RESEARCH ONLINE

University of Wollongong
Research Online

Faculty of Commerce - Papers (Archive)

Faculty of Business

2006

Protecting Consumer Privacy in the Company's Best Interest

Sara Dolnicar
University of Wollongong, sarad@uow.edu.au

Yolanda Jordaan
yolanda@uow.edu.au

Publication Details

This article was originally published as: Dolnicar, S & Jordaan, Y, Protecting Consumer Privacy in a Company's Best Interest, Australasian Marketing Journal, 2006, 14(1), 39-61.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

RESEARCH ONLINE

Protecting Consumer Privacy in the Company's Best Interest

Abstract
The increasing use of consumer databases by companies has led to increased levels of concern among consumers that their personal information may not be in safe hands once divulged to companies. A few studies have shown that consumer concern about information privacy may impact on consumer behaviour in ways directly opposed to the aims of the very marketing campaigns developed to increase sales. Should this indeed be the case, it would be in companies' best interest to make protection of consumer privacy a priority. The aim of this paper is to investigate whether there is potential for such a market-driven mechanism of consumer privacy protection. An empirical survey within the Australian context was conducted to investigate the general level of concern among Australians about information privacy. Furthermore, associations between privacy concern levels and behaviour, as well as prior experiences with information privacy violations are examined. Results indicate that: general privacy concern levels are high; associations exist between privacy concerns and protective behaviour; people tend to protect themselves in active ways, such as requesting the removal of information, rather than in passive ways, such as changing the distribution channel to reduce risk of privacy violation exposure; reactions to violations are typically very emotional and include behavioural intentions to take the matter to court.

Keywords
consumer privacy, Australia, personal information, legislation

Disciplines
Business | Social and Behavioral Sciences

Publication Details
This article was originally published as: Dolnicar, S & Jordaan, Y, Protecting Consumer Privacy in a Company's Best Interest, Australasian Marketing Journal, 2006, 14(1), 39-61.

This journal article is available at Research Online: http://ro.uow.edu.au/commpapers/260

Protecting Consumer Privacy in the Company's Best Interest

AUTHORS (alphabetical):

Sara Dolnicar
University of Wollongong, Australia

Email: sara_dolnicar@uow.edu.au

School of Management & Marketing
marketing research innovation centre (mric)
University of Wollongong
Wollongong, NSW
Australia
2522

Tel. (02) 4221 3862
Fax. (02) 4221 4154

Yolanda Jordaan
University of Pretoria, South Africa and
University of Wollongong, Australia

Email: yolanda.jordaan@up.ac.za

School of Management Sciences
Department of Marketing and Communication Management
University of Pretoria
Pretoria
South Africa
0002

Tel. +2712 4202997
Fax. +2712 3625085

Sara Dolnicar is an Associate Professor in the School of Management & Marketing at the University of Wollongong. She finished her degrees in Psychology and Business Administration at the University of Vienna and the Vienna University of Business Administration, respectively. She was awarded her PhD in Business Administration 1996. Her primary research interests are in strategic marketing, marketing research and market segmentation.

Yolanda Jordaan is an Associate Professor in the Department of Marketing and Communication Management at the University of Pretoria in South Africa. She finished her PhD in Marketing at the same university in 2003. She is very active in the direct marketing industry, facilitating several research and management programmes. Her research interests relate to direct marketing, consumer behaviour, service marketing and information privacy.

Acknowledgement

This project was supported by the Faculty of Commerce Special Initiatives Fund at the University of Wollongong.

Protecting Consumer Privacy in the Company's Best Interest

Executive Summary

Companies are harvesting the many ways of reaching consumers, whether the consumers are pleased about this or not. While this kind of organisational behaviour is aimed at maximising profit, it could well be that increased sensitivity of consumers about the use and misuse of their personal information could backfire, leading to boycotting of companies who do not use personal customer information in compliance with law or their own privacy policies.

A study was conducted to investigate how Australians feel about the use of their personal information by companies, in which way they expose themselves to misuse, and what actions they take to protect themselves. Results indicate that consumer privacy certainly is an issue for Australian consumers in the 21st century. Furthermore, it provides some detailed insights into consumers' feelings towards privacy issues: respondents feel very concerned about the protection of their personal information; concerned respondents will engage in active protective behaviour; many respondents presently engage in Internet shopping behaviour that endangers their data to be misused, but do not actively prevent the use of this medium; most Australians would not hesitate to undertake actions to prevent misuse of their information; and the open-ended responses to a scenario in which their information has been misused elicit highly emotional negative responses.

This information can be used to assure that maximising profits by communication with customers is undertaken in ways which are acceptable to consumers, and thus do no lead to negative emotional responses which could cause long-term loss of customers.

Future work should investigate actual boycotting behaviour as a consequence of information privacy breaches in order to quantify the potential profit-risk to companies that do not handle their customers' information with care.

Protecting Consumer Privacy in the Company's Best Interest

Abstract

The increasing use of consumer databases by companies has led to increased levels of concern among consumers that their personal information may not be in safe hands once divulged to companies. A few studies have shown that consumer concern about information privacy may impact on consumer behaviour in ways directly opposed to the aims of the very marketing campaigns developed to increase sales. Should this indeed be the case, it would be in companies' best interest to make protection of consumer privacy a priority. The aim of this paper is to investigate whether there is potential for such a market-driven mechanism of consumer privacy protection. An empirical survey within the Australian context was conducted to investigate the general level of concern among Australians about information privacy. Furthermore, associations between privacy concern levels and behaviour, as well as prior experiences with information privacy violations are examined. Results indicate that: general privacy concern levels are high; associations exist between privacy concerns and protective behaviour; people tend to protect themselves in active ways, such as requesting the removal of information, rather than in passive ways, such as changing the distribution channel to reduce risk of privacy violation exposure; reactions to violations are typically very emotional and include behavioural intentions to take the matter to court.

Keywords: consumer privacy, Australia, personal information, legislation

Protecting Consumer Privacy in the Company's Best Interest

1 Introduction

Privacy is a multi-faceted concept encompassing a number of specific issues. The term 'privacy' is widely used to refer to a group of related rights that are accepted nationally and internationally. In Australia, privacy is defined as "people's right to the privacy of their own body, private space, privacy of communications and information privacy" (Collier, 1995, p.44). From this definition, one can see that the key aspects of privacy relate to the privacy of the person, the privacy of personal behaviour, the personal right to communicate freely and the right of a person to control information about him/herself.

The rise of the Internet, which permits companies to obtain information about customers more easily than before, has brought much attention to the issue of information privacy. The information revolution, moreover, opens up important public policy issues as companies are increasingly building comprehensive consumer databases and applying sophisticated data-mining techniques to target consumers. The issue of consumer information privacy has attracted a lot of attention from different groups world-wide: academic researchers have mainly focused on exploring privacy concerns; market researchers have focused on quantifying the share of consumer concern about information privacy violations and tracking changes over time; and public policy-makers have reacted with laws and regulations to protect consumers.

Some privacy studies suggest that there may be an association between consumers' privacy concerns and their behaviour. This raises the question why the protection of consumer privacy does not seem to be an issue that lies at the core of all companies' marketing activities. This situation is compelling public policy-makers to develop privacy legislation in an attempt to alleviate consumer concern. The aim of the study is therefore to investigate whether the association between consumers' privacy concerns and behaviour provide support for the notion that companies should become actively involved in consumer privacy protection through the development, implementation and management of proper information handling practices. If the behaviour of concerned consumers differs from those who are not concerned about the security of their personal information, companies can play an active role in the privacy protection process, reducing pressure on public policy makers to protect consumers.

In order to explore the potential of company-motivated consumer privacy protection, several research questions are investigated, using a sample of Australian respondents. The article is structured as follows: First, Australian privacy legislation and prior information privacy work are discussed. Next, the data set, measurement instrument and research methodology are described. Thereafter, before reporting on the results, the level of concern among Australian respondents regarding information privacy issues for single items is discussed, as well as the underlying dimensions of information privacy concerns. The results section reports on the research questions, followed by a discussion of the results and implications for companies.

2 Information privacy: legal and consumer behaviour aspects

2.1 Australian privacy legislation

There is no international consensus regarding the elements of privacy that relate to the collection, maintenance, use, disclosure and processing of personal information. In the last twenty years, 'fair information practices' have become an international standard for privacy. Virtually all privacy laws enacted around the world in recent years are an implementation of fair information practices. What came to be known as 'privacy protection' in the United States, and 'data protection' in Europe is addressed as 'privacy of personal data or information privacy' in Australia (Rotenberg, 2001).

Australia is one country that attempts to limit the use of collected and stored information by both public and private organisations. The first privacy legislation in Australia came into existence in 1988 through the Privacy Act that details information handling practices of Australian Commonwealth (federal) government agencies by regulating the way in which the public sector collect, store, use and disclose personal information (Rotenberg, 2001). In December 2000, the Privacy Amendment (Private Sector) Bill 2000 was passed by the Australian Parliament and became effective on 21 December 2001 (Rotenberg, 2001). For the first year, this Act applied to all health organisations as well as organisations (including not-for-profit) with an annual turnover of more than AUS$3 million. From 21 December 2002 this Act also applies to small businesses with an annual turnover of less than AUS$3 million that trade in personal information (Moghe, 2003).

Australia's Privacy Act sets standards for handling personal information, gives individuals the right to know what information private sector organisations hold about them, as well as a right to correct that information if it is incorrect. To comply with the Privacy Amendment Act 2000, private sector

organisations have to comply with ten national privacy principles (NNPs). These include collection, use and disclosure, data quality, data security, openness, access and correction, identifiers, anonymity, transborder flow of data and sensitive information (Moghe, 2003).

