

Security and Privacy in E-consumer Protection in Victoria, Australia

Huong Ha

► **To cite this version:**

Huong Ha. Security and Privacy in E-consumer Protection in Victoria, Australia. Ian Wakeman; Ehud Gudes; Christian Damsgaard Jensen; Jason Crampton. 5th International Conference on Trust Management (TM), Jun 2011, Copenhagen, Denmark. Springer, IFIP Advances in Information and Communication Technology, AICT-358, pp.240-252, 2011, Trust Management V. <10.1007/978-3-642-22200-9_19>. <hal-01568680>

HAL Id: hal-01568680

<https://hal.inria.fr/hal-01568680>

Submitted on 25 Jul 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Security and Privacy in E-consumer Protection in Victoria, Australia

Huong Ha

University of Newcastle, Singapore
artp6075singapore@yahoo.com

Abstract. *Governments in many countries have actively promoted both regulatory and self-regulatory approaches to govern e-commerce and to protect e-consumers. Nevertheless, the desired outcomes of e-consumer protection have not fully materialised. Although there are many research projects about e-commerce, security, privacy, trust, etc., few relate to e-consumer protection. In addition, most projects on e-consumer protection only focus on individual issues, rather than examining the entire coverage of the protection of e-consumers. This paper, a theoretical one, aims to fill these gaps by (i) identifying five issues in e-consumer protection, (ii) discussing the current regulatory and non-regulatory framework of e-consumer protection, (iii) examining the effectiveness of this current framework, and (iv) proposing how this framework can be improved to address current and future problems. This paper will use Victoria, Australia as a case study and takes into account the view of all stakeholders.*

Key words: *E-consumer, e-consumer protection, e-retailing, jurisdiction, privacy, security, redress, regulation, self-regulation*

1. Introduction

It is no doubt that e-commerce has generated several benefits to e-users, and it is still a popular platform for commercial transactions in the next few years. The volume of e-transactions is expected to reach over US\$71 billion by 2012 [1]. However, e-commerce also raises many problems for e-users and the operations of the e-market, especially consumer protection [2]. This paper has identified five issues relating to the protection of consumers in the online market (or e-consumer protection), which are the barriers for the development of e-commerce. They are (i) information disclosure and verification, (ii) security, (iii) jurisdiction, (iv) redress, and (v) privacy.

To address these issues, the Australian government has implemented a mixture of approaches, including government regulation and guidelines, self-regulation by industry, professional associations and businesses. However, the effectiveness of the current regulatory framework of e-consumer protection has not been adequately assessed. In addition, the self-regulatory approach has not worked for e-consumers. The number of consumer complaints about online purchases and payment has steadily increased [3]. Although many works and research have attempted to address issues in e-consumer protection, most of them only focus on individual issues. Also, there is insufficient academic work analysing the current state of e-consumer protection and

assessing the effectiveness of the current e-consumer protection in Australia. Thus, this paper aims to (i) identify five issues in e-consumer protection, (ii) examine the current regulatory and non-regulatory framework of e-consumer protection, (iii) evaluate this current framework, using Victoria (Australia) as a case study, and (iv) recommend how e-consumer protection can be enhanced.

Overall, although this is a theoretical paper, it will contribute to identify positive and negative impacts of the current regulatory framework on e-consumer protection. This paper is important as protecting e-consumers means protecting e-businesses which, in turn, can improve the online global market. It will also trigger further research on how to protect global e-consumers more effectively.

2. Five Issues in E-consumer Protection

Due to the differences between the offline and online market places, consumers have to face more risks when shopping online. Apart from the common issues faced in traditional forms of commerce, e-consumers have to deal with the five issues relating to e-transactions, namely (i) information disclosure, (ii) security, (iii) jurisdiction, (iv) redress, and (v) privacy. These issues are important and interdependent. Although no issue is more critical than others, this paper focuses on two main issues, security and privacy, given the nature of the online market and e-consumer protection.

Information Disclosure and Verification

In the online market place, e-consumers are disadvantageous as they have to provide all information required via the Internet, while they do not know about e-retailers. E-consumers have to make decision with limited or asymmetric information. Thus, information about the registration status and the location where e-retailers register their business must be displayed on their website [4]. E-consumers must also know the description about goods/services as they will purchase based on the description of goods/services provided on websites. Without sufficient and precise information, e-customers are unable to make informed decisions [5]. In addition, information about transaction processes, refund, exchange, delivery, etc. must also be available to e-consumers as they have to pay in advance and have to make decision without having a chance to negotiate with e-retailers. All terms and conditions must be presented precisely and simply to help e-consumers to make their best choices [6].

