CHAPTER 8
CONCLUSIONS, IMPLICATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

8.1 INTRODUCTION

In the final chapter of the study, interpretations are made based on the empirical results presented in Chapter 7. A Maximum Likelihood Exploratory Factor Analysis was conducted, as reported in Chapter 7, to determine the underlying dimensions of consumers' information privacy concerns. A four-factor solution emerged as the most interpretable factor structure, and the factors were labelled 'privacy protection', 'information misuse', 'solicitation' and 'government protection'. In this chapter, the main findings from the previous chapter are presented and conclusions are drawn on the use and application of the information privacy dimensions as an instrument for organisational decision-making. Thereafter the implications of each main set of findings are discussed and recommendations are made. The limitations of the study are also presented and recommendations for future research are highlighted. The chapter concludes with an evaluation of the research results obtained for each of the formulated objectives.

8.2 MAIN FINDINGS RELATING TO PRIVACY PROTECTION CONCERNS

The first underlying dimension identified by the research was consumers' concerns regarding protection of their privacy. The privacy protection dimension was related to several of the information privacy issues identified in the theory. The concerns mainly pertained to the behavioural intentions of consumers to protect their privacy and privacy protection policies of organisations regarding data collection, storage, use, disclosure and solicitation. The privacy protection concerns included concerns about the sharing of personal information with third parties, the reasons for collecting information and the safe-keeping of information by organisations.

The empirical findings regarding privacy protection concerns indicated that there were differences between consumers' privacy protection concerns and their manifest behaviours to protect privacy. Consumers may engage in various protective behaviours, when they believe that they can manage their information and thus minimise the potential negative consequences. Several differences were found between consumers who exercise different levels of protective behaviour. Consumers who were more concerned about their privacy protection than consumers who exerted no form of protective behaviour displayed the following behaviour: they refused to give their personal information to an organisation; they requested having their name removed; they notified an organisation of solicitation; they requested that their information not be shared; and/or they requested that their information be kept safe.

Demographic differences were also found between different groups of respondents with regard to their privacy protection concerns. Older consumers had more privacy protection concerns than younger consumers. Females had higher privacy protection concern levels than males. English- and Afrikaans-speaking groups had the highest levels of privacy protection concern. Both the middle and high income groups had higher levels of privacy protection concern than the low income group.

8.2.1 Conclusions regarding the main findings on privacy protection concerns

The privacy protection dimension indicated that consumers feel that their personal information is not protected by organisations. Consumers clearly expect organisations to have privacy policies in place that will protect their personal information during all organisational activities. They also reported that they would request the removal of their information, or refuse to provide information in future transactions, if organisations do not address the protection of their information. Organisations have to realise that consumers are aware that their information is not always safe while in the possession of the organisation. Respondents have, however, indicated that they would support an

organisation's efforts to ensure that their personal information is safely kept, thereby showing their willingness to participate in protection activities.

With regard to privacy protection, consumers reported that they were the most concerned when their personal information is shared with other organisations without their permission. This intentional sharing of consumers' personal information by an organisation, coupled with the risk that the information could be unintentionally shared because it has not been secured worried consumers who felt that their information might not be used or protected as they had intended. If such misuse occurs, organisations are not living up to consumers' expectations, leading to a situation where consumers may stop their future dealings with a given organisation.

The research findings suggest that certain consumers may have higher levels of privacy protection concern than others. Consumers who are older or in the higher income group report higher levels of privacy protection concern. Some respondents have indicated a willingness to change their behaviour, or adopt protective behaviour, if they sense that an organisation has invaded their privacy. Whether consumers will actually exert such behaviour is not very clear, but at least they are signalling their intentions to change their behaviour if an organisation does not protect their information. This indicates that consumers are not comfortable with the current level of protection of information provided by organisations, and that they expect more protection if a long-term relationship is to be built.

It should be noted, however, that although several significant differences were found between groups in terms of their specific privacy protection concerns, the descriptive statistics indicated very high percentages of concern among the majority of consumers. Privacy protection can thus be seen as an issue that is of great importance to all consumers, irrespective of their behaviour or demographic characteristics. Organisations need to realise that privacy concerns are very real and will not go away. Effective customer relations now requires organisations 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.

8.2.2 Implications of the main findings on privacy protection concerns

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. Organisations can use privacy protection policies to communicate with consumers, and organisations can use their privacy practices as a selling point. A clear privacy policy can increase consumer trust and confidence in an organisation's data practices, but not having a privacy policy can have the opposite effect. As organisational privacy policies have come to be regarded as the norm, organisations without privacy policies risk adverse reactions from consumer segments that actively seek protection. However, many organisations are still reluctant to offer consumers privacy protection options, such as opt-in features that require getting consumers' permission to collect or transfer personal information. Organisations fear that if they offer privacy protection options, they will lose their ability to control customer data and share such information with other organisations. Organisations have to recognise that they will not lose customers if they offer privacy protection options, but that they may forfeit access to some further information.

Because consumers have signalled that they view privacy protection as very important, organisations 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. One obvious reason why organisations have to address the privacy protection issue is to minimise the costs associated with defending the organisation against possible privacy lawsuits. Moreover, many organisations should invest in privacy for a more positive return on their investment and active participation by consumers.

In today's economy, some organisations may experience a strong urge to cut costs and re-evaluate budget allocations and investments. An organisation's commitment to an overall privacy protection programme is one investment that should not be compromised. Having a strong compliance framework around privacy protection not only ensures that an organisation is complying with its internal policies and legal requirements, but also serves to strengthen and renew an organisation's commitment to the customer. In return, this builds the confidence of a customer and fosters an ongoing relationship built on trust.

Disclosing an organisation's privacy policies can be a key step towards transparency where consumers learn more about an organisation's data collection practices. An informed customer demonstrates trust in an organisation when (s)he willingly share his or her personal information with an organisation in exchange for a product, service or personalised experience.

8.2.3 Recommendations regarding privacy protection concerns

One of the first steps that an organisation needs to take to ensure customer privacy protection is to develop a privacy protection policy and communicate this to its customers. A well-designed strategy for communicating the goals and objectives of an organisation's privacy policy should be based on a deep-rooted understanding of the privacy protection concerns of consumers as well as the laws and regulations affecting the organisation. The strategy should be clear and comprehensible, should gain and maintain the trust of all participants, and be efficient in meeting the privacy protection requirements. This will be in line with the eighth principle of the OECD Guidelines, namely, the principle of accountability (see Chapter 3, Section 3.5 of this study). To assist in the development and implementation of a privacy policy, organisations should consider appointing an accountable executive, sometimes known as a Chief Privacy Officer.

Leading organisations have to develop privacy policies that reflect their corporate philosophies, business models and the needs of their target market. They have to understand what kind of information they are collecting, how they use such information, how it is shared and whether they really need all of it. Having clear policies that are easily accessible and provide visibility into the organisation's privacy practices and how information is being collected, used and protected is a critical component of earning consumer trust and confidence.