The Australian Government has also acted to combat the increasing problem of spam by passing the Spam Act 2003. The Act came into effect on 10 April 2004 and prohibits the sending of unsolicited commercial electronic messages that contain an Australian link. Electronic messages are defined by the Act to include messages sent by e-mail, instant messaging, Short Message Service (SMS) and Multimedia Message Service (MMS). The Act requires that all commercial electronic messages are sent with the express or inferred consent of the recipient, and that they include accurate information about who authorised the sending of the message and a functional unsubscribe facility. The Act also prohibits the supply, acquisition or use of address-harvesting software for the purpose of sending unsolicited commercial electronic messages (Shannon, 2004).

2.2 Prior work on consumer information privacy concerns

There is ample evidence to suggest that consumers world-wide recognise a problem of lack of information privacy and control over personal information. Consumer attitudes about privacy have been researched in various countries and have been addressed in numerous public opinion surveys. Most international studies indicate that information privacy is an important concern to many consumers. For example, the findings of one study by Nowak and Phelps (1992) show that privacy is an important concern that is affected by the type of practice and the specificity of information. The findings of a study by Wang and Petrison (1993) demonstrate that certain consumers (particularly in the older age groups) are more negative about potential threats to their privacy than others. Several other studies' findings show that consumers who believe they do not have control over their personal information are more concerned about privacy (Culnan, 1993; Sheehan and Hoy, 2000). This has been supported by findings of yet another study indicating that as privacy concerns increase, respondents report that they were less likely to provide personal information to companies (Sheehan and Hoy, 1999). Phelps *et al*. (1994) report that public concern about privacy was high even before increased media coverage in the United States in the mid-1980s, and they argue that the dramatic increases in the frequency of media coverage have little relation to public salience. Loro (1995) contends that rising consumer concerns about privacy are forcing companies to utilise the information in their databases to the benefit of consumers.

Various studies have also investigated cross-cultural differences with regard to consumer privacy. The findings of a comparative study by Petrison and Wang (1995) indicate that Americans express more concern about privacy issues pertaining to solicitations, while British consumers are primarily concerned with informational privacy issues pertaining to the collection and exchange of information. In another comparative study, Maynard and Taylor (1996) concluded that Japanese respondents express a stronger concern about privacy issues than United States respondents do. The IBM/multi-national consumer privacy survey conducted among consumers in the United States, Britain and Germany demonstrated that consumers are moving from passive concerns about how their personal information is used into patterns of 'individual privacy activism', and that high levels of concern about privacy continue (Harris Interactive and Westin, 2000). In a comparison between privacy sensitive segments in South Africa and the United States, findings indicate that the distribution between high-concerned segments and low-concerned segments are almost exactly the same, with a third of respondents in these two countries in the high-concerned segment (Jordaan, 2003).

Recent international research studies have focused on privacy in an online environment. The results of two separate studies indicate that privacy and security concerns are the number one reason why web users are not purchasing over the Internet, in part because they have no confidence that the e-commerce legal environment is secure (Miyazaki and Fernandez, 2000; Udo, 2001; Earp and Baumer, 2003). In a series of three consumer privacy surveys, findings consistently indicate that consumers are willing to provide both online and offline companies with basic information, but are more protective of personal information and are less comfortable sharing more sensitive information (Harris Interactive, 2001a, 2001b, 2001c). Results from another online study indicated that a vast majority of consumers believed that the Internet has made it easier for someone to obtain personal information about them (Graeff and Harmon, 2002). A study by Ha (2004) indicated that online users want highly visible privacy policies telling them precisely how a company will use their personal information. More specific protective behaviour was reported in an online study suggesting that users will cease web site access if too much personal information is requested when registering on the site (Chen and Rea 2004). The results from a recent study demonstrates that the willingness to provide information to web merchants increases as the level of privacy guaranteed by the online privacy statements increase (Meinert *et al*., 2006).

Several studies propose ways to decrease high levels of consumer privacy concern. Nowak and Phelps (1997) suggest strategies and tactics for alleviating consumer privacy concerns, such as informing consumers when information is collected, how it will be used, who will have access to the data, and offering consumers 'opt-out' opportunities. Milne and Boza (1999) have established that companies

can improve consumer trust by managing their personal information better, which reduces concern about privacy. Phelps *et al*. (2000) suggest that privacy concerns can be reduced by providing consumers with more control over the initial gathering and subsequent dissemination of personal information. Some researchers recommend that effective self-regulation and corporate privacy policies may help to make consumers more comfortable to disclose their personal information (Culnan, 2000; Caudill and Murphy, 2000; McCarthy, 2002).

Some research sources that report on consumer privacy come from non-academic citations and/or institutions. One example is the Privacy Segmentation Index (PSI) created in 1995 by Harris Interactive for the American market. The purpose of the PSI is to divide respondents into three privacy-sensitive segments based on their level of privacy concern (ranging from low to high). Respondents' degree of agreement or disagreement with three questions about consumer privacy is used to form three privacy-sensitive segments. The first segment is labeled as 'Privacy Fundamentalists' and groups individuals with very high concern about privacy. The second group (labeled 'Privacy Pragmatists') has a moderate, but balanced concern about privacy. The final group, the 'Privacy Unconcerned', has no real concerns about privacy and has far less anxiety about how other people and companies use information about them (Taylor, 2003).

While international studies show ample evidence of information privacy concerns among consumers, these concerns have not been thoroughly examined in Australia. Some of the academic information privacy work that has been done in Australia mainly focused on information privacy from a legislative perspective (Hewett and Whitaker, 2002) or a business perspective (Moghe, 2003). One recent Australian Direct Marketing Association (ADMA) consumer attitudes study investigated how comfortable Australian consumers are in providing information to companies. Results relating to information privacy indicate that young consumers are more comfortable in providing information to companies, as they are more aware of the benefits this offers in terms of time management and better customer service (Shannon, 2005b). Another Australian study among consumers report that Australians are happy to receive relevant and beneficial direct contact from companies they know and trust, and that they are comfortable with providing a basic level of personal information for marketing purposes to companies they know (Shannon, 2005a). None of the Australian studies investigated privacy-related behaviour or the consequences that companies face when they violate consumers' privacy.

2.3 Prior work relating information privacy concerns with consumer behaviour

From the multitude of studies conducted on information privacy, some suggest that behaviour is associated with information privacy concern. One study investigated direct marketing media used by banks and found that the intention to purchase is positively influenced by respondents' favourable attitude toward the direct marketing media used (Page and Luding 2003). The researchers suggested that companies should refine market segments to cater for individuals who are privacy sensitive. Evans *et al*., (2001) report that individuals who feel strongly towards privacy, attempt to minimise the information held on them and rarely, if ever, provide direct marketers with personal details or request communications from them.

The results from a study by Sheehan and Hoy (1999) show several significant correlations between consumers' online privacy concern and behaviour. Typical protective behaviours include asking for removal from mailing lists, sending flame messages to spammers, voicing concern in newsgroups or communications with friends, complaining to the service provider and/or providing inaccurate or incomplete information. The behaviour most frequently adopted was providing incomplete information when registering for web sites. The message from their research was that the frequency of engaging in protective behaviour increased as the level of privacy concern increased.

A study by Berendt *et al*. (2005) showed interesting results. They argue that while many users have strong opinions on privacy and do state privacy preferences, they are unable to act accordingly. Once they are in an online interaction, they often do not monitor and control their actions sufficiently. They also state that online privacy statements seem to have no impact on behaviour. Unfortunately, because customers do not act according to their preferences, many of them later react with resentment towards the company because of their use (or misuse) of the information. The results of five major consumer privacy surveys conducted in 2001 were reviewed by Turner and Varghese (2002), and they reported a disconnection between consumer preferences and behaviour.

Findings from a study by Earp and Baumer (2003) indicate that consumers are adopting protective behaviour by discriminating about the type of information they are willing to reveal to certain web sites (more willing to reveal gender and age, less willing to reveal identification numbers). More specific protective behaviour was reported in an online study suggesting that users will cease web site access if too much personal information is requested when registering on the site (Chen and Rea, 2004). Their study identified several control behaviours adopted by respondents to protect their privacy. Some of these behaviours include the falsification of personal information to obtain access to certain online

resources, and ignoring or deleting unwanted contact from the company due to concern about unauthorised use of personal information.

A recent study revealed that respondents are more willing to provide contact information as opposed to biographical information, and likewise, biographical rather than financial information (Meinert *et al.*, 2006). This suggests that consumers concerned about disclosing biographical information may opt to forgo providing any information, including contact with the service provider. Furthermore, individuals with prior familiarity with policy statements were more likely to provide information when companies had a strong privacy policy statement, and less likely to provide personal information when a no-policy statement was present.

This section provided an overview of some of the research studies on information privacy and provided direction for our research. The next section addresses the aim of the research.

3 Aim of the research

Despite the multitude of studies conducted on information privacy, there is a lack of available information about Australian consumers and their privacy concerns and behaviour. No Australian study, to our knowledge, has empirically focused on investigating privacy concerns and privacy-related behaviour, as well as the possible consequences that companies face when they violate consumers' privacy. If there is an association between consumers' privacy concerns and unfavourable consumption-related behaviour, companies may realise that it is in their best interest to take action to reduce consumers' privacy concerns. For the purpose of this study, behaviour is classified into two types: active protective behaviour and passive protective behaviour. An example of active protective behaviour is where a consumer calls a company and requests that his/her information be deleted from the database. Passive protective behaviour is when a customer reduces the use of certain purchasing channels because they feel that these channels expose their personal information to security risks. Both kinds of protective behaviour have negative effects on companies' marketing activities. Active protective behaviour includes a loss of information and contact with consumers because they cease contact with the company. The negative effect of passive protective behaviour can be seen in the reduction of the use of distribution channels, which are typically associated with lower cost to companies such as purchasing using the Internet or telephone.

