enforced, current law is sufficiently robust to address many of the issues that consumers complain about, for example misleading representations and scams.

The TPA and mirror state and territory fair trading legislation have been on the statute books for many years and their general requirements are generally understood. This simplifies administration and compliance costs.

In addition to the existing law, the special aspects of e-commerce have been addressed by the development of best practice standards within the BPM. This incorporates standards on all the matters identified in section 7 of the paper.

In a developing market, it is appropriate to rely on "light-touch" regulation in the first instance. This will enable the market to develop without placing additional regulatory costs on e-traders. Further, where the nature and extent of the consumer detriment is not known, it is inappropriate to introduce new laws.

Disadvantages

Current law, while robust and effective, is essentially negative in that it prohibits unethical and undesirable behaviour but does not impose positive requirements on online traders. Consumers may need a range of additional information (as outlined in section 7.3) to enter the online market and to make informed purchasing choices.

The BPM has been in existence for three years and while its effectiveness has not been formally assessed, available evidence suggests the take up rate has not been significant.

Where the market does not address consumer concerns, it is appropriate for government to act and require adherence to specified standards. This can be criticised as adding to the regulatory burden, however the current approach has not seen online shopping emerge to the extent expected or envisaged. The additional regulation may, in fact, have only a small cost impact on business when overseas jurisdictions have implemented similar regulations. It might also be argued that clarity and certainty would assist the development of the market for online shopping.

Other jurisdictions, particularly the European Union and Canada have determined that governments, and especially ministers responsible for consumer protection need to take a more pro-active approach and have pioneered mandatory disclosure requirements.

Question 23

Is the current mix of regulatory and voluntary measures effective in addressing online consumer protection issues?

8.2 Other non-regulatory measures

8.2.1 Education and information

Consumer affairs agencies currently produce and provide reasonably extensive fact sheets on various e-commerce issues. Newer methods to guide consumers have also been developed, for example Consumer PING[71] and ShopSafe™[72]. These efforts could be increased.

Advantages

Informed consumers know their rights and know what to look for when trading online. They are more likely to be able to assess the risks involved in a particular transaction.

Disadvantages

There is already a plethora of information on online issues available online and offline. The issue is not that there is inadequate information available, but that it does not get to the consumers who need it when they need it.

Question 24

Is there a need for further consumer education and information in regard to online shopping?

Question 25

What type of measures are needed?

8.2.2 Co-ordinated compliance efforts

As noted by the Parliament of Victoria Drugs and Crime Prevention Committee[73], the ease with which fraud transcends domestic and international borders necessitates a high degree of co-operation between law enforcement and regulatory agencies. The OECD

> *Recognising that fraudulent and deceptive commercial practices against consumers undermine the integrity of both domestic and global markets to the detriment of all businesses and consumers, and undermine consumer confidence in those markets, and*
>
> *Recognising that most existing laws and enforcement systems designed to address fraudulent and deceptive commercial practices against consumers were developed at a time when such practices were predominately domestic, and that such laws and systems are therefore not always adequate to address the emerging problem of cross-border fraudulent and deceptive commercial practices, and*
>
> *Recognising that, despite differing national systems and laws for the protection of consumers, a consensus exists on the need for a common framework to enable the further development of close co-operation among consumer protection enforcement agencies, to tackle cross-border fraudulent and deceptive commercial practices* [74],

has recently released Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders. The Guidelines suggest some principles for co-operation and areas where closer co-operation is needed, for example, in regard to information sharing

[71] Consumer PING is a free piece of software designed to assist consumer shopping on the Internet. See http://www.consumerping.gov.au/content/what.asp

[72] See section 7.1.

[73] Parliament of Victoria Drugs and Crime Prevention Committee, op.Cit page 166.

[74] OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders, 11 June 2003, page 7.

The concept of better co-operation and co-ordination in compliance work is unlikely to be countered. The challenge however is to put in place mechanisms to achieve co-operation. For example, consumer affairs agencies operating within Australia currently lack, agreed, formal protocols for handling of cross-jurisdictional complaints and alleged breaches of consumer legislation[75].

Question 26

Are differing national laws and enforcement systems likely to impede the development of effective, co-operative enforcement mechanisms?

8.2.3 Web seals of approval

The Web Seals of Approval Options Paper[76] released by the Working Party on 15 September 2003 looked at the role web seals or trustmarks could play in enhancing consumer confidence in the online world. Web seals are accreditation schemes established to promote good online practices and/or target specific problems perceived to hinder consumer confidence.