To evaluate their relative performance, organisations should benchmark their policies not only against industry-specific requirements, but also against internationally accepted fair information principles and any self-regulation programmes that the organisation has pledged to honour. However, true leaders design their policies and practices to attract and retain consumers, not merely to meet minimum compliance requirements. Organisations should not be reactive and await privacy legislation, but should be pro-active and develop their own privacy policies, becoming accountable for their customers' personal information. If organisations take leadership in privacy protection, they can build consumer confidence in the market by ensuring that personal information is protected while it is in their possession.

Organisations can consider the following privacy protection guidelines:

- Provide customers with privacy policies containing detail on the organisation's information-gathering practices, including what personal information is collected, how it is collected and how the organisation plans to use it.
- Collect only the amount of individual and household data necessary to complete the marketing transaction.
- Implement appropriate security methods and technologies to protect personal data while in the possession of the organisation.
- Offer consumers the option to opt out of having their personal information collected, shared or used.
- Provide individual customers with reasonable access to their personal data and provide them with the opportunity to correct or delete information.

A privacy protection programme can have several tangible benefits for an organisation. First, it can lead to improved business performance. An organisation should not spend too much time and effort collecting information that it does not need or plan to use. This excess information creates data integrity, quality and accuracy problems. Eliminating excess data collection and retention reduces privacy risk and, at the same time, increases business performance. Second, organisations that respect the privacy preferences of their customers can create enhanced customer loyalty. Third, privacy protection can decrease the frequency of customer turnover, leading to higher profitability. Customers switch business for a variety of reasons, and one of the emerging factors identified by the present study is consumers' concern about privacy protection. Finally, an additional benefit of a well-managed privacy protection programme is favourable publicity.

It is important for organisations to realise that privacy policies as such do not earn consumers' trust or their business. Organisations seeking active participation from consumers (purchasing goods and services, sharing personal information and referring family and friends) need to do more than merely provide consumers with their privacy protection policies. The active participation of consumers hinges strongly on trust and value (which must be earned). Business transactions rely on an exchange of personal information, but majority of consumers resist this exchange based on their principle of privacy. Given the diversity of business models, and the prevalence of outsourcing, it is no longer sufficient for organisations to manage the privacy practices internally. Organisations must also manage the chain of trust they create when they share customer information with other organisations. Privacy issues are central to gathering market information, and the trust between consumers and marketers needs to be handled with care. Organisations should develop a framework that balances consumer privacy concerns with the information needs of the organisation(s) involved.

8.3 MAIN FINDINGS RELATING TO INFORMATION MISUSE CONCERNS

The second underlying privacy dimension identified by the empirical analysis related to consumers' concern regarding misuse of their personal information. Their concerns included how personal information is used, the possible misuse of information by organisations, the sharing of personal information with other organisations and the safety of personal information while it is stored in a database. If an organisation wishes to keep its customers' information safe, the personal information which it collects has to be stored in a way reasonably calculated to prevent its loss, theft or modification. When information is not safely kept, unauthorised access to or the modification of information (whether in storage, processing or transit) can possibly lead to information misuse.

A total of 64 per cent of the respondents in this study said that they believed that organisations regularly use consumers' information for other purposes than those for which it was supposedly collected. The majority of consumers also felt that their personal information was not safe while stored in organisations' databases. These concerns are addressed in the OECD's fourth and fifth principles, which state that the use of personal data ought be limited to specified purposes, and that there should be security safeguards for personal data, which must be collected and stored in a way reasonably calculated to prevent its loss, theft or modification (as discussed in Chapter 3, Section 3.4.4 and 3.4.5 of this study).

The empirical findings regarding information misuse concerns indicated that there were differences between consumers' information misuse concerns and their manifest behaviours to protect privacy. Consumers who exercised protective behaviour were more concerned about misuse of their personal information than consumers who have not changed their behaviour to protect their privacy. Another finding pertaining to information misuse concerns related to consumers' personal experiences of privacy invasion. The results showed that respondents who had experienced invasions of privacy were more concerned than respondents who stated that they had not experienced invasions of privacy. When a consumer's information is misused by an

organisation, it manifests in a situation where the consumer feels that his or her privacy has been invaded.

The findings also suggested differences in terms of consumers' level of knowledge about information protection practices and their information misuse concerns. The results indicated that respondents who did not have knowledge about information protection practices were more concerned about possible misuse of their information. This study also uncovered differences in information misuse concerns between respondents who use the Internet for certain transactions and respondents who do not. The Internet user group was more concerned about information misuse than the Internet non-user group.

Demographic differences were also found between respondent groups with regard to information misuse. Consumers older than 40 years were more concerned about information misuse than younger consumers. English-speaking consumers were more concerned about information misuse than Afrikaans-speaking and Black African language consumers. The consumers who had the highest level of education also manifested the highest level of information concern. The only difference between employed and unemployed respondents was detected on the information misuse dimension. Employed consumers had higher levels of information misuse concerns than unemployed consumers. This seems consisted with another finding that pointed to higher levels of information misuse concern among high income consumers, compared to middle and low income consumers.

8.3.1 Conclusions regarding the main findings on information misuse concerns

Some researchers believe that consumer anxiety regarding the collection of personal information has much to do with **how** the information is used. The information misuse dimension in the survey confirmed this belief, because respondents are very concerned about how their information is used (or misused) by organisations. The identification of information misuse as an important privacy dimension is consistent with the current

privacy practices in South Africa, where there are no restrictions on secondary uses of personal information gleaned from consumers. This situation has resulted in concerned consumers, explaining why 79 per cent of the respondents stated that they felt concerned about the misuse of their personal information by organisations.

The above-mentioned findings strongly suggest that the majority of consumers are becoming increasingly uncomfortable knowing that information about them is being collected and then used for other purposes than the ones originally intended. This study has uncovered what consumers considered to be a misuse of their information, and signals to organisations that they should be cautious how they use consumers' information once they have collected such information. If they use this information for other purposes than the purposes stated during collection, if they share the information with other organisations, and if they do not keep consumers' personal information safe while stored in their database, consumers will believe that their information has been misused. It is often said that an organisation's most valuable asset is the data it generates, emphasising why it is so important not to misuse this information, or to create a perception that it is being misused.

As has been mentioned previously, the findings indicated that consumers who exercised protective behaviour had higher levels of information misuse concern than others. This should suggest to organisations that consumers will change their behaviour and request the removal of their personal information from the organisation's database if they suspect the information is being misused. The findings also demonstrated that consumers who were not aware of name removal procedures, had higher levels of information misuse concern than consumers who were aware of name removal procedures. From this one can deduce that consumers who have knowledge on how to protect their information privacy (by requesting the removal of their information from organisational records) feel less vulnerable to information misuse than those who do not know of any means to protect their information once they have provided it to organisations. Another significant result was that employed consumers were more concerned about misuse of their information than consumers who were unemployed.