In order to explore the potential of company-motivated consumer privacy protection, the following research questions are investigated, using a sample of Australian respondents: (1) do respondents who

demonstrate higher levels of concern about information privacy issues show more active and passive protective behaviour; (2) are different privacy concern dimensions associated with active and passive protective behaviour; (3) is there a difference between victims and non-victims of privacy invasion in terms of their privacy concern levels, as well as their active and passive protective behaviour; (4) is there a difference between the fundamentalist segment and the other segments (as defined by the USA Privacy Index) with relation to their active and passive protective behaviour; and finally (5) how do consumers describe their reaction to a violation of their consumer privacy.

The scope of the study is not limited to any particular context such as the Internet or direct marketing, but encompasses all areas of consumer transactions that expose personal consumer information to misuse by companies. The focus in this study is on privacy in the commercial rather than the governmental sphere, and mainly addresses the use of consumer data for marketing purposes, excluding other areas of concern such as medical privacy, identity theft, workplace monitoring, intelligence systems, and biometrics.

4 Empirical study

4.1 Measurement instrument

The survey conducted in Australia in May 2005 used the information privacy scale introduced by Jordaan (2003). Jordaan's measurement instrument included 66 questions and consisted of four sections: a 5-point Likert scale measurement containing 45 information privacy concern items; a 4-point Likert scale measurement containing 3 items from the Privacy Segmentation Index; 12 binary 'yes-no' items measuring consumers' behaviours, experiences of privacy invasion and knowledge of specific data practices; and finally, certain basic socio-demographic questions.

Questions 1-45 (Section A) from the above-mentioned instrument, contained the main constructs designed to measure information privacy concerns. Eight main dimensions were included in the survey: data collection; data storage and security; data use; data disclosure and dissemination; solicitation; privacy protection policies; legislation and government protection; and behavioural intentions. Exploratory factor analysis for Questions 1-45 resulted in 25 items loading highly (above 0.50) onto the four factors labeled 'privacy protection' (f1), 'information misuse' (f2), 'solicitation' (f3) and 'government protection' (f4). Reliability results (Nunnally, 1978) indicated the following values for each subscale: privacy protection (f1) = 0.87; information misuse (f2) = 0.86; solicitation (f3) = 0.81;

and government protection (f4) = 0.87. Confirmatory factor analysis was conducted to validate the four-factor solution. The measurement model showed acceptable fit (GFI=0.95, AGFI=0.92, CFI=0.97, and RMSEA=0.06) and subscales showed construct validity through adequate discriminant validity (Average Variance Extracted: 0.72; 0.61; 0.61; 0.53 respectively) and within-method convergent validity (path coefficients ranging from 0.67 to 0.89; significant at $p<0.05$).

Section B from Jordaan's (2003) measurement instrument contained the three questions from the Privacy Segmentation Index. As discussed in the literature review, the Privacy Segmentation Index is a tool used to divide the American public into three privacy-sensitive segments: Fundamentalists (high concern); Pragmatists (medium concern); and Unconcerned (low concern). The distribution of respondents into a segment is based on responses to three statements: (1) consumers have lost all control over how personal information is collected and used by companies; (2) most businesses handle the personal information they collect about consumers in a proper and confidential way; and (3) existing laws and organizational practices provide a reasonable level of protection for consumer privacy.

Section C contained the 12 binary items measuring a combination of consumers' protective behaviour, Internet and direct marketing behaviour, experiences of privacy invasion and knowledge of specific data practices. Section D contained the socio-demographic questions measuring gender, age, ethnic orientation, level of education, employment status and household income.

In addition to the above-mentioned questions used in the South African study, a number of additional items were adapted and/or added for the Australian study. First, a few socio-demographic criteria as, for instance, the education and income variables were adapted to better capture the Australian marketplace. Second, an open-ended question was added asking respondents to state what their reaction would be if a company would misuse the personal information they have given.

A pre-test of the final Australian questionnaire was conducted with 15 respondents to assure that wording of all questions was clear and all answer options were relevant to the Australian context. It also set out to determine the required time to answer all questions, indicating that respondents needed between 17 and 20 minutes to fully complete the questionnaire.

4.2 Data collection

An established Australian permission-based online Internet panel (Pureprofile) was used to conduct the survey which was made available online. Based on an expected completion time of 20 minutes, a response rate of 40 percent was predicted by Pureprofile. Given that the aim was a sample of 1000

respondents, 2500 invitations to participate in the survey were emailed. Respondents received eight dollars for their participation - the standard compensation for Pureprofile panellists for a questionnaire with a completion time of 20 minutes. A total of 1055 respondents fully completed the survey, leading to a final response rate of 42 percent. While the Pureprofile panel is representative of the Australian population based on the Australian Bureau of Statistics census data (Table A in the Appendix shows a comparison of the sample characteristics with the comparative figures from the Australian census carried out in 2001), the sample is not expected to be representative of the Australian population with respect to Internet usage given that all respondents have Internet access. It can therefore be expected that results relating to the use of the Internet will be impacted by the sample (this affects only two behavioural items included in this study). It is expected that the respondents will be more open to, and feel more secure, in using the Internet as they would be when the sample were collected using a different medium. Given the nature of the survey, which included privacy-related behaviour of different kinds, alternative ways of data collection could have led to a similar sample distortion. For example, telephone interviews could have affected the behavioural items regarding telephone usage and mail surveys could have affected the behavioural items regarding mail ordering.

Another potential source of bias could be that one could argue that people who are most concerned about privacy may not participate in these self-selected surveys because of their privacy concerns. This would equally effect all data collection approaches and may cause the results to underreport those consumers who are highly concerned about their privacy.

Biases resulting from this sample can be expected: (1) with regard to the two Internet-related behavioural questions seeing that all respondents actively use the Internet (We therefore discuss the results regarding Internet-related behavioural items in the context of prior work among Internet users); and (2) in the results reported in Tables 1 and 2, which give proportions of respondents agreeing with questionnaire items. The fact that the sample is not precisely matching the census data could have a minor effect on the proportions reported.

4.3 Methodology

For most of the research questions investigated, summated scale values are used rather than individual items. As mentioned above, 25 privacy concern statements represented four privacy concern dimensions. These 25 statements were presented in random order and respondents were instructed to consider each statement from the point of view of a person buying from companies who need their

information before a sale can take place. Respondents indicated their level of privacy concern for each statement using a 5-point Likert scale. The following summated scales values were derived for each respondent based on the known scale properties of the *privacy concern scale*, as discussed in the above measurement instrument section (Jordaan, 2003):

- Overall privacy concern score: sum of all 25 variables included in the privacy scale.
- Privacy protection sub-score (f1): sum of the 9 variables that form the first factor of the privacy scale.
- Information misuse sub-score (f2): sum of the 7 variables that form the second factor of the privacy scale.
- Solicitation sub-score (f3): sum of the 6 variables that form the third factor of the privacy scale.
- Government protection sub-score (f4): sum of the 3 variables that form the fourth factor of the privacy scale.

When constructing summated scores for the items capturing *protective behaviour*, the nature of the items suggests a division into active and passive protective behaviour. Active protective behaviour includes actions such as calling a company and having personal data removed from their database, or contacting the company and requesting not to receive any more advertising material. Passive protective behaviour, however, would entail avoiding to shop through distribution channels that expose personal information to potential misuse. In order to check whether this division (between active and passive) is appropriate, principal components analysis with Varimax rotation was computed. Surprisingly, three factors with Eigenvalues higher than one (1.97, 1.39, 1.38) were extracted accounting for 47 percent of the variance (19 percent explained by the first, 14 percent by the second and 14 by the third factor). The loadings matrix (see Table 1) indicates that the first component includes all active protective behaviour items, whereas components 2 and 3 split the passive protective behaviours into two groups: Internet-related items and shopping behaviour through telephone, catalogues and brochures.

---------- take in Table 1 ----------

Based on the findings shown in Table 1, three separate summated scores were constructed:

- Active protective behaviour score: sum of all 5 active protective behaviour items.

- Passive protective behaviour score (telephone and catalogue): sum of the 3 passive protective behaviour items capturing shopping through the telephone, toll-free-numbers, and catalogues and brochures - negatively coded because of the measurement of risky behaviour.
- Passive protective behaviour score (Internet): sum of the 2 passive protective behaviour items capturing Internet shopping behaviour - negatively coded because of the measurement of risky behaviour.

The results of the descriptive analysis for all the summated scores are provided in Table 2. The empirically observed range covers the possible theoretical range for each sub-scale, indicating that respondents are heterogeneous with regard to both privacy concerns and protective behaviour.

---------- take in Table 2 ----------

Pearson correlation coefficients and the nonparametric Spearman's Rho were computed to investigate Research Questions 1 and 2, proposing that the level of privacy concern is significantly associated with protective behaviour. Both the measures for privacy concerns and protective behaviour are summated scales of metric nature. Analyses of variance and binary logistic regressions were computed to investigate Research Questions 3 and 4, which propose that prior experience with privacy violations, as well as the classification as a Fundamental in the USA Privacy Segmentation Index, will be associated with higher levels of protective behaviour. Analyses of variance were used to assess differences in summated scores, and binary logistic regressions were used to determine the predictive value of socio-demographic and behavioural variables (classifying respondents into victims and non-victims, as well as Fundamentalists and Non-Fundamentalists). Membership was used as the dependent variable and original items were used as independent variables in the model.

As mentioned earlier, the United States Privacy Segmentation Index (PSI) was applied in this study with the aim to identify the 'Fundamentals' among the Australian respondents. It can be expected that consumers with the high level of concern (the so-called Fundamentals) will more frequently display protective behaviour. Australian respondents were therefore classified following the assignment rule for the PSI using the three original items from the measurement instrument (refer to discussion in measurement instrument section). All the Australian respondents who strongly or slightly agreed with the first statement, and strongly disagree or slightly disagree with the second and third statements were

grouped into the Fundamentalist segment. All the other responses were grouped to form the non-Fundamentalist segment.

4.4 Results

Before proceeding to the discussion of the five formulated research questions (which will be based on the summated scores across single items), respondents' answers to the individual privacy concern and behavioural items are provided. This is followed by a description of the general results to give an overview and set the basis for the investigation of the research questions.

