December 2002

Are Business Websites Complying with Government Privacy Legislation?

Carol Alcock
Faculty of Informatics, University of Wollongong

Lois Burgess
Faculty of Informatics, University of Wollongong

Joan Cooper
Faculty of Informatics, University of Wollongong

Nicole Watt
Faculty of Informatics, University of Wollongong

15th Bled Electronic Commerce Conference
eReality: Constructing the eEconomy
Bled, Slovenia, June 17 - 19, 2002

Are Business Websites Complying with Government Privacy Legislation?

Nicole Watt

Faculty of Informatics, University of Wollongong
Australia
Nlw08@uow.edu.au

Joan Cooper

Faculty of Informatics, University of Wollongong
Australia
Joan@uow.edu.au

Lois Burgess

Faculty of Informatics, University of Wollongong
Australia
Lois_Burgess@uow.edu.au

Carol Alcock

Faculty of Informatics, University of Wollongong
Australia
Carole_Alcock@uow.edu.au

Abstract

2001 was a key year for privacy in Australia. In December 2001 new privacy legislation came into existence for both the public and private sector. This legislation changes how organisations handle their information management. This study reports on a survey of 70 Australian Business websites from August to September 2001. The purpose of the survey was to determine what percentage of

the businesses had a privacy policy and where a policy was evident it was analysed to determine to what extent it complied with the new privacy legislation guidelines.

1. Introduction

The objective of this research was to determine whether Australian business websites are providing adequate levels of privacy protection in line with the recently implemented (21 December 2001) Privacy Amendment (Private Sector) 2000 Act [20]. The research provides evidence of areas of deficiencies in the privacy protection which organisations offer online. It also establishes what can be done to increase privacy protection to comply with current Australian Privacy Legislation.

The following areas were explored in this study.

- The Australian government requirements in relation to online privacy.
- The discrepancies between new legislation, the Privacy Amendment (private sector) 2000 Act [20], and on-line business privacy policies.

Determination of what businesses need to do to address the Privacy Legislation.

2. Information Privacy

An issue of continuing concern among consumers using the Internet is that of privacy of information. However, what might be considered "private" may vary from consumer to consumer. Private information has been defined as "those facts, communications or opinions which relate to an individual and which would be reasonable to expect him to regard as intimate or confidential and therefore want to withhold or restrict their circulation" [11]. This statement reflects the primary issue of information privacy: control. Schoeman [25] reinforces this notion by categorising the fundamental elements of privacy to include autonomy, particularly dealing with control over intimacies of personal identity. This is also suggested by Clarke [4] who regards information privacy as being the interest that an individual has in controlling or influencing, the handling of data about themselves.

E-commerce or electronic commerce is the online exchange of goods, services and money between firms and their customers [26]. May [14] describes E-commerce as encompassing a "wide array of interconnected business concepts, technologies and cultural phenomena". With the advent of e-commerce, many opportunities are now available to businesses: transcending geographic boundaries, being open 24 hours and expanded profiling and marketing capabilities [22]. This last opportunity is one that also creates a dilemma: to deliver to your customer, you need to know and understand your customer. However, the customer may not be willing to provide businesses with information they wish to keep private for fear it may be misused.

An immense amount of data is being collected in a consumer's day to day life, not only from browsing on the Internet, but from credit cards, mobile phones and frequent buyer programmes such as "fly buys" [7]. It is interesting to note that "traditional bricks and mortar" retailers have been exploiting personal information for years, for example, every time a credit card is used [23]. The mild response to such instances is in sharp contrast to the sensitivity of similar actions over the Internet. It could be the case that as more individual activities from various aspects of life are linked in some way to the Internet, more data may be linked through sophisticated data mining techniques. In its beginnings, the Internet allowed a certain level of anonymity. With the development of new technologies, this is no longer the case. As a result, individuals feel increasingly susceptible to privacy invasion, which can include not knowing that personal boundaries are being intruded upon.