This implies that consumers who are employed and earn an income are more likely to be targeted by organisations, and it is their information which is used most by organisations, opening up the possibility of over-use and misuse by organisations.

The advent of the Internet as a medium for efficiently transacting business, sharing information and creating personalised exchange experiences has changed the nature of relationships that organisations have with the consumers, suppliers, partners, competitors and the government. These relationships are complex and are riddled with trust issues that must be addressed in order for all parties to continue to participate in online transactions. The findings also established differences in terms of consumers' information misuse concerns and their Internet use. Use of the Internet has grown considerably during the past decade, particularly in respect of its application as a tool for market exchange. This rapid growth has been accompanied by concern regarding the collection and dissemination of consumer information by marketers who participate in online activities. The Internet offers opportunities to use database information for other purposes than its original intended application and to solicit prospective customers (at a low cost). Many organisations 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.

8.3.2 Implications of the main findings on information misuse concerns

Privacy sensitive consumers are likely to reconsider the possible consequences of submitting their information to organisations. This is especially true if those consequences are negative. In an effort to minimise the effects of negative consequences, consumers may actively avoid situations in which they are required to give information, or they may refuse to give information. If organisations want to avoid this situation, they can offer consumers control over their personal information by providing them with choices regarding the future use of their information. This can be done during the data-collection phase by offering consumers a choice to opt in or to opt out.

When consumers have the perception that their personally identifiable information may be misused by an organisation, they are likely to refuse to provide the information, or may supply incorrect information. Organisations should therefore build trust with their consumers and not misuse customers' personal data. Building trust requires the organisation first to ensure that promises made to customers regarding information use are supported by corresponding actions within the organisation, as well as its extended network with its business partners. Organisations need to ensure that their people, processes and technologies are aligned to comply with their intentions.

Trust issues range from the reliability of systems and processes to meet promised service levels, the confidentiality with which information is shared among business partners, and the integrity of the transactions in terms of the protection of personally identifiable information collected from consumers. Any organisation that does not safeguard consumers' personal information properly will be subjected to the same fate as a bank that does not safeguard people's money: it will go out of business. A failure to generate trust can have equally damaging effects on brand value, corporate reputation and marketing relationships. This is especially relevant to online transactions. If Internet users discover that the online environment creates additional opportunities for the misuse of their personal information, this medium will suffer and not grow to its full potential. Organisations 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 than they currently do.

8.3.3 Recommendations regarding information misuse concerns

Leading organisations need to understand that a privacy policy is only as good as its supporting infrastructure. When a privacy policy is developed, appropriate infrastructure has to be deployed across the organisation – people, processes and technologies – to maintain and enforce the privacy policy on a continuous basis. It requires ongoing effort to ensure that the business develops procedures, processes and programmes to

accomplish its privacy objectives. Internally, organisations should ensure that all employees understand and adhere to the requirements of the organisation'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 organisation's operating strategies. Privacy officers must assume responsibility for the data entrusted to their organisations, and they should expect to be held accountable for information misuse. Externally, organisations should communicate their commitment to privacy policies to consumers, join industry self-regulatory programmes and work with government agencies to ensure privacy protection.

All organisations have an obligation to protect consumer data from unauthorised access, disclosure, modification or use. In computer security, privacy protection is seen as the establishment of appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of data records and to protect both the security and confidentiality against any misuse that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual about whom such information is kept. Organisations may also need to be sensitised not to use the information collected for any other purposes than those stated when the information was collected and to obtain consumers' permission before sharing information with other organisations.

Given heightened media attention and public awareness of privacy issues, having a privacy policy on paper is not enough without an adequate compliance framework to enforce the policies internally. Organisations must also be accountable to their own policies. Organisations must support their intentions with actions and develop procedures that will fortify business practices against breaches of privacy and protect customer information from unintentional exposure. This requires an organisation pro-actively to adopt technical measures to monitor the customer data flows in and out of the organisations through their customer relationship systems.

Privacy and security are synonymous with regard to the safeguarding of customer information. A sound security infrastructure must be in place to maintain consumer trust. Organisations should adopt appropriate monitoring and controls to prevent a customer's information from being compromised. An organisation should 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. The first step in planning for a security policy is to undertake a study to assess the organisation's risk. After that the policy should be formulated by setting specific standards which should be communicated throughout the organisation. Security is an ongoing issue and policy should be reviewed regularly. Very important elements in security are that staff buy in, co-operate and commit themselves to the policy. The importance of the information, the reasons for security policies and the benefits of security should be emphasised.

Organisations should establish the following guidelines to protect consumers from information misuse:

- Institute security policies and practices that ensure uninterrupted security of information systems.
- Create and implement staff policies, procedures, training and response measures to protect personal data in everyday practice.
- Employ and periodically reassess physical and technological security safeguards.
- Inform business partners and service providers of their responsibility to protect the security of personal data.

An organisation can consider engaging in a relationship with an independent third party to audit the organisation's compliance with stated privacy policies. It can create a favourable position where trust may be earned or re-established when organisational policies, technologies and processes are routinely tested to prove that organisations are living up to their promises. Independent parties can be used to verify and proactively communicate the organisation's investment in privacy protection, confirming that the organisation will not misuse consumers' information. Organisations can also become involved in privacy seal programmes which encapsulate industry standards and

regulatory requirements. Participation in a privacy seal programme can serve as a benchmark to gauge an organisation's activities to meet certain privacy standards and can help to build consumer confidence, in short, it creates a visible manifestation of trust. This may have a higher credibility value than mere statements by organisations about their privacy practices. In the online environment, a number of organisations operate as privacy-seal custodians (for example, TRUSTe or BBBOnline).

Online organisations should also be working to assure customers of privacy in their online transactions. They should develop sound web privacy policies and communicate their web practices to customers on their web site. The very nature of the web makes it imperative that organisations pro-actively manage web site privacy, both to stay in compliance with and to earn customer trust. Web sites typically have powerful techniques for gathering data and personal information. Privacy problems occur when that information is shared with third parties without authorisation, or when personal or behavioural information is collected inappropriately through web page forms or cookies. Software to block online advertisements and cookies should receive national government support to create a safer environment.

8.4 MAIN FINDINGS RELATING TO SOLICITATION CONCERNS

The third underlying privacy dimension identified by the empirical analysis related to consumers' concerns regarding the intrusion of companies into their lives by means of unsolicited advertising material or telephone calls. The solicitation concern dimension included all concerns with regard to how consumers feel when organisations send unrequested advertising material to them: whether they think it is of interest to them; whether they approve if organisations which they have not done business with before communicate with them; whether they feel that too many organisations send them unsolicited communication; or whether they approve of organisations' using telephone calls to sell products and services to them.