Current evidence suggests that within Australia web seal accreditation schemes have not contributed greatly to consumer confidence in online transactions. However, with further action – the Options paper canvasses various options including the development of a guide to web seals and the establishment of a national seal accreditation body similar to the TrustUK scheme, – web seals may provide a non-regulatory means of addressing the range of consumer concerns described in section 7.

8.3 New government regulations

New government regulations are generally only proposed where there is clear market failure and voluntary measures have failed to address the problems adequately.

The online sales market presents several risks for consumers which have been identified in this paper as those relating to payment security, risks to the privacy of personal information and fair trading concerns. Of this group, only fair trading concerns fall squarely within the jurisdiction of MCCA.

There is some evidence that consumers buying online do not get the information necessary to make informed purchasing decisions. Shopping offline, this information would be gauged directly, for example the location of the trader and the cost of the product. Online, this information may be missing or may not be presented in adequate detail.

One option is the development of an Internet Sales template, much along the lines as that developed by Canadian Federal, Provincial and Territorial Ministers responsible for consumer affairs[77]. The Canadian template covers contract formation, cancellation rights, credit card charge-backs and information disclosure.

[75] This issue is being addressed as a matter of priority by the Fair Trading Operations Advisory Committee (FTOAC).

[76] This paper can be at www.consumer.vic.gov.au and www.consumer.gov.au

[77] Internet Sales Contract Harmonisation Template May 2001. http://strategis.gc.ca

A common Australian template might include the following:

Information Disclosure Requirements

Suppliers would be required to disclose:

- their name, and if different, their business or trading name
- their business address (a physical address), telephone number and email address
- all costs, in the applicable currency
- a fair description of the goods or services including any relevant technical or systems specifications
- the terms, conditions and method of payment and any payment security measures exercised by the supplier
- the supplier's delivery arrangements including a delivery date
- the supplier's refund, exchange or cancellation policies
- the supplier's privacy arrangements.

The above information would need to be disclosed in a clear and comprehensive manner. It would also need to be easily accessible from the traders home page.

Cancellation rights would only apply where there was a failure to disclose the required information.

Additional government regulation would have advantages and disadvantages. The disadvantages are immediately apparent and relate to additional costs that would be imposed on e-traders and the cost and difficulty of enforcing any new law particularly beyond Australian borders[78]

The benefits are not so readily quantifiable. However, an information disclosure regime may lead to greater certainty about transactions thereby increasing consumer confidence in online transactions.

Question 27

Would there be any benefit in developing an Australian Internet sales template?

[78] In regard to enforcing rules beyond Australia's borders, it is interesting to note that while Australian consumers have in the past purchased more goods from overseas sites (mainly American sites selling CD's, DVD's books etc), more traffic is now being directed at domestic sites. See, for example www.nua.ie/surveys/index.cgi?f=VS&art_id=905357694&rel=true
"Hitwise executive director Adrian Giles said the gap between Australian and international sites was closing, with more than 61% of all traffic heading to local sites during December (2000)."
Hitwise December 2000 study quoted in B&T Marketing Media http://www.bandt.com.au/articles/fc/0c0032fc.asp
E-tailing: Christmas crunch time at http://brw.com.au/stories/20001124/8036.htm

Section 9
Conclusions and next steps

9

As noted by Zoë Baird[79], in the early years of Internet development, the prevailing view was that government should stay out of Internet governance and that self-regulation and market forces would suffice to create order and enforce standards of behaviour. However, as the Internet has become more an integral part of peoples' lives, there has arguably been some shift to government regulation to deal with issues such as spam, and online pornography.

E-commerce consumer protection has thus far relied on existing consumer protection legislation and the voluntary BPM.

The aim of this paper has been to identify issues which impact on consumers who buy goods or services online and to consider whether all these issues are being adequately addressed with the existing regulatory framework.

Readers are encouraged to respond to the questions and issues raised in this paper.

[79] Zoë Baird Governing the Internet Engaging Government, Business, and Nonprofits, in Foreign Affairs November/December 2002, vol 81, No 6. Zoe Baird is President of the Markle Foundation.

Notes

Notes

Notes

Consumer Affairs Victoria
Consumer Helpline
1300 55 81 81 (local call charge)
Website www.consumer.vic.gov.au

May 2004
eC-13-01