Security

Security embraces two issues: data and payment security. Data security refers to the protection of personal identity and information (contact number, income, etc.). Personal information and identity may be collected for many purposes or even for committing crimes [7] [8]. Online payment is a special feature of e-retailing. To enjoy the convenience of shopping online, buyers have to pay mainly by credit cards. Global e-consumers have been increasingly concerned about the misuse of credit card information and the theft of credit card details. In Australia, the security of online payment is one of the main reasons discouraging consumers to shop online [9]. Charge back is another sub-issue. Many e-customers do not know how to collect the

refund or the amount of money wrongly charged by e-retailers if e-retailers ignore their requests [10].

Jurisdiction

Consumers encounter higher level of risks relating to security, privacy, fraudulence, and scam when they are online. It is more difficult to address these cyber misdeeds due to different legal frameworks from different countries. Consumers face two key issues when they buy from sellers locating in different jurisdictions: (i) which regulation they should follow, and (ii) which government bodies will resolve any subsequent dispute [11]. Since cross-border trade involves in many countries, jurisdiction concern needs to be addressed at multilateral levels of government.

Redress

E-consumers will not shop online if there is no redress mechanism available [12]. This kind of fear grows bigger in the online market when the transactions are done across nations. Ironically, many customers may find it too troublesome to ask for a refund or an exchange when the quality of goods/services is not acceptable or products purchased are not delivered. Customers are often afraid that costs spent for redress may be higher than the amount of compensation [13]. In the offline market, many options are available to consumers when they need to seek compensation for defective goods purchased [14]. Nevertheless, traditional ways of resolving disputes may not be applicable in the global e-market. For example, consumers may not be able to return products purchased to e-retailers due to the distance and cost involved. Therefore, addressing redress concern may contribute to facilitate online transactions.

Privacy

E-consumers are very concerned about misuse of personal details via illegal collection and dissemination of such information [15] [16]. To worse this situation, many e-traders in Australia do not publish privacy policies on their websites [17]. There are two main privacy concerns: (i) e-consumers' personal particulars and their credit card details will be used by unauthorised persons or by authorised persons without their consent or knowledge; and (ii) their e-mail address and correspondence will be unlawfully accessed and used for unknown purposes [18]. Paradoxically, some customers do not hesitate giving their particulars to e-retailers or promoters in exchange for some economic gain such as discount or cheaper purchases.

3. The Current Regulatory and Non-regulatory Framework of E-consumer Protection

Consumer protection aims to protect the benefits of consumers in commercial transactions [19]. Since online transactions are cross-border, the protection of consumer must be exercised at three levels: international, national and state levels.

International and National Initiatives to Protect E-consumers

Electronic transactions have obtained the same status as other forms of transactions as they have been legally recognized by the *Model Law on Electronic Commerce*

enacted by the United Nations Commission on International Trade Law, the *Commonwealth Electronic Transactions Act 1999* and the *Victorian Electronic Transactions Act 2000* [20]. Hence, e-consumers must receive equal protection as consumers in traditional markets [21].

The United Nations General Assembly adopted the principles of consumer protection in 1985 [22]. These guidelines provide the direction for member countries to develop, strengthen and modify the legal framework and policies related to e-consumer protection in their countries. The UN guidelines also seek strong cooperation among all stakeholders to develop a healthy global online market. This resolution consists of six general principles and seven guidelines aiming to achieve the above objectives. Nonetheless, this set of guidelines is applicable for consumer protection in general, not particular for e-consumers.

The 1999 *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* aim to (i) promote a conducive online environment for all players to increase cross-border trade; (ii) provide direction for countries to align their e-consumer protection policies with international laws and practices; (iii) call for self-regulation by and active participation from all stakeholders; and (iv) call for equal protection of consumers in both the online and offline markets [23] [24]. The *OECD guidelines* suggest eight principles of consumer protection in B2C e-commerce.

The Australian government has addressed the issues arisen in e-commerce by introducing the national guidelines, “*Building Consumer Sovereignty in Electronic Commerce: a Best Practice Model for Business*” (the BPM) [25] which complements the five principles of consumer protection discussed in *Policy Framework for Consumer Protection in Electronic Commerce (1999)*. This BPM aims to enhance consumer sovereignty by encouraging stakeholders to adopt a self-regulatory approach and to exercise their social responsibility to protect consumers. The BPM does not apply to overseas traders and neither does it include e-auction [26].