Until recently, in Australia there was no enforced privacy legislative protection covering the private sector. The value of the new Privacy Amendment (Private Sector) 2000 Act [20] in this regard is yet to be tested.

3. Legislation

The Australian government has been under pressure for some years to reform existing privacy legislation. Previous legislation applied mainly to the public sector. The extension of this legislation to the private sector was seen as an essential next step and new legislation was passed and came into effect in December 2001.

Initial moves to the establishment of privacy legislation in Australia comprised of implementing the OECD guidelines for protection of privacy and trans-border flows of personal data. In 1988, the Privacy Act was introduced. This gave effect to the OECD agreement, and also included obligations under article 17 of the International Covenant on Civil and Political Rights. [21]. The main points of the old legislation are as follows:

1. Commonwealth government departments are bound to observing detailed standards, known as the information privacy principles regarding the handling of information;
2. Credit providers are bound to comply with the provisions concerning consumer credit information in part 111A of the privacy act; and
3. All those who handle tax file numbers are bound to observe the standards known as the tax file number guidelines [12].

What was a concern to the consumer was the fact that the private sector was omitted from these provisions. It is also clear that at the time of the act E-Commerce was not even thought of as an information sensitive medium. Consumer's needs in the current information society were not met by this act. Additionally, under this act there was no protection and so concern from consumers and consumer groups put pressure on the Australian government for reform.

4. The Privacy Amendment (private sector) 2000 Act

The public's privacy concerns prompted the Federal Government to introduce new privacy legislation, which was enforced on December 21st 2001. As noted by the Attorney General [9], this legislation establishes the minimum standards for the protection and handling of personal information in the private sector. The act has been described as a "light touch". At its core is the co-regulatory ideal, being that business can develop their own policy within the sanctions defined in the legislation. [9].

The privacy amendment, as noted by the Attorney General requires that web site operators who collect information, take actions to ensure Internet users know who is collecting their data and how it is stored. Sites are also required to gain consent to collect and use information. The legislation allows people access to their own records and provision for correction. In addition, web site operators are required to comply with a specified level of encryption technology. As well, their policy on privacy must be available [8]. These requirements are a huge step forward on what was previously in existence, but whether they will meet the publics' privacy needs is another matter.

At the root of the legislation is a set of privacy principles. According to the Privacy Commissioner, organisations can have their own codes. However, these codes must comply with the National Privacy Principles and be approved by the privacy commissioner Malcom Crompton [17].

The privacy principles include:

- NPP1: Collection
- NPP2: Use and disclosure
- NPP3: Data Quality
- NPP4: Data security
- NPP5: Openness
- NPP6: Access and correction
- NPP7: Identifiers
- NPP8: Anonymity
- NPP9: Transborder data flows
- NPP10: Sensitive information

5. Methodology

The central tenet of this study is to find the gap between government expectations from the new Privacy Legislation and evidence of the implementation of privacy policy on business web sites. The results are drawn from a service quality gap

analysis. What is used is the purpose and philosophy of the GAPs model in measuring service level, using privacy protection as the service attribute. This is an effective measure for determining the level of privacy protection a site is providing and hence, whether it meets Government legislation. The notion of a gap in service is the difference between customer expectations and perceptions of actual service provided by a business [3]. Privacy has been identified as an important dimension of e-service quality [28].

An analysis of the new government legislation produced a list of key expectations for privacy. A series of questions was developed from these key expectations. Seventy commercial web sites, determined from an established list compiled in a report by SAS, "Australian e-business web sites" in October 2000 [24] were then surveyed using these questions. This list of businesses primarily deals with business to consumer sites and is divided into 14 categories: shopping, business and finance, employment, freight and couriers, news and media, travel, automotive, computers and Internet, search engines and directories, utilities, telecommunications, lifestyle, entertainment and government. Gereralisability was obtained by using a sample of sites from each of these industries, covering a broad spectrum of E-Commerce applications

The web site survey was undertaken in the following manner

- Web site selection
- Locate the privacy policy or any other privacy information on the site. Print a copy of the policy. Analyse the policy and test with the web site survey.
- Review corresponding policy with site collection activities.