The findings regarding solicitation concerns identified differences in terms of consumers' solicitation concerns and their manifest behaviours to protect their privacy. Consumers who exercise protective behaviour were more concerned about solicitation activities, compared to consumers who have not changed their behaviour to protect their privacy. Another finding pertaining to solicitation concerns was associated with consumers' personal experiences of invasions of privacy. The results showed that respondents who had been victims of privacy invasions were more concerned about solicitation than the non-victims. The findings also revealed a relationship between consumers' knowledge about information protection practices and solicitation concerns. The results indicated that consumers who did not have knowledge about information protection practices were more concerned about unsolicited communications from organisations.

The research findings further suggested differences between consumers who had purchased directly in the past year and those who had not purchased directly in terms of their solicitation concerns. The results indicated that direct shoppers and non-direct shoppers only differed significantly on the solicitation concern dimension. Respondents who had not purchased directly during the past year had higher privacy concerns with regard to the solicitation practices of organisations.

The empirical findings also revealed demographic differences between respondent groups in terms of the solicitation dimension. Older consumers reported higher solicitation concerns than younger consumers. English- and Afrikaans-speaking consumers showed higher solicitation concerns than Black African language consumers. Consumers with a middle to high level of education were more concerned about solicitation than consumers with a low level of education. High income consumers had higher solicitation concern levels than the middle and low income consumers.

8.4.1 Conclusions regarding the main findings on solicitation concerns

Many consumers perceive unsolicited communication as intrusive, signifying that their privacy has been invaded. Increasingly, consumers are becoming annoyed by telephone sales calls' interrupting their dinner, and regard the telephone as an intrusive marketing medium. Unsolicited communication is sent by organisations to market their products and services to consumers. In their eagerness to leverage technology and their databases of customer information, organisations have alienated consumers to the extent that most consumers fear that they will receive unwanted product offers. From a marketing point of view, an alarming majority of respondents in this study (94 per cent) expect that privacy protection policies have to make provision for consumers who would prefer not to receive unsolicited communication. This demonstrates their dissatisfaction with media intrusiveness into their lives. Moreover, respondents also indicated that they are willing to change their behaviour or adopt protective behaviour (such as requesting the removal of their information) if they feel that an organisation solicits them with (unwanted) communication.

Advances in computer technology, combined with lower communication costs, have made it much easier and cheaper for organisations to mail unsolicited advertising to consumers. Not only have the costs for using the traditional methods of direct mail and telephone solicitations decreased, but new communication media with especially low costs have recently appeared, such as fax transmission and e-mail. Although receiving these messages is 'costless' (t least to the marketer), consumers must spend time sorting through, reading and processing a variety of messages in order to find the goods, services and charities that they are interested in.

Many direct marketing organisations believe that more interaction with consumers will result in increased knowledge of consumers' buying patterns and will improve the organisations' future marketing actions. This view may lead to media intrusiveness, and may even be the reason why the respondents who were classified as 'non-direct shoppers' in this study had higher solicitation concerns than the direct shoppers. They

do not want to purchase directly, because they want to avoid organisations' intrusion into their lives with unsolicited communication, and therefore they have high solicitation concerns.

There are no laws that restrict access to consumers via the telephone, mail or fax in South Africa. The South African DMA has set up Media Preference Services (MPS) for South African consumers who want to eliminate unwanted calls or stop receiving mail or fax solicitations. Their database contains information about individuals who have asked to be excluded from mail, telephone and fax marketing (refer to Chapter 3, Section 3.3.1 for more detail on the MPS). Despite the best intentions of the DMA, this service does not address the solicitation problem. First, the majority of respondents in this study (79 per cent) were not aware that they could remove their information from direct marketing lists. Second, this service only includes some of the major national direct marketing lists – only providing a solution to part of the problem, since it only regulates the direct marketing industry. Third, adherence and access to this service is purely voluntary, with no legal obligation by organisations to honour the MPS, since it is only a Code of Practice. The results regarding direct purchasing behaviour in this study show that a minority of South African consumers have, for example, purchased products or services offered by a telephone call (14 per cent). This suggests an opportunity for direct marketers to proactively educate and influence expectations in respect of direct marketing practices. One way to achieve success is to send only wanted, relevant or appropriate communications to consumers.

The success of protective information practices depends on consumers' knowledge of these methods of protection, their willingness to use the facilities provided to them, and their actions to register complaints about offending organisations. The results of this study indicate that consumers who were aware of name removal procedures had lower solicitation concerns than those who were not aware of name removal procedures. If organisations inform and educate their customers on protective information practices, they will empower their customers to protect their own privacy by requesting the removal of their names from organisations' databases when they feel that they are

being solicited against their wishes. Consumers who do not know that they can remove their names from organisations' databases have higher solicitation concerns because their names are still on the contact lists of organisations, and they are probably inundated with unsolicited communication.

8.4.2 Implications of the main findings on solicitation concerns

Over-use of consumer lists or organisational databases can contribute to problems associated with unwanted and unsolicited communications. Organisations sending unsolicited messages impose a negative externality on consumers by distributing messages to consumers who may not want the products and services, but are forced to read the received message to establish whether they need what is offered. The consequence of unsolicited communication for organisations may be that consumers will stop reading any messages sent to them, thereby decreasing response rates. Response rates to bulk commercial e-mail are thought to be as low as 0.005 per cent. That means that the typical message appeals to 50 people and annoys 999 950 (France, 2002). The implication of the solicitation concerns is that marketers and organisations need to be more protective of their consumer lists. Direct marketers should subscribe and honour the MPS to demonstrate their commitment to consumer privacy and by removing from their lists consumers who do not wish to be contacted. Attention should also be given to informing and educating consumers about this protection option available in the direct marketing industry.

Consumer information is a valuable commodity and is therefore a source of power. Personal information privacy rights could have a significant impact on information-trading practices. Many consumers counteract their privacy concerns by refusing to provide permission to disclose their information to third parties and diminishing the marketing opportunities of the organisation which is dependent upon list availability. Organisations can consider placing ownership in the hands of consumers, recognising consumer ownership rights to personal information because consumers perceive these rights to exist and resent their violation. Personal information should be regarded as

property, and consumers should be able to control its dissemination and safeguard their personal privacy better.

If organisations do not respond to how much their intrusions annoy consumers, South African consumers may turn to the anti-marketing products that are currently emerging in the USA. Several electronic devices have been developed to screen telephone solicitation calls (refer to Chapter 3, Section 3.3.1.1 for more detail on these devices). In the hope of stemming the telemarketing tide, 28 states in the USA have adopted no-call lists for consumers who no longer wish to be harassed by incessant telephone solicitations. This no-call registry aims to prohibit telemarketers from sharing a consumer's billing information with other telemarketers, and blocking caller identification services or interfering with consumers who want to be on the no-call list (refer to Chapter 3, Section 3.3.1.1 for more detail).

The implication for organisations is that they will have to become more sensitive to privacy concerns, and exercise good judgement when conducting database marketing activities such as data mining. One way in which organisations may accomplish this is by using database marketing to cultivate their best customers carefully, rather than constantly to prospect by sending mass mailings to purchased customer lists.