These three sets of guidelines share a common element of calling for voluntary compliance and self-reviewing of national consumer protection policies [27].

Current Measures to Protect E-consumers in Victoria, Australia

This section examines the current regulatory and non-regulatory framework to address five issues in consumer protection in e-retailing in Victoria, Australia.

Information Disclosure and Verification

In Australia, information disclosure and fair trading in both offline and online markets are regulated by the *Trade Practices Act 1974* (TPA 1974) which aims to protect the welfare of all stakeholders nationally [28]. Under the TPA 1974, businesses must avoid misleading advertising, fraudulence and other unfair and dishonest practices such as unauthorized billing or selling faulty products [29] [30].

Consumer protection is highlighted in Part V of the TPA 1974. Although the TPA 1974 originally aims to protect consumers and promote fair trade practices in traditional commerce, many of its provisions in Part V can be applied in e-commerce [31]. The TPA 1974 can only partially address the issues relating to information disclosure. Besides, the TPA 1974 does not cover all types of companies and all businesses in Australia [32]. Another source of legislation is acts enacted by states

and territories, such as the *Victorian Fair Trading Act 1999*, *South Australian Fair Trading Act 1987*, *New South Wales Fair Trading Act 1987*, and others.

Security

Addressing security concern to counteract cyber threats and vulnerabilities can positively affect the global economic growth [33]. This task requires strong cooperation and collaboration among all sectors and among nations. At national level, security concern is addressed by both the public and the private sectors.

The Commonwealth government introduces several measures to ensure confidentiality, integrity and availability in the online environment [34]. The first measure is the enactment of legislations relating to security. These legislations include the *Commonwealth Cybercrime Act 2001* (amended in 2004), the *Australian Security Intelligence Organisation Act 1979*, the *Crimes Act 1914*, the *Criminal Code Act 1995* and the *Telecommunications (Interception) Act 1979*. These Acts aim to prevent potential cyber attacks of security systems of businesses and government agencies. According to the *Cyber Crime Act 2001*, some individuals and agents may be exempted from this Act [35]. The *Security Legislation Amendment (Terrorism) Act 2002* deals with potential attacks by terrorists via the cyberspace [36]. Nevertheless, there is an absence of initiatives of states in the combat against cyber-crimes. For example, Victoria does not pass any legislation relating to security or identity theft.

The Australian government also works closely with industry to set up “a Business-Government Task Force on Critical Infrastructure” which oversees problems associated with cyber-security [37]. The National Information Infrastructure (2000) was introduced to promote the cooperation of all stakeholders and create a reliable online environment [38]. Launched in April 2003, the Trusted Information Sharing Network for Critical Infrastructure Protection engages an “all-hazards” approach to tackle current and potential vulnerabilities [39]. *OnSecure* website (2003) by the government offers a convenient and secure platform for inter-departmental use. The public can also access its public site at www.onsecure.gov.au to obtain information about e-security threats [40]. The private sector exercises social responsibility by introducing more inclusive hi-tech solutions. These solutions range from e-cash, e-certificates, to e-signatures which enable customers to protect their details in e-purchases. Bio-technology is also explored to enhance data and payment security [41]. Surprisingly, Victoria does not enact specific legislation relating to security. There is no record of the participation of consumer associations in e-security projects.

Jurisdiction

So far, jurisdiction concern has not been received sufficient attention at the international and national levels. The *TPA 1974* and the *Victoria Fair Trading (Amendment) Act 2003* mainly apply to businesses registered in Australia. Even the *OECD Guidelines* and the Australia BPM only emphasize on self-regulation by businesses and industry. Only the Free Trade Agreements (FTAs) between Australia and Singapore, Australia and Thailand as well as Australia and USA state clearly the responsibility of each party in the protection of e-consumers [42]. Most FTAs do not specify any mechanisms or collaboration to address problems relating to e-transactions. Although these FTAs acknowledge the importance of consumer laws

and policies of counterpart countries in the facilitation of international trade, they do not really demonstrate how jurisdiction concern can be tackled.

Redress

The dispute resolution framework in Australia includes three stages: (i) settlement between e-customers and e-retailers, (ii) settlement via a third party, and (iii) settlement via an independent Ombudsman or going to court.