A statistical analysis on how many web sites met each of the criteria was then undertaken.

6. Results and Discussion

The results indicate how many sites meet each level of privacy criteria and their depth of coverage.

Table 1 contains a list of the different industry sectors surveyed. Table 2 details the different services offered by the 70 sites.

Industry	Portion
Automotive	6%
Banks	4%
Insurance	4%
Computer & Internet	8%
Department Stores	7%
Employment	6%
Entertainment	7%
Flowers & Gifts	4%
Food & Wine	7%
Health	6%
News and media	6%
Search & Directories	6%
Shopping:misc	6%
Telecommunications	6%
Travel	7%
Flight	4%
Utilities & Services	7%

Table 1: *Profile of Sites Surveyed*

Service Offered	% of sites with Service	No. of Sites with Service
Purchasing	54%	38
Register/member	71%	50
Purchasing & Registration	39%	27
Online booking	7%	5
Subscription	10%	7
Email/News	41%	9
Request for info/feedback	36%	25

Table 2: *Services Offered*

A privacy policy is pivotal to providing privacy protection. Just over 64% of the 70 sites had a privacy policy, yet a recent survey showed that over 55% of Australians trust a site if it has a privacy policy [19]. Another 14% of the sites displayed some form of privacy disclaimer and the remaining 21% of sites had no privacy information at all. Of those sites with a policy, 84% were accessible from the home page.

6.1 Legislation Compliance

Table 3 contains the summary statistics from the survey in relation to the privacy criteria that are required by the new legislation. As can be seen, few sites are reaching the required level of compliance. Alarmingly, only one site gave an indication as to what will happen to the data after it is no longer required for the purpose for which it was collected or if the company dissolves.

Government Expectation	Of sites with a policy	Of all sites
NPP1: The organisations identity is known	100%	100%
NPP1: A person can gain access to information	38%	24%
NPP1: The purpose is known of collection	91%	59%
NPP1: Consequences are known if information is not submitted?	0%	0%
NPP2: Choice in how information used	20%	13%
NPP3: Data quality information?	7%	4%
NPP4: Data security information?	73%	47%
NPP4: Data destroyed or de-identified when used?	4%	3%
NPP5: Can you make inquiries on privacy?	64%	41%
NPP6: Can amend/correct records?	38%	24%
NPP7: The use of identifiers	6%	6%
NPP8: Anonymity should be provided if applicable	3%	3%
NPP9: The use of information in overseas transactions	0%	0%
NPP10: Sensitive information is collected	0%	0%

Table 3: *Legislation Particulars*

6.2 Policy Changes

The question arises as to what will happen to data previously collected, when a policy is replaced. Is there an option to remove information when data use policies change? Of the 64% of sites with a privacy policy, 38% indicted that policies may change and only 4% allowed "opting out" (Table 4).

Particular on changing policy	%	No.
Policy mentions there could be a change of policy	38%	17
Policy mentions you can opt out of the new policy	4%	2

Table 4: *Policy Changes*

6.3 Privacy Inquiries

Two important issues for consumers are being able to opt out of an email list and being able to make enquires on privacy issues. Just over half of the sites are offering these services with:

- 60% of sites with a policy mentioning that you can remove yourself from email lists; and
- 64% of sites with a policy mentioning you can make inquiries on privacy.

6.4 The Law

Only 16% of sites mentioned a law in relation to privacy. Of these two of the sites privacy policies consisted of a statement that they were getting ready for the new amendment in December 2001.