8.4.3 Recommendations regarding solicitation concerns

Organisations will have to focus on a multi-faceted approach to address consumers' solicitation concerns. They should probably opt for a combination of endorsing the adoption of new technologies, consumer education and rigid enforcement of privacy policies. If a consumer asks an organisation to remove his or her information from its database, the organisation should respond to and honour such a request. As an organisational level, consumers need to be educated on how to protect their information, how to query information held in an organisation's database, and how to remove their information if they want to. At an industry level, consumers should be made aware of their privacy rights. Given that consumer knowledge of marketing

practices is a factor of how they perceive the industry, marketers need to allow consumers greater access to information. Consumers should be educated on acceptable and unacceptable behaviour in terms of data collection and utilisation by organisations.

The USA has moved closer towards addressing consumers' solicitation concerns pertaining to telemarketing. President Bush signed into law legislation in March 2003 creating a national do-not-call list intended to help consumers to block unwanted telemarketing calls. Telemarketers have to check the list every three months to establish who does not want to be called (Kieckhefer, 2003). If South African organisations do not address consumers' solicitation concerns themselves, the South African government may be forced to enact similar legislation to protect consumers from marketing intrusions.

Results from this study indicate that only 21 per cent of the respondents were aware of name removal options offered by organisations. This suggests that the marketing industry needs to implement fair information practices in two regards. First, individual organisations need to do better in informing their own customers about name removal options. Marketers may also need to develop new procedures for communicating with consumers who are aware of name removal procedures. Implementing such a policy can provide a source of competitive advantage. Second, consumers who have not shopped directly suggest that new methods are needed to educate consumers who do not participate in direct marketing about the ways their personal information is used by direct marketers, and about their options for exercising control over such use.

Many of the arguments about solicitation tend to focus on the issue of 'opt-in' versus 'opt-out'. With opt-out schemes, consumers have to take action to declare their unwillingness to receive unsolicited bulk mail from the organisation. If the system is opt-in, then organisations have to be able to show that consumers have given their consent to receive solicitations. Many organisations prefer the opt-out option, even though the opt-in system seems to be more consumer-friendly. Organisations that really have their

customers' interests at heart would employ an opt-in system, and only market to consumers who have given their consent to solicitations. The European Parliament recently voted to adopt opt-in requirements, putting Europe far ahead of other countries in acting against unsolicited communication (Gleick, 2003). The South African government may have to follow international trends in addressing solicitation concerns effectively.

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 spite of their privacy concerns, consumers are willing to part with their most sensitive and private information in return for certain benefits. 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.

8.5 MAIN FINDINGS RELATING TO GOVERNMENT PROTECTION

The fourth underlying privacy dimension identified by the research related to consumers' expectations in respect of the role of government in the protection of their information privacy. The government protection dimension included expectations relating to governmental activities to restrict the collection of personal information by organisations, to limit the use of personal information and to provide increased protection regarding the safety of personal information.

The empirical findings on government protection showed that there were differences between consumers in terms of their knowledge about information protection practices and their government protection expectations. The findings indicated that respondents who did not have knowledge about information protection practices had higher expectations from government in terms of protection. The only significant demographic difference found was between males and females, with females having higher expectation levels in terms of government protection.

The privacy protection dimension indicated that consumers argue that their personal information should be protected by government and/or legislation. The descriptive statistics demonstrated very high expectations (percentages ranging from 75 to 93) among the majority of South African respondents. Government protection measures can thus be seen as an issue that is of great importance to the majority of consumers, with very few and non-significant differences in the expectations of different respondent groups.

8.5.1 Conclusions regarding the main findings on government protection

Consumers in this study clearly indicated that that they perceive privacy protection to be the responsibility of government. Respondents specifically stated that they expect government to limit companies' collection and use of personal information only to that needed for a specific transaction, and that government must do more to protect the safety of personal information. It is thus evident that it is not only the global community that is forcing the South African government to adopt privacy legislation and actions (refer to Chapter 2), but that local consumers are also developing strong expectations regarding government's future role in the protection of information handling practices.

The findings suggested that consumers who have knowledge about information protection practices had lower government protection expectations. From this it can be deduced that consumers who are aware of name removal procedures do not expect government to protect their information privacy, since they believe that they can protect their own privacy by requesting the removal of their names from organisations' databases.

8.5.2 Implications of the main findings on government protection

As has been mentioned in Chapter 2, South Africa has not yet established formal data protection mechanisms and standardised privacy practices. Although the Law Commission in South Africa has implemented Project 124 to consider the development

of data privacy legislation in the near future (refer to Chapter 2, Section 2.6.2), there is at present no separate data privacy act in South Africa to address the relevant data issues. Consumers' high government protection expectations, as noted in this study, can be seen as a signal to the South African government that protection legislation is long overdue and would be embraced by consumers.

Many South African organisations are reactive in their management of privacy issues, waiting for an external threat before they implement cohesive policies. If organisations and industry groups fail to self-regulate effectively, then legislation is likely to be enacted to force compliance. Organisations are now faced with a situation where regulators can impose new laws that are more restrictive than self-regulatory programmes. Until self-regulation becomes effective, regulators will have to continue to consider new privacy and information-gathering legislation.

Organisations which put off complying with regulations are likely to have more regulatory mechanisms imposed on them. Such delays may not be conducive to a trusting relationship with consumers. Waiting for regulation may be a further signal to consumers that organisations will not protect their information unless forced to do so. At the outset, South African organisations intended to demonstrate that self-regulation was the answer to local consumer and government privacy concerns. The high level of information privacy concern that emerged in this study demonstrates that these programmes have failed to provide enforcement mechanisms and that consumers now expect government to address the issue.

Understanding the controls and processes around information flows can help an organisation to mitigate legal, regulatory and reputation risks. Posting a privacy policy delineating how personally identifiable information is treated is an external promise that, if the policy is not followed, the organisation can be exposed to consumer scrutiny, lawsuits, governmental regulators and other legislative actions. Moreover, organisations will be held accountable by consumers with whom they should build trust. Pro-actively setting up internal monitoring and management systems will help legal counsel, chief

privacy officers and risk-management staff to minimise the risk that privacy promises are not being honoured.

8.5.3 Recommendations regarding government protection

Based on this study's findings, effective self-regulation will require the establishment of guidelines which clearly delineate what types of personal information can legitimately be collected, how often information should be updated and who can have access. Visible steps, such as implementing periodic consumer reviews to ensure the accuracy of database information, also have merit. It is essential that consumers be made aware of self-regulatory actions and that they be educated about information practices in general. Without such commitment, it is likely that consumers will continue to voice their disgust with legitimate marketing information practices and look, instead, for governmental protection and legislative action. Organisations not only need to communicate their privacy policies, but also need to provide proof of their compliance. Enforcement mechanisms need to be built into self-regulatory models in order for consumer trust in practices to be established. Pro-active independent verification by a qualified accredited organisation can serve as an enforcement mechanism that can provide this assurance.