If customers are not happy with the online purchase, they can directly complain to e-retailers who will address problems via their internal dispute resolution processes. However, many customers find it difficult to settle the matter with e-retailers from different jurisdictions [43]. They may not pursue the case if it is too time consuming.

If the problems are not solved at the first stage, e-consumers can employ Alternative Dispute Resolution schemes (ADRs) or Online Dispute Resolutions (ODRs) by external parties [44]. ADRs/ODRs can provide users with cheap, expedient and effective solutions and help to avoid jurisdiction problems [45]. The Australian Competition and Consumer Commission (ACCC) [46] provides e-consumers and e-retailers with dispute resolutions before these parties have to involve in litigation. The Australian National Alternative Dispute Resolution Advisory Council [47], a government-linked agency, also helps users to manage commercial disputes. At state level, Consumer Affairs Victoria [48] also provides ADR schemes. In some instance, these government agencies will refer unresolved cases to the ACCC or the Australian Securities and Investments Commission for investigation and settlement [49]. Some popular organisations offer industry-based dispute resolution schemes are the Telecommunications Industry Ombudsman, the Australian Direct Marketing Association (ADMA) and the Internet Industry Association (IIA). Schemes offered by international consumer associations are mainly online. Consumer International, an international consumer association, helps consumers to “exercise their rights and responsibilities” in dispute resolution [50]. Other international online ODR services are *Sentinel*, the American Better Business Bureau, CyberSettle, SquareTrade, etc. [51].

Finally, if consumers do not satisfy with the outcome of an ADR procedure, they can approach an independent Ombudsman to help their cases resolved or they can seek legal action through the Small Claim courts or other courts [52].

Privacy

In Australia, personal privacy is protected based on two main mechanisms, namely (i) common laws, and (ii) self-regulatory approach by firms and industries [53].

Common Laws. The *Commonwealth Privacy Act 1988* applies to the public sector, and the *Privacy Amendment (Private Sector) Act 2000* covers the rest in the handle of personal information [54] [55]. These acts require that personal data must be collected, used and stored confidentially. Recipients must be informed about the purposes of the collection of their personal data. The *Spam Act 2003* states that sending of “unsolicited commercial electronic messages” [56] with an Australian link and using “address-harvesting software” (spyware) is prohibited [57]. However, many government agencies, registered political parties, religious organisations, small businesses (revenue of less than \$3 million), the media, etc. are excluded from its

coverage [58]. Finally, only Australian citizens and permanent residents are protected under these Acts [59]. Another privacy act is the Commonwealth *Telecommunications Act* which specifies the responsibilities of service providers in terms of the usage and the disclosure of customers' personal information [60]. Victoria only passed the *Information Privacy Act* in 2000 which regulates the handling of personal information, but excluding "personal health information", in the public sector [61].

Self-regulation. Currently, there are two industry associations that introduce voluntary codes of practice dealing with spam. They are the ADMA and the IIA. The ADMA also appoints an independent Code Authority to monitor the compliance of its members with the code of practice [62]. Both sets of code of practice mainly apply to their members and code subscribers (if any), though non-members can adopt these codes. Other initiatives from the private sector include services relating to audits of privacy policies and privacy seals [63]. The audits ensure that private enterprises adhere to their own privacy policies.

4. The Effectiveness of the Current Regulatory and Non-regulatory Framework in E-consumer Protection

Facts and Figures

Internationally, 64% of the respondents will not shop online [64]. In another global survey, 42% of the respondents received spam e-mails which accounted for more than 50% of their e-mails [65]. In Australia, 3,317 complaints relating to e-transactions were lodged with the ACCC in 2001 and 2002. 19.17% of these were complaints about online issues such as deceptive advertising, guarantee and refund [66] [67]. Until June 2003, 2,899 similar complaints, accounted for 5.4% of total complaints, were recorded [68]. The amount of money lost due to online fraud was AU\$980 million with 806,000 victims in 2007 in Australia [69]. The loss due to online scams was A\$839,365 in 2008, and A\$544,694 in 2009 [70]. Also, "Internet shopping trustmarks in 2005" was assessed as "little effectiveness" by Australia [71].

In Victoria, 183 e-commerce complaints were handled by Consumer Affairs Victoria in 2002. This figure indicated an increase of 45.24% of complaints compared to year 2001. 41% of these complaints were related to e-sales; 35% were related to "domain name services", and 24% of the complaints were about "Internet Service Providers" [72]. In the survey in May 2003 by Consumer Affairs Victoria, only 4% of 380 Australian trader websites posted information about procedures to handle complaints [73]. It should be noted that the statistics are not updated as only 25% of fraud cases was reported to policy or the respective authorities or agencies [74].