Table 3 shows the percentage of respondents that strongly agreed with each of the 25 privacy concern statements.

---------- take in Table 3 ----------

From Table 3, one can see that a very high proportion of Australian respondents strongly agrees that they would request a company to remove their information if they felt it was misused, or in case information were sold to other companies. Sixty-five percent of respondents state that they would refuse to provide any personal information if no reasons are provided by the company on why they are collecting the information. Also worth noting is the strong feelings toward the solicitation practices of companies. Only 3 percent state that they do not mind when they receive telephone calls from companies wanting to sell products and services with only 6 percent being pleased to receive information from companies with whom they have not done business before. It is also clear from the results that very few respondents (3 percent) feel that their information is safe while stored in a company's records. However, the majority has indicated that they will become involved in safety measures with 63 stating that they will support a company's efforts to ensure safety, together with the view that government should assist them in the protection process (61 percent).

With regard to the views about who should take measures to assure that consumer privacy is protected, there appears to be agreement that both companies and the government should take action to prevent violations of consumer privacy. The majority of respondents feel strongly about the fact that companies should have privacy protection policies in place. Seventy-eight percent agree that companies should have privacy protection policies and 74 percent feel that these privacy protection policies should indicate how it will protect personal information. Some consistently high concern levels relate to the

fact that 70 percent of respondents feel uncomfortable when companies share their information with others and 72 percent state that they will request removal of their information if it was sold to third parties.

In sum, it seems that Australians feel concerned about the protection of their personal information and that they see a strong responsibility on the side of companies as well as government, with generally higher agreement levels for organisational measures of protection. The findings reported in Table 3 are in line with the findings from previous international studies, with generally high overall information privacy concerns among consumers (refer to literature section). It also correlates with findings published by the ADMA who report that 92 percent of people believe it is very important that they understand why the company is requesting this information and how it will be used (Shannon, 2005a). The concerns reported in Table 3 are slightly lower than that of the AMDA study, where 74 percent of respondents stated that companies should indicate how they would protect their information, with 70 percent wanting reasons why they should provide companies with their personal information. Furthermore, as mentioned earlier, some of the findings from Table 3 show that only 6 percent of respondents are pleased to receive information from companies with whom they have not done business before, suggesting that consumers prefer to deal with familiar companies. This is again supported by the ADMA study showing that 74 percent of respondents are happy to receive relevant information from companies they know and trust (Shannon, 2005a).

As explained earlier, 12 behaviour-related questions were included in the questionnaire. The responses showing the individual behavioural items are presented in Table 4.

---------- take in Table 4 ----------

As can be seen from Table 4, a total of 88 percent of respondents have engaged in Internet purchases, followed by 84 percent being involved in Internet banking - both risky behaviours in terms of privacy protection. Interestingly, a total of 82 percent state that they have refused to pass on their information to companies in the past, showing their distrusting behaviour. This is supported by the 69 percent of consumers who have actually requested a company to remove their name from the records. Just over half the respondents (56 percent) feel that they have been victims of privacy invasion in the past. The high number of victims (an alarming one in every two people) may signal that although many have privacy concerns, they do not cease engaging in risky behaviour (such as Internet shopping). This may

be because they do not want to stop using this convenient channel, or they have no other option. Less than one third of respondents called a toll-free number, bought a product or service over the telephone or requested companies to provide information on how they protect consumer privacy.

The behaviour reported in this study is in line with the findings from previous international studies showing different activities including risky shopping behaviour (such as Internet shopping), protective behaviour (such as requesting company to remove information) and being victims of privacy invasion. One Australian study reported that 89 percent of people open direct mail, with 48 percent taking action to purchase provided they knew the company (Shannon, 2005a). The findings from our study moved in the same direction, showing that 61 percent of respondents confirmed that they have bought something from a catalogue or brochure, confirming that direct mail is still a viable communication and/or shopping channel.

4.4.1 Research question 1: Do respondents who demonstrate higher levels of concern about information privacy issues show more active and passive protective behaviour?

Both the Pearson correlation coefficient and Spearman's Rho value are highly significant for active protective behaviour (p-values < 0.001), indicating that higher levels of privacy concern are associated with higher levels of active protective behaviour (Pearson: 0.160, Spearman: 0.214). The same is true for passive protective behaviour regarding shopping over the telephone, or through catalogues and brochures (Pearson: 0.164, Spearman: 0.149, both p-values < 0.001). These results are plausible, indicating that respondents who are worried about the protection of their personal information, engage in active protective behaviours more, and have higher levels of avoidance regarding telephone or catalogue shopping. One has to note that the descriptive statistics from Table 4 indicate that a total of 61 percent of respondents have purchased from catalogues, giving reason to believe that it is probably the low 18 percent of respondents' telephone shopping behaviour that contributed to this result.

Interestingly, however, this is not the case for Internet-related passive protective behaviour. The Spearman test leads to the conclusion that there is no significant association between privacy concerns and Internet usage at all. The Pearson correlation coefficient even shows a negative association (-0.090, p-value < 0.01). It appears from this analysis that the use of Internet banking and shopping through the Internet may be less affected by consumers' privacy concerns, than other forms of risky shopping behaviour. Of course, this could in part be due to the sample bias towards Internet users, as discussed

earlier. Another possible reason for this could, however, be that the use of certain services, such as Internet banking, is more difficult to substitute because of a significant increase in time effort and transaction fees to achieve the same end result. Findings from a study by Earp and Baumer (2003) indicate that consumers are more willing to provide personal information to a well-known site (such as one's bank) compared to a lesser-known site. This may explain why Internet banking may be less affected by consumers' privacy concerns, in that most consumers are very familiar with, and have a strong connection with their bank. Banking institutions may instil trust in their customers in that many of them have proper privacy policies in place due to a regulated financial environment. Furthermore, it may be that consumers assume that their financial institution offers some form of legal protection when it comes to financial transactions, creating a sense of privacy protection. Some researchers have mentioned that consumers understand that different types of companies require different levels of personal information, with banks, financial institutions and government departments inherently generating greater consumer trust (Shannon, 2005a). Other studies have also shown that people's willingness to disclose personal information is linked to their familiarity with the company – with consumers being more positive when contacted by companies with whom they already do business (Vidmar and Flaherty, 1985; Wang and Petrison, 1993; Sheehan and Hoy, 1999).

Another possible reason why shopping through the Internet may have no association with privacy concerns, as opposed to shopping using the telephone and/or catalogues and brochures, can be the issue of privacy control. When consumers conduct their shopping through the Internet, it allows them to choose the time of contact, the amount of information provided, and the extent of the interaction – giving a sense of privacy control. Results from a study by Berendt *et al.* (2005) show that given the right circumstances, consumers forget about their privacy concerns and often do not monitor and control their online actions sufficiently. This holds true in particular when the online exchange is entertaining, and appropriate benefits are offered in return for information exchange. It is also likely that consumers are not fully aware of privacy violations that take place in the Internet environment, for example when companies deposit cookies to users' computers when they visit their web sites.

In sum, the findings lead to the conclusion that the Internet is used as a channel, irrespective of consumers' privacy concerns. Whether the reasons be the visibility of privacy policies in this medium, the convenience or entertainment value of the channel, the benefits of online activities that outweigh consumers' privacy concern, or the trust of the online service provider, companies have to take care not to harm the trusting relationship that seems to exist with the Internet as a medium. On the other hand, as privacy concerns increase, so does consumers' active protective behaviour.

While these findings are very interesting and highly relevant for industry which makes increased use of the Internet as a business platform, it is likely that the effects described above are due, in part, to the bias of the sample toward Internet users, and in part to other behavioural reasons discussed above (as found in prior studies). In order to arrive at conclusive findings, a replication study would be required using a telephone or mail sample.

4.4.2 Research question 2: Are different privacy concern dimensions associated with active and passive protective behaviour?

The analysis of association on the four privacy dimensions supports the results from Research question 1. Test results indicate that active protective behaviour is highly significantly associated with all four dimensions of the privacy scale (Pearson: 0.160 for the privacy protection dimension, 0.182 for the information misuse dimension, 0.164 for the solicitation dimension and 0.127 for the government protection dimension; Spearman: 0.187, 0.174, 0.147, 0.129; all p-values < 0.001). These findings suggest that consumers will take action to protect their personal information if they are concerned about any dimension of privacy. These actions can consist of a variety of activities such as requesting companies to remove their personal information, refusing to provide personal information to companies, notifying companies not to send them advertising material and requesting companies to inform them which safety measures are in place. The passive protective behaviour relating to telephone and catalogue shopping is significantly associated (p-value < 0.001) with three of the four dimensions: privacy protection (Pearson: 0.164, Spearman: 0.133); information misuse (Pearson: 0.131, Spearman: 0.121); and government protection (Pearson: 0.192, Spearman: 0.179), but not with solicitation (Pearson: 0.049, Spearman: 0.070). The insignificant 'solicitation' result suggests that the prospecting efforts of companies do not seem to impact on their protective behaviour, probably because consumers have little or no control over companies' solicitation activities. This result may also be due to the fact that some telemarketing and catalogue companies do not offer alternative shopping channels, creating a situation where consumers find value in their solicitation activities. To some extent, this finding also correlates with the result from another study, which shows that many consumers are willing to trade privacy (when they sign up for mailing lists or provide information) for benefits, even though these same consumers are concerned about their privacy – showing paradoxical behaviour (Milne and Gordon, 1994). Other surveys suggest that although most consumers say they do not look at direct mail solicitations and favour some regulation, they still purchase products through the mail (Petty, 2000).