Organisations which are serious about protecting their customers' personal information should consider appointing a chief privacy officer (CPO). CPOs must keep track of their customer data, prevent misuse of data, and be knowledgeable about their data practices. According to the Association of Corporate Privacy Officers (ACPO) in the USA, the general duties of a CPO should include training employees regarding privacy, comparing the organisation's privacy policies with potential risks and filling the gaps, managing a customer-privacy dispute and verification process, and informing senior executives on how an organisation deals with privacy issues (Nash, 2000:62). If information privacy is not addressed effectively by local organisations' information handling practices, the South African government may reach a point where it has to compel South African organisations to employ privacy officers.

Consumers, organisations and policy-makers must work in unison to lessen consumer information privacy concerns. Government needs to emphasise that finding a balance between organisations' information needs and consumers' privacy concerns necessitates compromises. Consumers and organisations must be reminded that privacy issues and concerns cannot be considered in a vacuum, especially in the commercial environment, since privacy can clash with freedom of speech. However, if industry self-regulation efforts are not effective, then mandatory governmental regulations will be necessary.

The South African government and South African businesses have to realise that a lack of proper data protection can have consequences for future transactions. Much international legislation forbids the transfer of personal data to a country (such as South Africa) that does not provide a level of protection similar to its own. Therefore, it is quite likely that South African organisations may be denied access to information from their own subsidiaries or other organisations located in such countries. The South African government has to realise that adequate privacy protection is increasingly becoming a necessary condition for being on the global information highway. A lack of proper regulatory frameworks may have far-reaching implications if South Africa fails to comply with existing global regulations. It is hoped that Project 124 Committee (currently investigating the privacy and data protection issue with the aim of improving existing legislation and adding new legislation) will address all the relevant data protection issues to resolve the current lack of consumer trust.

8.6 MAIN FINDINGS RELATING TO PRIVACY SEGMENTS

A United States Privacy Segmentation Index divided the American public into three privacy segments labelled 'Privacy Fundamentalists', 'Privacy Unconcerned' and 'Privacy Pragmatists'. The majority of Americans are seen to be in the Privacy Pragmatist segment. As has been mentioned in Chapter 7 (Section 7.4.1.4), the same privacy index was used in this study, with similar results. Table 8.1 below provides a

comparison between the percentages of American versus South African respondents in the different privacy segments.

Table 8.1 Privacy Segmentation Index comparison

PRIVACY SEGMENTS	USA 1999[1] %	USA 2000[1] %	USA 2001[1] %	SA 2002 %
Privacy Fundamentalists	25	25	34	30
Privacy Unconcerned	20	12	8	11
Privacy Pragmatists	55	63	58	59

Source[1]: Harris Interactive. 2002b. Privacy on and off the Internet: what consumers want. **Privacy & American Business**. Study no 15229:20-22.

8.6.1 Conclusions, implications and recommendations based on findings relating to privacy segments

The purpose of using the Privacy Segmentation Index in this study was to develop a better understanding of the distribution of South African consumers in terms of privacy concerns, and to compare them to consumers in the USA. Contrary to common belief, the results indicate that South African consumers do not differ from Americans in their views of and approach to information privacy. The findings show that information privacy is a salient and relevant issue to many people, and this supports the conclusion of international studies that consumers world-wide are concerned about threats to their personal privacy. The message of the results from this index to South African organisations and government is that a substantial proportion of consumers are moderately to very concerned about information privacy.

Similar to the situation in the USA, the majority of South Africans were in the 'Privacy Pragmatist' segment (59 per cent). Consumers in this segment have balanced attitudes regarding information privacy. The 'Privacy Fundamentalist' segment represents 30 per cent of the South African public, versus 34 per cent of the American public. A minority of

respondents were in the 'Privacy Unconcerned' segment (as is also the case with the American consumers). Consumers in this segment are not concerned about the level of control they have over their personal information; they think organisations handle their personal information in a proper and confidential way; and they see no need for creating laws to protect their privacy. Consumers in this segment have very low or no information privacy concerns.

Almost one-third of the consumers surveyed fell into the 'very concerned' category. Consumers in this segment regard information privacy as something with an especially high value, and have very high privacy concerns. This group favours the enactment of strong laws to secure privacy rights and to control organisational discretion. These are consumers who express the maximum level of privacy concern. They believe that consumers have lost all control over how information is collected and used by organisations, that organisations do not handle personal information in a proper and confidential way, and that existing laws and organisational practices do not provide a reasonable level of protection. The large number of consumers who are moderately to very concerned about information privacy (89 per cent) should alert South African organisations to the fact that this issue is very real and should be addressed. Since the Privacy Index indicates that the concerns of consumers in this study are on a par with the privacy concerns of consumers in the USA, South Africans may expect that the privacy standards of the USA may set the pace for South African legislation. It is relatively clear that organisations which rely on personal information need to take proactive steps to alleviate consumer privacy concerns and to reduce the desire for legislative action.

8.7 SUMMARY OF RECOMMENDATIONS

The intention of this study was to develop a better understanding of the specific nature of consumers' information privacy concerns. The results from the study suggest that the ability to gather and maintain personal information does not necessarily imply that organisations are successful in establishing meaningful relationships with consumers.

Organisations need to be cautious of how they use the collected information and to collect only as much information as is really required to develop effective relationships with their customers. The focus of relationship marketing is establishing and enhancing a long-term, mutually beneficial relationship between consumers and the organisation. Such a relationship assumes that the organisation is oriented toward customer retention and developing a unique relationship with each individual customer and creating trust. To achieve this, organisations must have a greater organisational understanding of consumers' information privacy concerns. Organisations engaged, or interested in, relationship marketing must take action to ensure that the personal information of their consumers is protected, both internally and externally.

Several recommendations regarding information privacy can be made to facilitate relational exchanges between organisations and consumers. First, a commitment to information privacy must be made at a corporate level. There must be a corporate-wide initiative with input and enforcement from all functions in the organisation.

Second, the organisation has to develop a privacy policy that encompasses all processes and procedures. Privacy policies must start with 'fair information practices', with an opt-out option, whereby customers may refuse permission for organisations to use their personally identifiable data. Customers need the right to review and correct their data. Consumers should also be offered an opportunity to inspect their information for errors and correct errors if they decide to opt in. Proper privacy protection policies would shift some of the control of personal information to consumers, and would make certain marketer information-handling practices mandatory.

Third, organisations must provide consumers with many more opportunities to engage in consensual information exchange, whereby consumers could indicate what type of information they wish to provide and release for marketing purposes and to which organisations that information could be disseminated. Organisations should also be required to maintain records of 'do-not-contact' requests. By using increased opt-in or opt-out opportunities, consumers would receive a greater proportion of marketing offers

that are relevant to their needs and interests, and would not be excluded from the flow of marketing information. This could benefit organisations too, because this situation would effectively reduce the number of hostile, uninterested and inappropriate prospects, leading to an improvement in organisations' targeting efforts.