What Works and What Does Not Work?

The findings indicate that government acts and regulations do not cover all aspects of e-consumer protection. For example, many individuals and organisations are excluded from the *Cyber Crime Act 2001* and others. Such individuals and organisations may

take advantage of the legal loophole for their personal gain. In addition, guidelines and code of practice are not mandatory and must be back up by government regulation. However, states heavily rely on national legislation and guidelines for e-consumer protection as there is inadequate government regulation at the state level. Besides, there is insufficient involvement and coordination among stakeholders. For instance, in Victoria, few activities relating to e-consumer protection by civil society have been recorded. The private sector also provides limited contribution to address issues concerning security and privacy.

E-consumers would purchase online if they trust e-retailers. Trust is one of the business strategies of reputable e-retailers to retain existing customers and to attract new customers. Thus, self-regulation by e-retailers would strengthen the trade relationship between e-consumers and e-retailers. Nevertheless, the degree of employing self-regulatory approaches varies from one e-retailer to another, either in the same industry or in different industry. This causes confusion to e-consumers, and makes it difficult for the respective government agencies to monitor.

Generally, limited effectiveness has been achieved in e-consumer protection. Consumers can obtain fair treatment in business transactions when they can get sufficient and precise information about products and services, about e-retailers and about all terms and conditions. In the offline market, customers can get such information by various channels. However, the overloaded or underloaded information on the Internet make it difficult for customers to make good decisions [75]. Trans-national online incidents diminish consumer confidence in the e-market, directing consumers to decide that they must only have business relationships with well-known, local vendors [76]. Therefore, consumers will engage in online shopping only when they are ensured that they will be well protected and when the potential gain from online shopping will exceed the level of risks they have to face.

5. Recommendations to Improve E-consumer Protection

The above discussion suggests that special conditions are required to ensure the level of consumer protection in the online environment the same as in the offline market. While many legislative provisions and regulatory frameworks have been implemented to address consumer protection in traditional commerce, very few have demonstrated their effectiveness and efficiency in the protection of e-consumers. Besides, the current policy framework does not really adhere to the *OECD Guidelines* and the five Australian principles of consumer protection in e-commerce. Thus, recommendations to improve e-consumer protection are discussed as follows.

Firstly, government regulations and acts should cover as much as possible all aspects of e-consumer protections. The online marketplace evolves rapidly, and thus enforcement of regulations must be frequently monitored, and regulations must be revised to respond to changes and meet the needs of e-consumers in the online environment. Also, projects aiming to enhance e-consumer protection should focus on both macro and micro levels as online incidents will affect both e-consumers and e-retailers, and the whole industry. Importantly, governments must ensure that consumers in both traditional and online marketplaces receive equal protection [77].

Secondly, the online marketplace is cross-border and cross-jurisdiction. It is impossible for any single individual or agency, either in the public or private sector, to provide e-consumer protection without cross-support and external assistance. Hence, international and national collaboration is required to enable all stakeholders to share information about online incidents and how to deal with such incidents.

Finally, it is not feasible for governments to police the website of each and every e-retailer to ensure that regulations and policies are complied with. In addition, e-consumers would carry out transactions with e-retailers who can provide good quality of products and services, with reasonable price and flexible terms and conditions. In other words, e-consumers will deal with only trustworthy e-retailers. Therefore, adoption of both regulatory and self-regulatory measures may help e-retailers to retain existing e-customers and to attract new e-customers.

6. Conclusion

In brief, due to the cross-border nature and the speed of e-transactions, e-consumers have to face five additional issues when shopping online, namely (i) information disclosure and verification, (ii) security, (iii) jurisdiction, (iv) redress, and (v) privacy. These issues are interdependence and important to the development of the online market. However, security and privacy are more pertinent to e-consumer protection.

This paper has discussed the current regulatory and non-regulatory framework to protect e-consumers in Victoria, Australia. There are strengths and weaknesses in this framework and its implementation. There is also no empirical evidence whether this current framework is still valid, given the rapid development of the e-market and whether e-consumers are aware of what kind of protection which national and local governments can provide them and whether they are confidence in such protection. Thus, there is a need for further research on e-consumer protection. Further and systematic researches on consumer protection in e-retailing from the standpoint of e-consumers will certainly facilitate the advance of a theoretical framework and practical approaches to solve stagnant problems in e-consumer protection.