The other privacy laws mentioned were those determined by the Privacy Alliance, the 1988 Privacy Act, the Fair Information Principles and the OECD stance on privacy

6.5 Privacy Policy

A privacy policy is a simple and effective means to gain a consumer's trust [19]. A policy is a statement, which on December 21st 2001 was legally binding. A privacy policy's content should contain as a minimum the information that is collected from a customer, how the information is used and how the information is stored [21]. The Content of a policy can very: the more information conveyed to the consumer, the more expectations that are met, the higher quality the policy. Including details such as security, access to personal data, or how to remain anonymous are few of the marks of a higher quality policy.

Because a privacy policy is the prime deliverable in conveying privacy information, many Australian's expect a privacy policy. When testing this expectation in the web site survey, just over half (64%) of sites surveyed had a privacy policy. Upon analysis of the policies, it was found that the quality of the policies varied. The policy quality being determinable by how it conformed to the new Privacy Legislation.

A previous web site survey on privacy was undertaken by Andersen Legal in Australia [1] in 2000. This survey was a replicated methodology of a survey performed in the US by the American Federal Trade commission. The results found that 51% of Australian sites had an established privacy policy [1]. The firm also performed a follow up survey in 2001, in which 66% of sites were shown to have a privacy policy. [27]. The results of the Andersen research are close to the findings determined from this study in which 64% of sites had a policy. The findings of this research, however, have determined that the quality of policies vary among sites.

Even if a "privacy policy" is present it does not necessarily mean that all the privacy requirements of the legislation have been satisfied.

Quality aside, over time there have been improvements in the number of privacy policies. The results of this research (64% of sites with a privacy policy) when contrasted with previous Australian surveys show an improvement on what was found in a 1999 survey by Freehill, Hollingdale and Page [18]. That survey found that only 12% of sites had a privacy notice on their web site.

The comparative surveys from Andersen, Freehill, Hollingdale and Page [18] and this study have different methodologies and different objectives but it is beneficial to look at the trends. The use of privacy notices is increasing, but only 64% of sites providing a policy is not enough to meet the new legislation. The majority (90%) of Australians feel that it is an invasion of privacy if Internet activity is monitored without their knowledge [19]. The issue of a lack of policy is important as this survey focused on the branded, well-frequented, advertised web sites.

The results of the web site survey showed that some 14% of organisations tried to cover themselves in regards to privacy notification with a simple privacy disclaimer. A privacy disclaimer can be a simple statement either hidden in the web pages, in the fine print in the terms and conditions or within a site FAQ. In the case of a disclaimer the credibility of the statement is doubtful and privacy provisions are not satisfied. Disclaimers are often difficult to find or the wording must be carefully analysed. For example the following statement is the only information relating to privacy on the Chaos Music.com.au web page. "At Chaos Music we protect our customer's privacy. None of the information given by any visitor at this site will be sold, bartered or given to any third party without prior consent." Chaosmusic.com.au offers online purchasing and collects personal information. A similar example is at E-Store, whose disclaimer reads "No information given by any visitor or customer at this site will be sold to any third party".

These attempts at privacy statements (not policies) are not ample from a legal perspective. In regards to a disclaimer or terms and conditions, if a consumer agrees to them (unwittingly or not) or that they are on the site somewhere, this does not mean the consumer would be satisfied. One sentence does not tell the customer what information is collected not where it goes, which is the main function of a policy [19].

The quality of policy is an important aspect to consider. The policy is the first point for a customer in determining all their privacy rights and the source where privacy expectation should be met. A privacy policy should available on every site, it should be clearly identifiable to the consumer and with links to it if possible on each page.

6.6 Government Expectations and the Gap

On December 21st of 2001 when the Privacy Amendment (private sector) became enforceable, many businesses did not feel they would be ready in time and thought

that the provisions were too strict. [5]. The following is an analyses of the gap between businesses on-lines readiness to comply with the Privacy Act, as gained from the survey in August 2001, and what the government determines as good privacy and "light touch" legislation. Some of the particulars of the legislation pertaining to the privacy implementation could not be ascertained. These included the back end systems and management of privacy requirements. Those areas of legislation, which cannot be determined, have not been considered in the analysis of the gap.