Fourth, organisations have to create an industry standard for addressing the information privacy issue. Consumers need unambiguous, easy-to-read and understand statements that explain what information is collected, for what purposes it is to be used, and with whom it is or will be shared. This should be concurrent with a process of educating consumers and promoting privacy efforts. It is important that organisations maintain an ongoing dialogue with consumers.

Finally, organisations can consider undertaking regular independent audits by third-party experts to verify that data are securely stored and used only for the purposes disclosed, that access is restricted to employees authorised to handle the information, and that systems are intact to guard against leakage or corruption.

South African organisations will have to make a decision on the type of privacy standard they want. The choice may depend on whether an organisation is interested in being faultless, meeting customer expectations or becoming an acknowledged leader in protecting consumer privacy. This suggests three different privacy standards: the legal compliance approach, the customer expectation approach and the privacy leadership approach.

- The legal compliance approach aims to keep the organisation within the law, but does not use resources to meet a higher standard. With this approach, an organisation may lose customers who are privacy sensitive (89 per cent, according to Table 8.1).
- The customer expectation approach implies a higher standard than legal compliance, and is probably a prerequisite for an organisation with a customer relationship management programme. Complying with customer permission creates a new level of complexity for customer data management. The rewards are higher

for successful organisations, but the risk of mistakes is also higher. One limitation associated with this approach is that it could increase organisations' administrative costs associated with list management and opt-out compliance. However, these costs could be discounted against the savings associated with a reduction in the volume of inappropriate marketing contacts and improved response rates.

- The final approach, privacy leadership, requires high public exposure of an organisation's privacy commitment and demands extremely high compliance capabilities. Privacy leadership involves setting the highest standards of respect for and integrity of personal information, applying it to all customers, promoting the standards as a competitive edge and ensuring that the compliance is sound.

If an organisation wants to focus on building strong relationships with customers, it is imperative that it should seriously move beyond a legal compliance approach. An organisation can decide to start its privacy programme at a compliance level and improve consistently. The decision should be based on what level or standard the organisation wants to achieve after the privacy initiative has been fully implemented. With new technology, certain issues arise, such as the protection of personal information, the security of databases, the integrity and authenticity of information, and the responsibility for information flowing through the system. The benefits of new technology should result in improved security systems, and an enriched environment to protect customer information.

Since information privacy is becoming a global issue, a lack of privacy protection can have an impact on the South African economy. South Africa is lagging behind the rest of the world in terms of data protection, despite legislative action already being instituted by the South African government. The information privacy challenge to the South African government is to find a proper balance between the different competing social and economic interests when drafting legislation. The recommendation to the South African government is that it should use a multi-faceted approach to address information privacy effectively. This will involve a combination of education to organisations and consumers, supporting self-regulation efforts, drafting proper national legislation, and

setting adequate privacy protection criteria in line with international regulatory frameworks.

8.8 LIMITATIONS AND RECOMMENDATIONS FOR FUTURE RESEARCH

The present study attempted to make a significant contribution to the body of knowledge on consumer information privacy in South Africa, but certain areas still need to be explored or expanded.

8.8.1 Limitations

As a first study, there are several limitations that need to be recognised.

- Due to a lack of literature on information privacy in a South African environment, the theory relied very strongly on literature from other countries, especially the USA.
- The sampling frame for this study included all South African households with listed Telkom telephone numbers. Therefore, the results cannot be generalised to all consumers throughout the country, but is only representative of South Africans with Telkom landlines.
- The length of the telephone interviews (approximately 25 minutes) may have had an effect on the quality of the responses. Many consumers did not want to participate in the study due to the length of the questionnaire.

While the sample frame limits the external validity of the research findings, the high level of consumer information privacy concerns found in the study, is consistent with that found in international studies. Despite these limitations, the findings from this study provide guidance to organisations on adequate information practices and also facilitate addressing consumers' concerns on information privacy effectively.

8.8.2 Recommendations for future research

Recommendations for future research on consumer information privacy include the following:

- The disaggregation of overall information privacy concerns into specific dimensions such as privacy protection, information misuse, solicitation and government protection can be refined in future research efforts. There is a dire need for a refined framework for information privacy, especially for research that addresses the conceptual antecedents and consequences of various concerns. A conceptual framework could assess the degree to which each privacy dimension identified is subject to management control and influence.
- Due to the multi-faceted nature of information privacy, future research can investigate the determinants or antecedents of buyer-seller relationships. Since the aim of the present study was mainly to uncover underlying dimensions, the study did not make provision for relationships between different variables or dimensions. As this research has uncovered the basic underlying dimensions of information privacy, future research should confirm to what extent the privacy dimensions are linked. Future research can also test relationships between information privacy beliefs, attitudes, intent and behaviour. Structural equation modeling can be a useful tool to test such conceptual relationships.
- The privacy scale developed in this study should be tested across a variety of industries in order to confirm the scale's ability to produce useful results as an indicator of privacy concerns in those industries. The high reliabilities and consistent factor structure would benefit from tests across several independent samples to provide support for its trait validity. Information privacy may yield different information privacy concerns when measured in different industries, such as the banking or the medical industry. At an industry-wide level, industry comparisons can be made to determine whether progress relative to a stipulated industry standard has been made. Industries can be compared to determine how consumers assess them compared to information privacy concerns.

- The issue of name removal options merits additional research, because name removal is a key to ensuring that the implied social contract between marketers and consumers is fair. In this study, consumers' awareness of name removal procedures was measured by a single, dichotomous variable. This variable did not explain how consumers learn about name removal procedures. Future research may investigate the relationship between consumer awareness of name removal and specific issues such as the impact of privacy policies on their awareness, as well as the effectiveness of name removal options for protection. Future research should also investigate what proportion of the consumers who are aware of name removal procedures choose to exercise the option, and the reasons therefor.
- Longitudinal studies are recommended (given the ever-changing nature of the marketing environment) to provide an update for the research findings. In the case of information privacy, the growth of electronic information collection systems, continued debate on information collection and use issues, and continued regulatory and industry-wide efforts to address consumer privacy concerns necessitate the examination of consumer concerns on a continuous basis.
- The rapid growth of the Internet and e-commerce suggests that future research should focus on the electronic, computer-based marketing environment. The Internet and the World Wide Web as a marketing environment create new and often invisible methods for collecting and using personal information, along with several issues involving transactional security.
- It is important to note that a single study does not establish construct validity. Therefore, future research should be conducted to cross-validate the current findings. Furthermore, to test whether the scale is stable over time, the test-retest reliability should be examined by administering the measure to similar respondents in future.
- Since the South African government is planning to introduce data protection legislation in the near future, future research can monitor whether the new legislation leads to a decrease in information privacy concern and whether it provides constructive privacy protection to South African consumers (addressing the issues raised by consumers in this study).