Acknowledgment. The author would like to thank Associate Professor Ken Coghill (Department of Management, Monash University) and Dr. Ann Maharaj (Department of Econometrics and Business Statistics, Monash University) for their academic guidance and great support in many aspects to complete her PhD thesis successfully.

References

1. eCommerce Report, <http://www.ecommercereport.com.au/?p=183> (2011)
2. Fairfax Media, <http://www.bordermail.com.au/blogs/national-comment/online-shopping-vs-bricks-and-mortar/2012288.aspx?storypage=2> (2011)
3. Ha, H.: E-security and the Roles of the Police in E-consumer Protection - Australia Case. The 2nd Istanbul Conference on Democracy and Global Security, 14-16 June, Turkey (2007)
4. The Expert Group on Electronic Commerce, http://www.ecommerce.treasury.gov.au/bpmreview/content/DiscussionPaper/01_Summary.asp (2003)

5. Quo, S.: Spam: Private and Legislative Responses to Unsolicited Electronic Mail in Australia and the United States. *ELaw - Murchdoch University*, vol. 11(1), p. 45 (2004)
6. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
7. Grabosky, P., Smith, R. G., Dempsey, G.: *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press, Cambridge, New York (2001)
8. Identity Theft Resource Center, http://www.idtheftcenter.org/artman2/uploads/1/ITRaC_News_Q4_2009.pdf (2009)
9. Ha, H., Coghill, K., Maharaj, E. A.: Policy Framework for Protection of E-consumers' Privacy in Australia. In Chen, K. C., Fadlalla, A. (eds) *Online Consumer Protection: Theories of Human Relativism*, pp. 123--150. Idea Group, Inc. (2008)
10. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
11. Burns, E., <http://www.clickz.com/stats/sectors/email/article.php/3571381> (2005)
12. Endeshaw, A.: The Law Vis-A-Vis Electronic Commerce. In: Rahman S. M. and Rasinghani, M. S. (eds.) *Electronic Commerce: Opportunity and Challenges*. Idea Group Publishing, Hershey and London (2000)
13. Consumer Affairs Division: *Dispute Resolution in Electronic Commerce*. Commonwealth of Australia, The Department of Treasury, Canberra (2001)
14. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
15. Moghe, V.: Privacy Management - a New Era in the Australian Business Environment. *Information Management & Computer Security*, vol. 11(2), pp. 60--66 (2003)
16. Internet Society, http://www.isoc.org/internet/issues/docs/privacy-survey_2010.pdf (2010)
17. Consumer Affairs Victoria: *Online Shopping and Consumer Protection*. Standing Committee of Officials of Consumer Affairs - E-commerce Working Party, Victoria (2004)
18. Jackson, M.: Internet Privacy. *Telecommunications Journal of Australia*, vol. 53 (No. 2, Winter 2003), pp. 21--31 (2003)
19. Quirk, P., Forder, J.: *Electronic Commerce and The Law*, 2nd ed. John Wiley & Sons Australia, Ltd., Queensland (2003)
20. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
21. The Expert Group on Electronic Commerce, http://www.ecommerce.treasury.gov.au/bpmreview/content/DiscussionPaper/01_Summary.asp (2003)
22. The United Nations Department of Economic and Social Affairs (DESA): *Guidelines for Consumer Protection*. In Resolution 39/248: The United Nations (1985)
23. OECD: *Policy Brief: Electronic Commerce*. OECD, Paris (2001)
24. Smith, R., Budd, C.: *Consumer fraud in Australia: costs, rates and awareness of the risks in 2008*. Australian Institute of Criminology, Australia (2009)
25. Hockey, J.: *Building Consumer Sovereignty in Electronic Commerce: A best practice model for business*. Commonwealth of Australia, Canberra (2000)
26. Hockey, J.: *A Policy Framework for Consumer Protection in Electronic Commerce*. Commonwealth of Australia, Canberra (1999)
27. Harland, D.: The Consumer in the Globalised Information Society. The Impact of the International Organisations. *Australian Competition and Consumer Law Journal*, vol. 7, p. 23 (1999)
28. Martin, J.: The Roles of the ACCC in Protecting Competition and Fair Dealing. In: Murray Hume Business Enterprise Centre, 2 September 2004, Albury-Wodonga (2004)