Table 5 portrays the privacy gap in relation to government legislation. The Government perspective is taken from the National Privacy Principles guidelines September 2001. This was tested against the business implementation as determined from the web site survey.

Table 5: *Government Privacy Gap*

Expect ion	Business Implemen tion	Gap & Recomn ndations
A person must be told the collecting orgnisation's name and contact details NPP1	In 100% of sites the company identity was obvious. 100% of sites had some form of contact detail, either phone, address or email.	This particular was being serviced. At the time of collection the organisational identity was obvious, with contact details.
A person must be told they can gain access to personal information NPP1	Of the 64% of sites surveyed a minority (38%) of sites mentioned in their policy the ability to access their information and update it if applicable.	There was a large gap in meeting expectation by December. Few sites gave details at the time or after the collection. More sites need to consider having this information in a policy or a statement at time of the collection
A person must be told the purpose for collecting the information. NPP1	91% of sites with a policy stated a purpose of information collection, this was 59% of all sites These were generalised categories, no specifics. Of those sites, which gave a purpose, 78% mentioned it was for service, 24% for Marketing, 15% for personalisation, and 27% for statistics. Of the 64% of sites with a privacy policy less than half of these sites (38%) mentioned that there could be a possible change in policy and that the policy should be regularly checked. 4% of sites with a policy mentioned that you could opt out of any new use of information.	The NPP Guidelines expect that an organisation would keep the description of the purposes reasonably general as long as the description is adequate to ensure that the individual is aware of what the organisation is going to do with information about them. In this case the reasons were too generalised and no specific use was made clear. Companies need to be more coherent in purpose and outline it in the policy. A statement also needs to be made as to what happens to already collected data if the purpose of data use changes.
A person must be advised who data is shared with. NPP1	47% of sites with a policy would not share information what so ever. (30% of all sites) 11% of sites with a policy would share information, 38% of sites with a policy would share with consent the remaining 4% made no statement. For non-identifying information, only 38% of those with privacy policies admitted collecting information. Of those sites that do share information, 11% gave indication of whom they shared with.	The aim of NPP 1.5 is to ensure that an individual knows what happens to information about them regardless of whether the information is collected directly or indirectly. More information needs to be given as to what "with consent means" and how consent is given Specifics of how data is shared needs to be identified.

Expect ion	Business Implemen tion	Gap & Recomn ndations
A person must be advised the consequences of if submitting information if it is not complete NPP1	0% of sites gave any indication to this type of information	This could have legal implications or service implications so this needs to be laid out clearly in the policy This is especially important for financial or health related sites. The NPP recommendations states "An example of such a statement might be 'if you don't tell us this, we won't be able to process your application'"(privacy.gov.au, 2001)
If information is not collected directly, e.g by cookie. NPP1 needs to be satisfied. NPP1	89% of sites used cookie technology. 9% of sites had cookies generated from an advertisement on their site. A cookie was found on the machine from 63% of sites, Of the 64% of sites with a policy 76% mentioned cookies and 24% mentioned Add Server Cookies This results to 55% of sites that use cookies giving some notice. Of the 64% of sites with a policy only 60% gave indication of other methods of data collection (39% total). Of these 60% the breakdown was as follows IP Address- 42%, Date/time - 36%, Pages accessed- 38%, Referring page- 24%, Domain- 18%, Email- 2%, Browser type- 13%, OS- 4.00	This unknown collection needs to be explained. The technology needs to be identified and explained to the user. What kind of information is collected, why it is needed and if it is identifiable?
Opportunities must be provided for individuals to opt out of some uses of information NPP2	In relation to the check boxes 9% of sites had options for sharing details with others. 17% of these had permission defaulted on yes. 26% of sites surveyed had a check box for receiving marketing communication 20% of sites with a policy, 13% of all sites, mentioned options.	Opt out boxes when submitting information. Opt out available at a later date. Detailed in the privacy policy.
Data must be accurate, complete and up to date. NPP3	7% of sites mentioned this factor	A large discrepancy in expectation and implementation This practice needs to be reviewed by organisations.
Data should be destroyed if the purpose is completed NPP4	Only 4% of the 64% of sites with a privacy policy mentioned this.	This use should be identified.
On Request an organisation should be able to inform an individual what data is held, the purpose and use NPP5.	To help consumers in their understanding of privacy 64% of sites with a policy, 41% mentioned you could make inquiries on privacy.	With just under half (41%) of sites having this requirement there was still a significant gap Provide email, phone number or address with timely response.
Availability of Access and Correction of personal information NPP6.	Of the 64% of sites with a policy only 38% provided this facility. That equates to 24% of all sites.	The gap was large. An online service would be the most convenient, but if unfeasible then a staffed contact no.
Identifiers assigned by others can not be used/ disclosed NNP7	6% of sites required identifiers. Either a tax file, medicare card or drivers license.	Assign your own organisational identifier. Monitor what information is asked for from a web site so this provision is not abused.