Finally, the association with Internet-related protective behaviour is once again mostly insignificant. Again, part of this effect can be due to the fact that the respondents are active Internet users. It also supports the finding from a previous study, which indicate that online users easily forget about their privacy concerns and communicate much of their personal information relatively easily (Berendt *et al*. 2005). Unfortunately, these researchers also state that because consumers do not always act on their preferences, many of them later react with resentment towards the company who uses their information. Another reason why the Internet-related passive protective behaviour shows insignificant results, may be because this is a relative new medium (as opposed to telephone and catalogue) and that many consumers have not yet experienced privacy violation in this medium, or is still not active enough in this medium to warrant any protective measures. Furthermore, the Internet is a medium that offers privacy control to consumers in that they can choose the time and the extent of the interaction, reducing the need for protective measures. We could only hope that Australia's Spam Act of 2003 contributed to the result, in that it prohibits the supply, acquisition or use of address-harvesting software for the purpose of sending unsolicited commercial electronic messages. The Act also requires that all commercial electronic messages are sent with the express or inferred consent of the recipient, reducing the possibility of privacy violation.

4.4.3 Research question 3: Is there a difference between victims and non-victims of privacy invasion in terms of their privacy concern levels, as well as their active and passive protective behaviour?

The analysis of variance results indicate that respondents who have personally experienced a violation of their personal information in the past, have significantly higher privacy concern levels than those who have not been victims of privacy violation (F 71.9 at 1052 df, p-value < 0.001, victims: 103, non-victims: 98). This makes perfect sense that once a consumer has been a victim of privacy violation, whether it be through solicitation, information misuse or selling information without permission, they will be more sensitive to the privacy issue, increasing their level of concern. Previous research stated that an individual's concern for privacy is likely to vary over the course of his or her lifetime, based on personal experiences (Campbell, 1997). When consumers have had multiple previous negative experiences with data inaccuracies, they become more reluctant to provide subsequent information. The finding of this study is in line with the findings from previous empirical research, which suggests that consumers who have been victims of privacy invasion have higher privacy concerns than consumers who have not been victims of privacy invasion (Harris Interactive and Westin, 2000; Jordaan, 2003).

The analysis of variance results further indicate that respondents who have personally experienced a violation of their personal information in the past, demonstrate significantly higher levels of active protective behaviour (F 108.4 at 1053 df, p-value < 0.001), with the average value for victims being 3.6 and non-victims 2.8. This shows that consumers who feel that their privacy has been violated, will act in a way that should be very clear to companies, namely to explicitly request the removal of their information, notifying companies not to receive advertising material or refusing to provide information to a company. The victims and non-victims did not differ in either of the two subsets of passive protective behaviour variables (F values 3.2 and 0.5, both at 1053 df, p-values 0.075 and 0.498 respectively). This finding suggests that companies cannot assume that only the individuals who actively complain (for example requesting the removal of their personal information), are those that are displeased about the way their personal information was treated. This is in line with the findings from a previous study, which reports that certain behaviours are adopted less frequently when it comes to privacy protection (Sheehan and Hoy, 1999). The findings lead to the conclusion that privacy victims will take active protective measures, but will not necessarily make passive changes in their behaviour. This may also suggest the opposite, namely that consumers are moving from passive protection to privacy activism.

Based on these findings, a binary logistic regression was computed to determine which factors were actually predictive of having experienced prior violations. Socio-demographic variables and original items on privacy-related behaviour were included in the model, and only those respondents who have responded to all variables were included in the computation. The resulting model indicated which behavioural items were predictive of respondents who had personally experienced privacy violations and included: refusal to give personal information (regression coefficient of 0.99, p-value < 0.001); requesting the removal of information (regression coefficient of 0.52, p-value < 0.001); and notifying a company not to send advertising material (regression coefficient of 0.68, p-value < 0.001). Interestingly, these privacy violation victims are less aware of options to remove personal information from organisational databases (regression coefficient of -0.035, p-value < 0.05) and less frequently use the telephone to make purchases (regression coefficient of -0.42, p-value < 0.05). This correlates with a study by Culnan (1995), who reported that many respondents claim to be unaware of any name removal procedures. The results from her study show that consumers who were not aware of name removal procedures were less likely to have shopped using direct marketing channels.

Gender is found to be associated with having experienced privacy violations, with males being more likely to have had such experiences (regression coefficient of 0.39, p-value < 0.05). This is in line with the findings of a study by Sheehan (1999), which show that men are likely to adopt behaviours to

protect their privacy when they become concerned, and that women rarely adopted such behaviours. In another study among American and British consumers, findings are similar and indicate that males are more likely than females to report being a victim of privacy invasion (Harris Interactive and Westin, 2000). In yet another study among South African consumers, the findings show that males are more likely to perceive themselves as victims of privacy invasion (Jordaan, 2003).

To assess the predictive quality of the model, it was compared to the null model. The model including gender and behavioural items performed significantly better (p-value < 0.000) than the null model, thus supporting the interpretation that numerous behavioural variables and gender have predictive value to distinguish between victims and non-victims of privacy violations. The findings resulting from the binary logistic regression support the conclusions drawn based on analyses of variance of summated concern and behavioural scores.

4.4.4 Research question 4: Is there a difference between the Fundamentalist segment and the other segments (as defined by the USA Privacy Index) with relation to their active and passive protective behaviour?

Based on the results from the analysis of variance, Fundamentalists (those consumers postulated to be most concerned about consumer information privacy issues), take significantly more active protective measures, as opposed to non-Fundamentalists (F 18.3 and 13.2, both at 1052 df with $p < 0.001$; Fundamentalists: 3.4 and -0.94, Non-fundamentalists: 3.1 and 1.2). This is in line with all the previous findings, which suggest that consumers who are really concerned about their privacy will take the necessary action to protect their personal information. The findings do not, however, differ between Fundamentalists and Non-fundamentalists with respect to their Internet-related passive protective behaviour ($p = 0.562$). Again, it seems as if consumers who are active on the Internet, do not necessarily differ in terms of how concerned they are with their personal information.

From these findings, one can reason that, not only unconcerned consumers use the Internet, and that companies should take care not to violate consumers' privacy, otherwise they may soon change their Internet behaviour and take active protective measures. This finding show some agreement with another study which reported that 81 per cent of Internet users were concerned about threats to their personal privacy while online, although only six per cent have actually been victims of an online privacy invasion (Louis Harris & Associates and Westin, 1998). This result may also be explained by the findings of a study by Miyazaki and Fernandez (2000), which indicated that higher levels of Internet experience may lead to lower risk perceptions regarding online shopping. Finally, the result

can also stem from the online Internet panel sample, involving respondents who are more involved in the Internet, showing acceptance for this medium.

Another binary logistic regression is computed to investigate which behavioural and socio-demographic variables are best suitable to predict Fundamentalists. Note that Fundamentalists are defined based on their expressed concerns, not on behaviour or prior experiences of violations. Again, only respondents who have answered all questions were included in the model. As with the previous binary logistic regression, this model also highly significantly (p-value < 0.001) outperforms the null model. As opposed to the predictors of victims of privacy violations, many more socio-demographic variables show predictive value for being a Fundamentalist. Being male increases the likelihood of being a Fundamentalist (regression coefficient of 0.33, p-value < 0.05), whereas undergraduate tertiary education and diploma/TAFE certificate (regression coefficients -0.48 and -0.63, both p-values < 0.05) decrease the likelihood of being a Fundamentalist. Most empirical studies report a relationship between levels of education and privacy concern (Harris Interactive, 2002, Milne *et al*., 1996). The findings from a study by Harris Interactive (2002) show that adults with lower educational levels are more concerned about the potential misuse of their personal information than adults with higher educational levels. Our results also show that older respondents are more likely to be Fundamentalists (regression coefficient of 0.15, p-value < 0.05). Various previous studies have found that privacy concerns appear to increase with age (Nowak and Phelps, 1992; Campbell, 1997; Milne and Boza, 1999). One multi-national study among American, British and German consumers found that individuals over 50 years of age were more likely to fall into the category of the 'very concerned' (Fundamentalists) than consumers between 18 and 29 years of age (Harris Interactive and Westin, 2000). In yet another study, the higher mean values among the older age group showed higher concern about information privacy than younger consumers (Jordaan, 2003).

With respect to the behavioural variables, the demonstration of actively protective behaviour is associated with being a Fundamentalist. Refusing information (regression coefficient of 0.37, p-value < 0.001) and requesting information to be removed (regression coefficient of 0.77, p-value < 0.001) are, in particular, highly predictive. The active protective behaviour of requesting companies not to share information with others is, surprisingly, negatively associated with Fundamentalist membership (regression coefficient of -0.39, p-value < 0.05). Not being aware of name removal options (regression coefficient of -0.48, p-value < 0.01) significantly increases the likelihood that a respondent is a Fundamentalist. This is in line with the findings by Phelps *et al.* (2000) who report that previous name removal behaviour has a strong correlation to people's privacy concern level. This is also supported by the findings of Jordaan (2003) showing that respondents who are not aware of name removal

procedures are more concerned about their privacy. Based on the binary logistic regression, none of the variables on the use of risky shopping channels is significantly predictive of being a Fundamentalist. The use of the Internet in particular, does not improve the prediction at all, as opposed to information about the other risky shopping channels, which have negative regression coefficients, but are not significant.

In sum, the findings show that Fundamentalists take more active protective behaviour, tend to be male, tend to be older consumers, and are less aware of name removal options.

4.4.5 Research question 5: How do consumers describe their reaction to a violation of their consumer privacy?

One of the items in the questionnaire puts respondents in a situation where they have just realised that one of the companies they do business with has shared all their personal information with other companies without their permission. Based on this, respondents were asked how they would react to this and to indicate what, if anything, they would do about this. Using an open-ended question allowed us to gain deeper insight into respondents' reactions. Typically, consumer surveys relating to privacy issues use closed-format questions, thus limiting respondents' options to share their behavioural intentions with researchers. The open-ended question led to very extensive answers by respondents, which provided significant additional insight into their feelings and possible reactions in the case of privacy violations.