29. Graeme, S.: 30 Years of Protecting Consumers and Promoting Competition. Keeping Good Companies, Vol. 57 (No. 1, Feb 2005), p. 38041 (2005)
30. Horvitz, R., <http://www.slideshare.net/tomwinfrey/ecommerce-framework> (2002)
31. Attorney-General's Department (Australia): *Trade Practices Act 1974*. Volume 1 ed. (2005)
32. Productivity Commission: Australian and New Zealand Competition and Consumer Protection Regimes. Australian Government, Productivity Commission, Canberra (2004)
33. Ford, P.: Implementing a 'Culture of Security' in Australia. Attorney-General's Department, Deputy Secretary Criminal Justice and Security, Canberra (2003)
34. Department of Communications, Information Technology and the Arts, <http://www.dcita.gov.au/ie/e-security> (2005a)
35. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
36. Ford, P.: Implementing a 'Culture of Security' in Australia. Attorney-General's Department, Deputy Secretary Criminal Justice and Security, Canberra (2003)
37. Directorate for Science Technology and Industry, and Committee for Information Computer and Communications Policy, <http://www.oecd.org/dataoecd/16/27/35884541.pdf> (2004)
38. Department of Communications, Information Technology and the Arts, http://www.dcita.gov.au/ie/e-security?SQ_DESIGN_NAME=printer_friendly (2005b)
39. Ford, P.: Implementing a 'Culture of Security' in Australia, p. 2. Attorney-General's Department, Deputy Secretary Criminal Justice and Security, Canberra (2003)
40. Hill, R., Ruddock, P., <http://www.agimo.gov.au/media/2003/12/2936.html> (2005)
41. Directorate for Science, Technology and Industry Committee on Consumer Policy: Report on Consumer Protections for Payment Cardholders. OECD, Paris (2002)
42. Australian Competition and Consumer Commission, <http://www.accc.gov.au/content/index.phtml/itemId/563794> (undated)
43. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
44. Schellekens, M., Van Der Wees, L.: ADR and ODR in Electronic Commerce. In: Prins J. E. J., Ribbers, P. M. A., Van Tilborg, H. C. A., Veth, A. F. L., Van Der Wees, J. G. L. (eds.) Trust in Electronic Commerce. The Role of Trust Form a Legal, an Organizational and a Technical Point of View. Kluwer Law International, The Hagues/London/New York (2002)
45. Tyler, M. C., Bretherton, D.: Country Experiences of ODR: Australia - A Report of Research Conducted for the Department of Justice, Victoria, Australia. In: The UNECE Forum on ODR (2003)
46. Australian Competition and Consumer Commission: Role and Activities, <http://www.accc.gov.au/content/index.phtml/itemId/54137/fromItemId/3744> (2005)
47. National Alternative Dispute Resolution Advisory Council, http://www.nadrac.gov.au/www/nadrac/nadrac.nsf/Page/About_NADRAC (2007)
48. Consumer Affairs Victoria: Victoria Leads the Way in Consumer Protection. Consumer Affairs Victoria, Melbourne (2005).
49. Neave, C. N., Pinnock, J.: Setting the Scene Industry-based Customer Dispute Resolution Schemes. In: "ADR - A better way to do business" conference, 4-5 Sep, Sydney (2003)
50. Consumers International: Annual Report 2004, p. 1. Consumer International, London (2004)
51. Consumer Affairs Division: Dispute Resolution in Electronic Commerce. Commonwealth of Australia, The Department of Treasury, Canberra (2001)
52. Neave, C. N., Pinnock, J.: Setting the Scene Industry-based Customer Dispute Resolution Schemes. In: "ADR - A better way to do business" conference, 4-5 Sep, Sydney (2003)
53. Moulinos, K., Iliadis, J., Tsoumas, V.: Towards Secure Sealing of Privacy Policies. Information Management & Computer Security, vol. 12 (4), pp. 350--361 (2004)