8.9 EVALUATION OF THE OBJECTIVES SET VERSUS THE RESEARCH RESULTS

The empirical results as presented in Chapter 7 enabled the researcher to evaluate (support) the research hypotheses and attained the different formulated research objectives. In this section, the primary and secondary objectives of the study are compared to the outcome of the research findings. To structure the discussion, each objective (see Chapter 5, Section 5.3) of the study is stated, after which the research results are summarised to indicate whether the study objectives have been met.

The first secondary objective (SO1) was to determine the underlying dimensions of information privacy concerns. Exploratory factor analysis uncovered four main underlying information privacy dimensions, namely privacy protection, information misuse, solicitation and government protection. These dimensions provided valuable insight into South African consumers' concerns on information privacy. Very high levels of concern were found, indicating that South Africans know what information privacy is all about, and that they are not happy with some of the current information practices employed by organisations. They have also indicated that they expect the South African government to intervene and protect their information privacy in future. This objective has been satisfied.

The second secondary objective (SO2) was to ascertain whether there are differences between consumers' manifest behaviours to protect their privacy and their privacy concerns. Hypothesis testing revealed that consumers who have acted to protect their information privacy have higher privacy concerns in terms of privacy protection, information misuse and solicitation practices. This secondary objective has been met.

The third secondary objective (SO3) was to establish whether there are differences between consumers in terms of their personal experiences of invasions of privacy and their privacy concerns. The research results indicated that consumers who had been

victims of privacy invasions had more information misuse and solicitation concerns than consumers who had not been victims of invasions of privacy. Therefore, the objective has been achieved.

The fourth secondary objective (SO4) was to establish the dependency between gender and personal experiences of invasions of privacy. The findings of the empirical testing were that males are more likely to perceive themselves as victims of privacy invasion than females. There is thus a dependence between gender and personal experiences of privacy invasion. Thus, the set objective has been met.

The fifth secondary objective (SO5) was to establish differences between consumers in terms of their knowledge about information protection practices and their privacy concerns. The research results uncovered several significant differences. Consumers who had more knowledge about information protection practices had lower levels of information misuse, solicitation and government protection concern than consumers who did not have knowledge about information protection practices. This objective has been satisfactorily addressed.

The sixth secondary objective (SO6) was to establish the dependency between age and knowledge about information protection practices. No dependence between age and knowledge about information protection practices was found in this study. It is surmised that older consumers did not necessarily know more about information practices than younger consumers. Sufficient information was gleaned to state that this objective has been reached.

The seventh secondary objective (SO7) was to determine the dependency between education and knowledge about information protection practices. No association was established between consumers' levels of education and their knowledge of information protection practices. Their level of education had no impact on how much consumers knew about the information protection practices of organisations. The set objective has therefore been met.

The eighth secondary objective (SO8) was to ascertain whether there are differences between consumers' Internet usage and their privacy concerns. The research results indicate that consumers' information misuse concerns were related to whether they use the Internet for transactions or not. Consumers who had been involved in Internet transactions had higher levels of information misuse concerns than consumers who had not been involved in Internet transactions. This is in line with increased concerns among online users world-wide. Thus, this secondary objective has been satisfied.

The ninth secondary objective (SO9) was to establish whether there are differences between consumers' direct purchasing behaviour and their privacy concerns. Direct purchasing behaviour seemed to have an impact on consumers' privacy concerns, specifically in respect of solicitation concerns. Since direct marketers use solicited communication to market their products and services, consumers who had not purchased directly in the past year were the most concerned about solicitation by organisations. This secondary objective has been achieved.

The tenth secondary objective (SO10) was to classify consumers into different privacy sensitive segments based on their general privacy concerns. South African consumers were classified into one of three privacy sensitive segments, with the majority of South Africans belonging to the 'Privacy Pragmatist' segment. The percentage of consumers in each segment is relatively similar to findings on American privacy segments. This seems to suggest that consumers in different countries do not differ in respect of their information privacy, and that information privacy can be regarded as a uniform concern. This objective has been met.

The final secondary objective (SO11) was to identify differences between consumers in terms of their demographic characteristics and their privacy concerns. Several demographic characteristics were uncovered. The main differences between different demographic groups were found to be in terms of their age, home language, income, gender, levels of education and employment status. In the **privacy protection**

dimension, older consumers were more concerned than younger consumers; English- and Afrikaans-speaking consumers were more concerned than consumers from other language groups; middle and high income groups were more concerned than lower income consumers; and females were more concerned than males. In the **information misuse dimension**, older consumers, English-speaking consumers and high income groups were more concerned; middle and high level of education groups were more concerned, as were employed consumers. In the **solicitation dimension**, older consumers, English-speaking consumers and high income groups displayed higher levels of concern. Low and middle level of education groups were less concerned. In the **government protection dimension**, the only group that showed higher levels of concern was females as opposed to males.

The eleven above-mentioned secondary objectives were formulated in support of the primary objective, namely to identify and explore the information privacy concerns of South African consumers in a commercial environment. The research results has succeeded in meeting the primary research objective: four information privacy concerns of South African consumers were identified by means of the exploratory factor analysis, and these four information privacy concerns were explored by searching for dependencies, relationships or differences in terms of different behavioural and demographic characteristics.

8.10 SUMMARY

This study was conducted to investigate the underlying dimensions of South African consumers' information privacy concerns. The primary and secondary objectives were achieved and it can therefore be concluded that the results added value to the body of knowledge on marketing theory in general, and on information privacy theory in particular. The study has contributed to marketing literature in several ways.

First, the study has shed new light on information privacy concerns among South African consumers. It provides valuable insights into the information privacy concern dimensions of consumers.

Second, the study explored different relationships between information privacy, and behavioural and demographic variables. The research hypotheses indicated differences between groups in terms of their information privacy concerns.

Third, the study provided useful guidelines to allow for international comparison in terms of information privacy concerns. The results also indicate to the South African government that information privacy is a salient issue that needs to be addressed.

Finally, the findings of the study have established a foundation for future research into other important issues surrounding the information privacy issue.

Organisations and consumers should share consumer information in such a way that the interests of both are served, without unreasonably burdening or compromising each other's interests. Recognising that consumers have an interest in, and proprietorial rights to their personal information could improve marketing contact strategies and could help to reduce the negative concerns associated with current marketing practices. Organisations should take advantage of database technology to store and use information that indicates what kind of incentives and/or approaches will induce consumers to feel more comfortable and confident in maintaining relationships with organisations. When organisations use personal information in a way that offends consumers, the perception of marketing as a whole suffers. Recognising that consumers perceive that they have ownership of their personal information, and sharing that information in a way that is respectful, relevant and beneficial is a way to build improved relationships with and trust from consumers and to improve consumer satisfaction and industry performance.