The answers of all 1055 respondents were independently coded by two coders along the following dimensions: was an active and/or passive behavioural reaction described; did respondents state to contact the company that violated their privacy and/or a party external to the matter; was there an indication of boycotting the company's product; and did respondents consider spreading the word about the misconduct of the company among friends and family. Non-matching codings were discussed until consensus was reached.

A total of 73 percent of respondents indicated that they will react with active protective behaviour, 18 percent with passive protective behaviour and 9 percent will not react (3 percent does not know what to do and 6 percent will do nothing). This is very much in line with the rather unforeseen findings that emerged from the research questions, namely that there is a strong tendency to active protection, as opposed to passive reactions. Many respondents' reactions (39 percent) are to contact the company (through a telephone call or writing a complaint letter) and ask them to remove their personal details

from the database. This is followed by reactions to contact someone other than the company in question (29 percent), for example governmental bodies such as the Department of Fair Trading, Consumer Affairs, the Australian Consumer and Competition Commission, their local member of parliament, the ombudsman, the Privacy Commissioner, lawyers, the media and even the police, to address their concern. Several respondents feel very strongly about taking legal action and say they will see their lawyer and lodge a formal complaint against the company. An unexpected action from respondents was to involve the media in this process, specifically newspapers, radio and the team from the television programme 'A Current Affair'. Very few respondents seemed to be familiar with Australia's Privacy Act and the protection that it can provide them. Those who mentioned the Privacy Act, say they know about it, but do not know about the type of protection it provides. Twenty-seven percent indicate that they will ask the company to remove their data; in view of the other actively protective behavioural measures, a very mild reaction with only little negative consequences for companies.

A total of 4 percent of the respondents also state that they will spread the word and tell everyone they know about this company's information handling practices. From the responses it becomes very clear that many feel that they have no control over the way companies handle their information. They believe that the only way to put themselves in control is to actively warn others and possibly even try to punish the company for misbehaving, by trying to prevent as many other people as possible to buy products or services from them. It seems as if the word-of-mouth communication gives respondents some feeling of power in an otherwise powerless situation. Some respondents say that if this type of privacy violation should happen to them, they would be extra careful in submitting their personal information to any company in the future – having learned from their 'mistakes'.

One fifth of respondents declare that they would immediately stop doing business with the particular company and never deal with the company again. Several respondents state that they would feel very disappointed about the company's lack of integrity, and that they would be determined to not use their products in future, if at all possible. One respondent pronounced: "I would ring them and blast them for not obtaining my permission, then I would not deal with them ever again and l would spread the word that they do this." Most pledge not to support these companies and make others aware of their unethical practices. As one respondent so aptly put it: "The company would join my 'black list', never to be dealt with again." Others went so far as to state that they would post the details of the company's privacy breach on the Internet for others to see, or put an advert on their own personal website informing others to stop buying from this company.

Unfortunately, many consumers feel a lack of control over the protection of their personal information and do nothing to protect their privacy (9 percent). The response from one respondent may provide insight into this situation. "I have contacted that company to complain and ask that my details be taken off their records, yet I was bombarded with advertising from the company and other related companies, until my address changed and I got married and my name was changed." It thus seems as if many companies do not pay attention to consumers' privacy concerns or requests for name removal. This probably explains some consumers' lack of action, because they do not believe that companies will address the issue and make the necessary changes.

The results from the open-ended question led to very interesting findings. First, it supports the findings that have emerged from the other research questions with respect to the asymmetry of active and passive protective behaviours. Respondents generally tend to react in an active way and they are less inclined to make passive changes in their purchasing behaviour in view of preventing the exposure to privacy violation. Second, the reactions signal that organisations need to be seriously concerned about the many ways in which negative consumer reactions can develop from careless information handling practices. Finally, the level of emotions that was expressed in these open-ended questions was extremely high (for example "Fuming!! I would be beside myself with anger"), indicating that the violation of information privacy is not a minor mistake in the view of consumers, it is a major breach of trust in the relationship which is taken very personally by consumers.

5 Discussion

5.1 Privacy concerns are very real

The findings from this study show that consumers are concerned about the protection of their personal information. The responses demonstrate that the privacy issue is very real to consumers, with more than half reporting that they have been victims in their dealings with a company. Unfortunately, once a consumer has been a victim of privacy violation, they will be more sensitive to the privacy issue, increasing their level of concern. At least two thirds of respondents report that they feel uncomfortable when companies share their information with others. Most respondents indicate that they would request companies to remove their information from the database if they sell the information to third parties. This intentional sharing of consumers' personal information by a company, worries consumers who feel that their information is not used or protected as it should be. It is also evident that Australian

consumers do not want to carry the 'protection burden' alone, but expect companies to have privacy policies as protective measures. To have this in place, companies will need to have a supporting protective information infrastructure. When a privacy policy is developed, appropriate infrastructure has to be deployed across the company – people, processes and technologies – to maintain and enforce the privacy policy on a continuous basis (Ravichandran, 2000).

Internally, companies should ensure that all employees understand and adhere to the requirements of the company's privacy policies. Chief Privacy Officers, or other dedicated officials, should be empowered to develop and oversee internal compliance processes that ensure that privacy is an important part of the company's operating strategies (Nash, 2000). Externally, companies should communicate their commitment to privacy policies to consumers, consider joining industry self-regulatory programmes (such as the ADMA) and work with government agencies to ensure privacy protection (Jordaan, 2003).

5.2 Consumers will take action

Eighty percent of respondents indicate that they will request to have their information removed if they suspected that companies were misusing it. If such misuse occurs, companies are not living up to consumers' expectations, leading to a situation where consumers will stop their future dealings with the company. The findings clearly demonstrate that consumers are prepared to engage in active protective behaviour to protect their privacy. A behaviour most respondents are in agreement with is that they will stop doing business with a company if they become aware of information sharing practices without their permission. Some consumers' behavioural intentions are clear: "I will never deal with the company again." Above and beyond this, many respondents say that they will ensure that all their friends and family know about the unethical practices of the particular company.

If companies want to minimise consumers' negative reactions when submitting their information, they will have to offer consumers control over their personal information by providing them with choices regarding the future use of their information. One way in which this can be done is to provide consumers with more control over the initial gathering and subsequent dissemination of personal information. Respondents in this study show that they feel a loss of control. The following excerpt from one respondent's reaction provides a good summary of how many feel: "I believe that companies frequently share my personal information. It angers me, but I do not really know if consumers can do much about it." For consumers to have control, they need to have a say in the type of information that is proper for companies to collect and use as a result of information exchanges. One solution, whether

it be through self-regulation efforts or legislation, is to provide consumers with the knowledge and opportunity to control the type of information a company collects, uses and transfers to third parties. Consumer privacy will be enhanced when consumers are aware of information practices and are given a choice over information provision and use, instead of handling the consumers' information without their knowledge and consent.

Another reason why companies have to address the privacy protection issue is to minimise the costs associated with defending the company against possible privacy lawsuits. Companies will have to negotiate a trade-off between the cost of addressing these consumer protection issues and the expected return from increased consumer confidence in their privacy practices. Moreover, companies should invest in privacy for a more positive return on their investment and active participation by consumers. Privacy sensitive consumers are likely to reconsider the possible consequences of submitting their information to companies. This is especially true if those consequences are negative. In an effort to minimise the effects of negative consequences, respondents have shown that they will behave actively to protect their information. Before consumers are prepared to accept the notion of sacrificing some of their privacy, they have to be convinced that they will receive some real benefit in return. In this trade-off, the key for marketers is to provide a perceived benefit to consumers, rather than to create the impression that they are forcing products on consumers.

5.3 Privacy behaviour and the Internet

Findings indicate that when it comes to shopping through direct marketing channels, most respondents (88 percent) are active in an online environment (which in this case was due to a 100% Internet usage rate of the sample), followed by catalogue shopping (61 percent), and least of all telephone shopping (18 percent). The Internet offers companies the opportunity to use database information for other purposes than its original intended application and to solicit prospective customers at a low cost. Many companies use the Internet for marketing, sales or information dissemination. These practices have the potential, if they are not used appropriately, to lead to a situation where information can be misused. The findings from this study show no significant differences between concerned and unconcerned respondents with regard to their Internet shopping behaviour, suggesting that respondents find the Internet to be a less risky than telephone or catalogue shopping.

One reason for this may be that the Internet has made it possible for companies to gather information without the immediate knowledge of consumers. By using cookies and tracking software, companies are able to gather new types of information that can be used to profile and target individual consumers.

Usually users do not become aware that information about them was collected until after the information is collected and they receive some type of marketing communication from a company that has collected information about them. Findings from previous studies indicate that when Internet users discover that the online environment creates additional opportunities for the misuse of their personal information, they become very sensitive when dealing online (Udo, 2001; Earp and Baumer, 2003). As the popularity of the Internet continues to rise, the privacy issue discussed here will inevitably change.

Companies involved in online transactions should have a greater understanding of the privacy thresholds of Internet users and take extra steps to ensure that the personal information of their users is protected. The first step can be to join a self-regulatory programme in which 'privacy seals' programmes certify that the company is complying with privacy requirements. Once customers are informed about the published privacy policy and educated in the risks of online practices, it should help to gain their trust, reduce their risk perceptions and increase purchase behaviour. A next step can be to seek certification by a credible independent third party and posting their logo on the web site. Privacy seal programmes are independent, non-profit organisations that try to boost users' trust in the Internet by promoting the principles of disclosure and information consent (Ashrafi and Kuilboer, 2005). Some of the leading seal programmes include TRUSTe and BBBOnline. Companies also have to keep in mind that privacy protection in an Internet environment needs the establishment of appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of customer information. A company should also have a security policy that guides security efforts, especially electronic security, since sensitive data is always more susceptible to attack or intrusion via an electronic medium (Sanderson and Forcht, 1996).