54. Jackson, M.: Internet Privacy. *Telecommunications Journal of Australia*, vol. 53 (No. 2, Winter 2003), pp. 21--31 (2003)
55. Curtis, K.: Privacy in Practice. In: the workshop at Centre for Continuing Legal Education, University of NSW, 9 March 2005, Sydney (2005)
56. Quo, S.: Spam: Private and Legislative Responses to Unsolicited Electronic Mail in Australia and the United States. *ELaw - Murchdoch University*, vol. 11 (No. 1), p. 4 (2004)
57. *Spam Act 2003*. Act No. 129 of 2003 as amended. 12 Dec 2003 - 10 Apr 2004, p. 35 (2004)
58. Jackson, M.: Internet Privacy. *Telecommunications Journal of Australia*, vol. 53 (No. 2, Winter 2003), pp. 21--31 (2003)
59. Vasiu, L., Warren, M., Mackay, D.: Personal Information Privacy Issues in B2C E-Commerce: a Theoretical Framework. *COLLECTeR* (2002)
60. Ha, H.: "Three-Sector Governance System" Model to Address Fives Issues of Consumer Protection in B2C E-commerce in Victoria, Australia. In: 19th ANZAM Conference, 7 - 10 Dec 2005, Canberra (2005)
61. Moghe, V.: Privacy Management - a New Era in the Australian Business Environment. *Information Management & Computer Security*, vol. 11(2), p. 61 (2003)
62. Quo, S.: Spam: Private and Legislative Responses to Unsolicited Electronic Mail in Australia and the United States. *ELaw - Murchdoch University*, vol. 11 (1), p. 45 (2004)
63. Egger, F. N.: Consumer Trust in E-Commerce: From Psychology to Interaction Design. In: Prins J. E. J., Ribbers, P. M. A., van Tilborg, H. C. A., Veth, A. F. L., van der Wees, J. G. L. (eds.) *Trust in Electronic Commerce. The Role of Trust form a Legal, an Organizational and a Technical Point of View*. pp. 11--43, Kluwer Law International, The Hagues/London/New York (2002)
64. PC Magazine: The Perils of Online Shopping. *PC Magazine*, 23 Aug 2005, p. 23 (2005)
65. Consumers International: Annual Report 2004. Consumer International, London (2004)
66. Lundy, K., <http://www.katelundy.com.au/October2002.htm#23October2002> (2005)
67. Consumer Affairs Victoria: Online Shopping and Consumer Protection, p. 4. Standing Committee of Officials of Consumer Affairs - E-commerce Working Party, Victoria (2004)
68. Consumer Affairs Victoria: Online Shopping and Consumer Protection. Standing Committee of Officials of Consumer Affairs - E-commerce Working Party, Victoria (2004)
69. Australian Bureau of Statistics: Nearly \$1 billion dollars lost by Australians to personal fraud. Australian Bureau of Statistics, Canberra (2008)
70. Dearden, J., [www.aic.gov.au/events/aic%20up coming%20events/2009/acft.aspx](http://www.aic.gov.au/events/aic%20up%20coming%20events/2009/acft.aspx) (2009)
71. Office of Fair Trading (UK), www.oft.gov.uk/shared_oftr/reports/consumer_protection/oft921.pdf (2007)
72. Consumer Affairs Victoria: Online Shopping and Consumer Protection, p. 14. Standing Committee of Officials of Consumer Affairs - E-commerce Working Party, Victoria (2004)
73. Wentworth, E., [http://www.nadrac.gov.au/www/nadrac/rwpattach.nsf/VAP/\(3A6790B96C927794AF1031D9395C5C20\)~ADR+-+A+Better+Way+to+do+Business+-+September+2003\(2\).PDF/\\$file/ADR+-+A+Better+Way+to+do+Business+-+September+2003\(2\).PDF](http://www.nadrac.gov.au/www/nadrac/rwpattach.nsf/VAP/(3A6790B96C927794AF1031D9395C5C20)~ADR+-+A+Better+Way+to+do+Business+-+September+2003(2).PDF/$file/ADR+-+A+Better+Way+to+do+Business+-+September+2003(2).PDF)
74. Smith, R., Budd, C.: Consumer fraud in Australia: costs, rates and awareness of the risks in 2008. Australian Institute of Criminology, Australia (2009)
75. Glenn, J. C., Gordon, T. J.: 2005 State of the Future, p. 2. American Council for the United Nations University, Washington, D. C. (2005)
76. Majoras, D. P., Swindle, O., Leary, T. B., Harbour, P. J., Leibowitz, J.: The US SAFE WEB Act: Protecting Consumers from Spam, Spyware, and Fraud. A Legislative Recommendation to Congress. Federal Trade Commission, USA (2005)
77. Ruddock, P., [hhttp://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_First_Quarter_31_January_2006_-_Australian_Law_Reform_Commission_to_review_Privacy_Act_-_0062006#](http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_First_Quarter_31_January_2006_-_Australian_Law_Reform_Commission_to_review_Privacy_Act_-_0062006#) (2006)