Expect ion	Business Implemen tion	Gap & Recomn ndations
Anonymity should be used by organisations where it is appropriate to do so. NPP8	Only 3% of sites offered the ability to use a service without identification	Improvements in technology may well provide new options in this area. In establishing or updating information systems, organisations should first examine whether a person's identity is necessary for the operation of the system.
Transborder data flow NPP9	0% mentioned this	Use overseas should be outlined.
No Use of sensitive information NPP10	No sensitive information was collected without consent.	Policy should have some explanation as to what is sensitive information

The expectations of the government were determined from the Privacy Amendment Act 2000. The main provisions of compliance determined by the 10 privacy principles. An organisation must obey these principles and develop a privacy code or policy based on these principles, which has the approval of the Privacy Commissioner. In implementation of the web site privacy survey, the factors of the Privacy Principles were anticipated in the site as well as the government's privacy recommendations.

7. Conclusion

The results show that many particulars of the legislation such as access and correction, openness and disclosure are not being serviced. Many sites were nowhere near meeting the new Legislation, the 36% of sites with no policy the prime offenders. In the conduction of the survey only two sites mentioned that they were getting ready for the new privacy legislation. At that time, that was the only privacy information that they displayed. As can be seen from the results of the survey, work needs to be done in information handling practices until compliance with government legislation is achieved. Post December 21 will be a testing time for businesses, the results form this research gave the perspective the many would not be ready.

The survey identified the privacy compliance gap to be quite prevalent. The main deficiencies included: not enough sites posting a quality privacy policy (64%); opt in provisions not being serviced; consent not clearly explained; or direct and collection technologies not clearly identified. Not enough information was provided on consumer rights, not enough control was allocated over personal data, and there was no chance to be anonymous and no quality of information.

A minority of sites allowed viewing and correction of personal data. (38% of sites with a policy). There is no evidence of NPP9, transborder data flow or NPP8, anonymity being served, with only 3% of sites offering the opportunity to be anonymous. There were no adequate details on information handling practices and NPP3: Data quality was not being met, with only 3% concerned over quality.

This research has identified a major deficiency in compliance with the new Australian Privacy Legislation and as Australian's regard privacy as the most important service attribute [19] this lack of compliance can have a major impact upon the acceptance of E Commerce by consumers [21].

In acknowledging the importance of the new Privacy Amendment Act, a longitudinal study is proposed. A repeat of the web site survey, one year later, will determine if the majority of businesses are complying with the legislation.