5.4 Privacy protection is in the company's best interest

Many respondents shared personal real-life examples in this study, demonstrating their loss of control and frustration. Many have decided to act on their frustration, however trivial their actions may seem to companies. One scenario went something like this (and this is similar to many other personal stories): "At the present I have a problem with a web site called XYZ. I have asked them to remove my email number from their records, but they still have not done so. So I forward each email I get from their customers (about 3 to 5 per day) back to their customer support section in the hope that they will get the message." In their eagerness to leverage technology and their databases of customer information, it seems as if companies have alienated consumers, affecting future transactions and mutually beneficial relationships. The fact that respondents have indicated that they are willing to change their behaviour

and adopt protective behaviour, demonstrate their dissatisfaction with the way companies handle their personal information. Still it does not seem as if many companies demonstrate full commitment to spend resources on privacy protection. Continuing to not take consumers' concerns seriously will inevitably have negative consequences for companies, as already demonstrated in the active protective behaviours of consumers. It is actually shameless to think that consumers have to ask for the protection of the information they have given in good faith to the company. Especially since privacy is a basic human right.

A sense of control among consumers may be a first step in alleviating privacy concerns. One way in which companies may accomplish this is by using permission-based marketing to give customers control, rather than constantly sending mass mailings to purchased customer lists. Another option would be to determine whether reasonable market segments of consumers, which share areas of sensitivity with respect to their information, could be constructed. Companies should be able to optimise the nature of communication with sub-groups of consumers to best accommodate their information privacy requirements if they segment according to privacy sensitivity. Companies have to realise that it only takes one very angry consumer to ruin a company's reputation. Consumer responses suggest a need for strategies and tactics that will alleviate consumer privacy concerns, such as informing consumers why information is collected, how it will be used and who will have access to the information. Effective customer relations now requires companies to communicate in ways that make their customers feel protected, and this includes the development of privacy protection policies and the avoidance of inappropriate sharing of customer information.

Industry groups and associations (such as the ADMA) have been active in self-regulation efforts to combat privacy violations. However, despite industry self-regulation efforts, many companies are still not following proper information handling practices. In a study among the top 500 interactive companies, results show that one-fourth did not have privacy policies published (Ashrafi and Kuilboer, 2005). For self-regulation to be more effective, all companies should realise the importance of protecting consumer information and implementing protective measures. The increase in consumer concern signals that companies should play an active role in the privacy protection process, otherwise public policy makers will have to step in to protect consumers. The Australian government is in the process of addressing the amount of unsolicited telemarketing approaches by proposing a national 'Do Not Call' register. The ADMA has proposed that this national service is developed and operated by industry, but underpinned by legislation that would make the use of the do-not-call service mandatory for all companies and imposes penalties for non-compliance (Shannon, 2006). These types of drastic

measures become necessary because companies do not take care to safeguard the personal information that consumers entrust to them.

From a business perspective, privacy is about acting in such a way that long-term relationships are built through the company's information handling practices. This involves providing some form of control to the consumer whilst providing privacy and security measures while the information is in the company's possession. There is no doubt that the information privacy issue is very real, and will continue to grow if companies do not pay attention to consumers' concerns. The message from the research is clear – it is in companies' best interest to protect their most valuable asset: the customer.

6 Conclusions

The presented study provided an overview of Australian consumers' concerns about information privacy. The main findings indicate that consumers with high privacy concern will show active protective behaviour on all dimensions of information privacy. Individuals who feel that they have been victims of privacy invasion will have higher concern and do more to actively protect their information. Victims are generally those who refuse to provide their personal information, notify companies not to send them advertising material and are not aware of name removal options. Those with high concern (the so-called Fundamentals) show active protective behaviour, refuse to provide personal information, request removal of information and are not aware of name removal options. Finally, 91 percent of respondents indicated that they intend to act if their privacy is violated. The remaining 9 percent, who does not show an intention to adopt protective behaviour, state that they do not know what to do or will do nothing because they do not feel that it will help.

The unexpected findings that emerged from this study related to consumers' tendency to take active protective measures. It does not appear that high levels of privacy concerns or prior experiences with privacy violations have an equally strong effect on passive protective behaviour. This can either indicate to companies that passive behaviour, such as reducing the use of certain distribution channels, is not a viable protective option to consumers, or that consumers are moving from being passive to privacy activism.

The fundamental message is that concerns about privacy issues tend to lower purchase behaviour, implying that if companies can lower the consumers' risk perceptions, they should have higher purchasing behaviour. This research validates the importance for companies to establish a privacy environment to instil confidence and build trust with consumers. Marketers are in the relationship

business and they have to recognise that privacy protection forms an important part in the value proposition when customers decide to purchase products and services in future. When companies use personal information in a way that offends consumers, the perception of marketing as a whole suffers.

Given heightened media attention and public awareness of privacy issues, having a privacy policy on paper may not be enough to make customers feel safe and protected. Companies who want to build a long-term relationship with their customers may have to consider supporting their intentions with actions, and develop procedures that will fortify business practices against breaches of privacy and protect customer information from unintentional exposure. This may require that a company will have to pro-actively adopt measures to monitor the customer information flows in and out of the business through their customer relationship systems.

The data captured in the survey has proved to be very rich, and there is considerable scope for further analysis. In the course of this study a number of follow-up questions have emerged. For instance, given the strong emotional reaction to simulated violations of privacy protection, it would be very interesting to further investigate the extent to which the expressed behavioural intentions of boycotting and spreading negative word-of-mouth are actually translated into real behaviour; in which way consumers react to information privacy invasions by companies who have a monopoly or monopoly-like market positions thus making boycott unfeasible; and whether different forms of privacy violations lead to different behavioural consequences by consumers. Such investigations would enable a more precise prediction of negative consequences for companies choosing not to protect the privacy of their customers and allow a translation of such negative consequences into loss of revenues, thus providing a strong argument for a market-driven reasoning to comply with Australian privacy protection legislation. The insignificant results relating to concern levels and Internet-related passive behaviour in this study are assumed to have several possible reasons: the sample of respondents consisted of active Internet users which are likely to be less inclined to refuse using the Internet due to privacy concerns or even experiences with privacy violations; that consumers do not always act on their preferences; the Internet offers privacy control to consumers in that they can choose the time and the extent of the interaction; and/or that higher levels of Internet experience may lead to lower risk perceptions regarding online shopping. It would be very interesting to evaluate the extent to which each of the two sources contributed to the insignificance by replicating the Internet-related part of the study with a telephone or mail sample. In any case, as consumers' use of Internet technology increases, so will companies' responsibility to educate consumers and adapt to their privacy needs. One of the fundamental aspects of successful relationships remains the information exchange between consumers

and marketers. Protecting the privacy of consumer information is becoming a measure of success in the business world. If companies safeguard the personal information that consumers entrust to them, they can improve their reputation, giving them an edge over competitors who do not make privacy a priority. When companies collect, store, handle and sell consumer information with consumer privacy in mind, they may just get a competitive incentive as a result. If companies do not want government or consumers to take control of the privacy issue, they will have to lead by example.

7 Appendix: Socio-demographic profile comparison

Table A: Comparison of Socio-Demographic Profiles (study sample versus Census 2001)

		SAMPLE %	CENSUS 2001 %
Gender (%)	Male	50	49
	Female	50	51
Age (%)	18-25 years	12	15
	26-35 years	22	20
	36-45 years	24	21
	46-55 years	16	18
	56-65 years	22	12
	66-75 years	4	9
	76-85 years	0	5
Income (%) *	No income	11	6
	AU$1-AU$159	5	7
	AU$160-AU$299	12	22
	AU$300-AU$499	17	17
	AU$500-AU$699	21	14
	AU$700-AU$999	18	11
	AU$1000-AU$1499	10	7
	Over AU$1500	6	4
Ethnic orientation (%) +	Australian	72	72[+]
	Other	28	28[+]
Employment status (%) [#]	Employed full-time	43	36
	Employed part time	13	18
	Self-employed	12	
	Not-employed	2	39
	Student	2	
	Homemaker/ Housewife	11	
	Pensioner/ Retired	12	
	Unfit for work	2	
Level of education	Secondary school – year 10	18	65
	Secondary school – year 12	16	
	TAFE diploma/certificate	26	22
	Undergraduate tertiary education	22	10
	Postgraduate tertiary education	19	3

*based on population aged 15 and above

the remaining respondents did not state their status, census categories could not be directly matched with survey categories.

+ based on birthplace of parents

8 References

Ashrafi, N., Kuilboer, J., 2005. Online privacy policies: an empirical perspective on self-regulatory practices. Journal of Electronic Commerce in Organizations, 3(4), 61-74.

Berendt, B., Gunther, O., Spiekerman, S., 2005. Privacy in e-commerce: stated preferences vs actual behavior. Communications of the ACM, 48(4), 101-106.

Campbell, A.J., 1997,. Relationship marketing in consumer markets: a comparison of managerial and consumer attitudes about information privacy. Journal of Direct Marketing, 11(3), 44-57.

Caudill, E.M., Murphy, P.E., 2000. Consumer online privacy: legal and ethical issues. Journal of Public Policy & Marketing, 19(1), 7-20.

Chen, K,. Rea, A.I., 2004. Protecting personal information online: a survey of user privacy concerns and control techniques, 44(4), 85-92.

Collier, G., 1995. Information Privacy. Information Management & Computer Security, 3(1), 41-45.

Culnan, M.J., 1993. How did they get my name: an exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly, 17(3), 341-362.

Culnan, M.J., 1995. Consumer awareness of name removal procedures: implications for direct marketing. Journal of Direct Marketing, 9(2), 10-19.

Culnan, M.J., 2000. Protecting privacy online: is self-regulation working? Journal of Public Policy & Marketing, 19(1), 20-27.

Earp, J.B., Baumer, D., 2003. Innovative web use to learn about consumer behavior and online privacy. Communications of the ACM, 46(4), 81-83.

Evans, M., Patterson, M., O'Malley, L., 2001. The direct marketing-direct consumer gap: qualitative insights. Qualitative Marketing Research: An International Journal, 4(1), 17-24.

Graeff, T.R., Harmon, S., 2002. Collecting and using personal data: consumers' awareness and concerns. Journal of Consumer Behaviour, 19(4), 302-318.

Ha, H., 2004. Factors influencing consumer perceptions of brand trust online. Journal of Product and Brand Management, 13(5), 329-342.

Harris Interactive, Westin, A., 2000. The IBM-Harris Multi-National consumer privacy survey. Privacy & American Business, 7(1), 1-16.

Harris Interactive. 2001a. A survey of Consumer privacy attitudes and behaviours. PLI/Harris, http://www.understandingprivacy.org.

Harris Interactive. 2001b. Consumer privacy attitudes and behaviours survey wave II. PLI/Harris, http://www.understandingprivacy.org.

Harris Interactive. 2001c. Consumer privacy attitudes and behaviours survey wave III. Privacy & American Business, The American consumer and privacy: P&AB's annual round-up and analysis of privacy surveys, as discussed at the 8th Annual National Conference 'Managing the new privacy revolution', 20-22 March, Washington, DC.

Hewett, W.G., Whitaker, J., 2002. Data protection and privacy: the Australian legislation and its implications for IT professionals. Logistics Information Management, 15(5), 369-376.

Jordaan, Y., 2003. South African consumers' information privacy concerns: an investigation in a commercial environment. Unpublished Doctoral thesis, University of Pretoria.

Loro, L., 1995. Downside for public is privacy issue. Advertising Age, 66, 32.

Louis Harris & Associates, Westin, A.F., 1998. Privacy concerns and consumer choice. Privacy & American Business, November, 1-122.

Maynard, M.L., Taylor, C.R., 1996. A comparative analysis of Japanese and US attitudes toward direct marketing. Journal of Direct Marketing, 10(1), 34-44.

McCarthy, J.A., 2002. Data privacy in the information age. Journal of Public Policy & Marketing, 21(2), 336-339.

Meinert, D.B., Peterson, D.K., Criswell, J.R., Crossland, M.D., 2006. Privacy Policy Statements and Consumer Willingness to Provide Personal Information. Journal of Electronic Commerce in Organizations, 4(January-March), 1-17.

Milne, G.R., Beckman, J., Taubman, M.L., 1996. Consumer attitudes toward privacy and direct marketing in Argentina. Journal of Direct Marketing, 10(1), 22-33.

Milne, G.R., Boza, M.E., 1999. Trust and concern in consumers' perceptions of marketing information management practices. Journal of Interactive Marketing, 13(1), 5-24.

Milne, G.R., Gordon, M.E., 1994. A segmentation study of consumers' attitudes toward direct mail. Journal of Direct Marketing, 8(2), 45-52.

Miyazaki, A.D., Fernandez, A., 2000. Internet privacy and security: an examination of online retailer disclosures. Journal of Public Policy & Marketing, 19(1), 27-44.

Moghe, V., 2003. Privacy management – a new era in the Australian business environment. Information Management & Computer Security, 11(2), 60-66.

Nash, K.S., 2000. The Direct Marketing Handbook, Second edition, McGraw-Hill, New York.

Nowak, G.J., Phelps, J.E., 1992. Understanding privacy concerns: an assessment of consumers' information related knowledge and beliefs. Journal of Direct Marketing, 6(4), 28-39.

Nowak, G.J., Phelps, J.E., 1997. Direct marketing and the use of individual-level consumer information: determining how and when privacy matters. Journal of Direct Marketing, 11(4), 94-108.

Nunnally, J., 1978. Psychometric Theory, Second edition, McGraw-Hill, New York.

Page, C., Luding, Y., 2003. Bank managers' direct marketing dilemmas – customers' attitudes and purchase intention. International Journal of Bank Marketing, 21(3), 147-163.

Petrison, L.A., Wang, P., 1995. Exploring the dimensions of consumer privacy: an analysis of coverage in British and American Media. Journal of Direct Marketing, 9(4), 19-37.

Petty, R.D., 2000. Marketing without consent: consumer choice and costs, privacy, and public policy. Journal of Public Policy & Marketing, 19(1), 42-54.

Phelps, J., Gonzenbach, W., Johnson, E., 1994. Press coverage and public perception of direct marketing and consumer privacy. Journal of Direct Marketing, 9(2), 9-22.

Phelps, J., Nowak, G., Ferrell, E., 2000. Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy and Marketing, 19(1), 27-42.

Ravichandran, T., 2000. Total quality management in information systems development: key constructs and relationships. Journal of Management Information Systems, 16(3), 119-156.

Rotenberg, M., 2001. The Privacy Law Sourcebook 2001: United States Law, International Law, and recent developments. Washington, DC: EPIC Publications.

Sanderson, E., Forcht, K.A., 1996. Information security in business environments. Information Management & Computer Security, 4(1), 32-37.

Shannon, L., 2004. Public urged to comment on new draft eMarketing Code of Practice. ADMA Press Office, 11 August.

Shannon, L., 2005a. New research shows Australian consumers' expect relevant direct contact from organisations. ADMA Press Office, 30 March.

Shannon, L., 2005b. Businesses urged to communicate in the right way to attract the 'Sophisticated New Consumer'. ADMA Press Office, 31 May.

Sheehan, K.B., 1999. An investigation of gender differences in on-line privacy concerns and resultant behaviors. Journal of Interactive Marketing, 13(4), 24-38.

Sheehan, K.B., Hoy, M.G., 1999. Flaming, complaining, abstaining: how online users respond to privacy concerns. Journal of Advertising, 28(3), 37-51.

Sheehan, K.B., Hoy, M.G., 2000. Dimensions of privacy concern among online consumers. Journal of Public Policy & Marketing, 19(1), 62-74.

Taylor, C.R., 2004. Consumer privacy and the market for customer information. The Rand Journal of Economics, 35(4), 631-650.

Turner, M.A., Varghese, R., 2002. Making sense of the privacy debate: a comparative analysis of leading consumer privacy surveys. Privacy & American Business, The American consumer and privacy: P&AB's annual round-up and analysis of privacy surveys, as discussed at the 8th Annual National Conference 'Managing the new privacy revolution', 20-22 March, Washington, DC.

Udo, G.J., 2001. Privacy and security concerns as major barriers for e-commerce: a survey study. Information Management and Computer Security, 9(4), 165-174.

Vidmar, N., Flaherty, D.H., 1985. Concern for personal privacy in an electronic age. Journal of Communication, 35(2), 91-103.

Wang, P., Petrison, L.A., 1993. Direct marketing activities and personal privacy. Journal of Direct Marketing, 7(1), 7-19.

Table 1: Sorted loadings matrix for principal components analysis of behavioural items

PROTECTIVE BEHAVIOUR	Factor 1	Factor 2	Factor 3
ACTIVE: Requested removal of information	**0.70**	0.05	0.03
ACTIVE: Requested not to share information with others	**0.68**	-0.03	-0.10
ACTIVE: Notified not to receive advertising material	**0.64**	0.09	0.06
ACTIVE: Refused to provide information	**0.57**	0.06	-0.04
ACTIVE: Requested to inform which measures used to keep information safe	**0.48**	0.15	-0.30
PASSIVE: Called a toll-free number to order	0.01	**0.71**	0.07
PASSIVE: Bought something from a catalogue or brochure	-0.11	**0.70**	0.04
PASSIVE: Bought through a telephone call	-0.16	**0.61**	0.06
PASSIVE: Purchased anything via the Internet	0.14	-0.04	**0.80**
PASSIVE: Used Internet banking	0.10	-0.06	**0.79**

Table 2: Descriptive statistics of summated scores

SUMMATED SCORES	N	Min	Max	Mean	Std. Dev.
Privacy concern score	1054	25.00	125.00	100.97	10.23
• Privacy protection score	1054	9.00	45.00	41.21	4.638
• Information misuse score	1054	7.00	35.00	26.78	3.74
• Solicitation score	1054	6.00	30.00	19.76	2.66
• Government protection score	1054	3.00	15.00	13.22	2.17
Active protective behaviour score	1055	0.00	5.00	3.23	1.35
Passive protective behaviour score (telephone and catalogue)	1055	-3.00	0.00	-1.07	0.91
Passive protective behaviour score (Internet)	1055	-2.00	0.00	-1.72	0.57

Table 3: Agreement with consumer privacy-related statements

	Agree strongly (%)
I would request company to remove information if misused	80
Companies should have privacy protection policies	78
Privacy protection policies should indicate how it will protect my information	74
I would request removal of information if sold to others	72
Companies should have privacy protection policies indicating reasons for protection	70
Companies must have privacy protection policies	70
I feel uncomfortable when companies share information	70
Government should limit companies' use of information	65
I refuse to provide personal information without reason supplied	65
I would support a company's effort to ensure safety	63
Government should do more to protect safety of information	61
Too many companies call to sell products and services	60
Government should restrict information collection	56
I am concerned about misuse	53
I receive too much advertising material	47
Companies send too much advertising material	41
I fear that personal information may not be safe while stored	39
Companies regularly share information with others to offer products and services	39
I believe that companies use information for other purposes	38
Consumer information is misused	37
Companies share information with other without permission	36
Consumers not interested in getting information from unfamiliar companies	13
I am pleased to receive information from unfamiliar companies	6
I do not mind receiving telephone calls	3
Information is safe while stored in a company's records	3

Table 4: Percentage of respondents who have engaged in exposing or protecting behaviour

	Yes (%)
Purchased anything via the Internet	88
Used Internet banking	84
Refused to provide information to company	82
Notified not to receive advertising material	79
Requested company to remove information from records	69
Requested company not to share information with others	67
Bought something from a catalogue or brochure	61
Victim of privacy invasion	56
Aware of options to remove information	43
Called a toll-free number to order	29
Requested to inform which measures are used to keep info safe	26
Bought through a telephone call	18