References

1. Andersen Legal, 2000, Internet Privacy Survey 2000, Andersen Legal.
2. Anonymous, 2001, *Australia: we're 'adequate'*, Privacy Journal, vol.27, no.7 pg. 4
3. Broadley, R. 2001, *Integrating Gap Analysis and utility theory in service research*, Journal of Service Research, vol.3, no.4 pp300-309
4. Clarke, R. 1997, *Introduction to Dataveillance and Information privacy, and definitions of terms, available online:* http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html
5. Dearne, K. 2001, *Firms push privacy delay*, Australian IT, 28 August 2001
6. Denton, T, 2001, *Warning on privacy changes*, The Australian IT, 31 July 2001, available online http://www.theaustralianit.com.au
7. Ghosh, A. 2001, Security and Privacy for E Business, John Wiley and Sons, Canada
8. Internet Industry Association, 2001, *A summary of the new privacy Amendment (private sector) Act 2001*, document ver 1.1, 12 Jan 2001, ACT
9. Internet Industry Association, 2001, *IIA Privacy Code to Tackle EU Compliance*, http://www.iia.net.au/news/000404.html
10. Internet Industry Association, 2000, *Time for the Industry to lift it's game on privacy*, IIA press release 2000, http://www.iia.net.au/news/001003.html
11. Introna & Pouloudi, 1999, *Privacy in the information age: stakeholders, interests and values*, Journal of business ethics, vol.22, no.1, pp27-38
12. Kelly, P. 1995, *Information Privacy and data protection Laws*, in: IT Security Conference, Canberra 1995.
13. Le Roux, G. 2001, *Privacy: The Next Big Thing?*, CommsWorld, Feb 2001
14. May, P. 2000, The Business of ECOMMERCE, Cambridge University Press, NY.
15. McCallum, R. 2000, *Easier said than done: Privacy friendly business practices on the Internet*, Gilbert and Tobin, available online http://www.gtlaw.com.au/pubs.easiersaidthandone.html

16. McClelland, R. 2000, *New Privacy Protections are a "soft touch"*, Australian Labour party website, available at http://www.alp.org.au/print.tml?link=/media/0400/rmmspab120400.html
17. Nicholas, K. 2001, *Survey finds cavalier approach to privacy*, I.T, available online http://it.mycareer.com.au/breaking.20010410/A35509-1001Apr10.html
18. NUA, 2000, *Freehill, Hollingdale & Page: Ecommerce suffering downunder*, NUA Internet Surveys, available online http://www.nua.com/surveys/f=VS&art_id=905355622&rel=true
19. Privacy.gov.au, Office of the privacy commissioner, 2001. *The results of Research into Community, Business and Government attitudes towards Privacy in Australia*, Available online http://www.privacy.gov.au/research/index.html#1.1
20. Privacy.gov.au, Office of the privacy commissioner, 2001, Privacy Amendment (Private Sector) Act 2000 and guidelines, http://www.privacy.gov.au/news/pab.html#3.2
21. Privacy.gov.au, Office of the privacy commissioner, 2000, Background to the Privacy Act 1988, http://www.privacy.gov.au/act/index.html#2.2
22. Reedy, J., Schullo, S. & Zimmerman, K. 2000, Electronic Marketing, Harcourt USA,
23. Rozwell, C. 2000, *Amazon Apology Foreshadows pricing and privacy standards*, Gartner First Take, October 2000
24. SAS, 2000, Australian e-business websites, October 2000
25. Schoeman, C. 1992, Privacy and Social Freedom, Cambridge University Press, New York.
26. Standing, C, 2000, Internet Commerce Development, Artch House, Norwood MA.
27. ZDNet, 2001, *Privacy becomes a strategic asset*, ZDNET, available online http://www.zdnet.com.au/printerfriendly/index.htm?AT=2000010455-20224899
28. Zeithaml, Parasuraman, & Malhotra, 2000, A Conceptual Framework for understanding e-service quality: Implications for Future research and managerial practice, Marketing Science Institute no. 00-225