UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

SOUTH AFRICAN CONSUMERS' INFORMATION PRIVACY CONCERNS: AN INVESTIGATION IN A COMMERCIAL ENVIRONMENT

by

YOLANDA JORDAAN

Submitted in fulfilment of the requirements for the degree

DOCTOR COMMERCII (MARKETING MANAGEMENT)

in the

DEPARTMENT OF MARKETING AND COMMUNICATION MANAGEMENT

FACULTY OF ECONOMIC AND MANAGEMENT SCIENCES

at the

UNIVERSITY OF PRETORIA

PROMOTER: PROFESSOR PJ DU PLESSIS

Pretoria, South Africa **April 2003**

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

ACKNOWLEDGEMENTS / DANKBETUIGINGS

'n Opregte dank aan al die persone wat op een of ander wyse 'n bydrae gelewer het tot die voltooiing van hierdie studie. In besonder wil ek my dank en waardering uitspreek teenoor die volgende:

- My Hemelse Vader wat my die deursettingsvermoë gegee het om hierdie studie suksesvol te kon voltooi. Ek is elke dag deur Sy krag gedra en weet hierdie studie is een van die grootste genades wat ek nog uit Sy hand ontvang het. Ek loof Hom vir die geleentheid op my pad en die leerervaring wat my nederig kon maak.
- My studieleier en mentor, Professor Flip du Plessis, wat deurlopende ondersteuning en aanmoediging gebied het. Hy het geen moeite ontsien om sy hulp op verskeie terreine van die studie aan te bied nie. Dis nie net sy bekwame leiding, motivering, entoesiasme, geduld en positiwiteit wat my gedryf om 'n sukses van hierdie studie te maak nie, maar veral die feit dat hy in my as mens belanggestel het.
- My eggenoot, André, vir sy bystand en ondersteuning tydens die studie. Dankie dat jy so goed verstaan het. Jou aanmoediging wat ek te midde van jou talryke opofferings ontvang het, sal my altyd bybly. Ek dra hierdie proefskrif aan jou op en bedank jou vir jou liefde en ondersteuning elke dag van my lewe.
- My wonderlike ouers vir jare van gewaardeerde belangstelling in my studieloopbaan. Dit was veral hulle geloof in my vermoëns wat my gemotiveer het om verder te studeer. My skoonouers vir hulle deurlopende belangstelling en aanmoediging gedurende hierdie studie. Dankie aan beide ouerpare wat baie maande van onsosiale gedrag verduur het, maar dit altyd met begrip en geduld verdra het.
- Ernst & Young, spesifiek Jaco van der Walt, wat die data-insamelingkostes geborg het en daardeur 'n omvangryke studie moontlik gemaak het. Die Buro vir Marknavorsing, spesifiek Jan Dorfling, wat die nasionale telefoniese onderhoude so sorgvuldig geadministreer en bestuur het.
- Die Departement Bemarkings- en Kommunikasiebestuur wat met behulp van werksverligting hierdie groot taak uitvoerbaar gemaak het. Veral ook aan al my kollegas wat op een of ander wyse harder moes werk in tye wat ek nie beskikbaar was nie.
- Rina Owen vir haar gespesialiseerde navorsingsondersteuning en hulp met die data-verwerking, asook Jeanette Pauw wat statistiese ondersteuning gebied het.

SYNOPSIS

More consumers are becoming concerned about the protection of their information privacy by organisations. Emerging technologies are allowing the amount of personal information which organisations collect, store, use and exchange to grow exponentially. Consumers increasingly display concern about intrusions on their privacy by marketers, and many want to protect the confidentiality of their personal information. At the same time, legislation governing privacy are proliferating world-wide. These regulations vary from country to country and change constantly. Within the current privacy sensitive environment, a thorough understanding of consumers' information privacy concerns can be critical to any organisation's profitability and sustainable competitive advantage. However, there is a lack of knowledge about, and understanding of the information privacy concerns of South African consumers.

The primary objective of this study was to identify and explore the information privacy concerns of South African consumers in a commercial environment. The secondary research objectives included in this study pertained to the underlying dimensions of information privacy concerns and required an exploration of the different information privacy concerns in relation to specific consumer behaviour actions and demographic characteristics.

Primary research data was collected by means of national telephone interviews. A systematic sampling procedure was used to identify a sample frame of South African households with a telephone number listed in a Telkom telephone directory. A total of 800 interviews were conducted with adults in the selected households. The measurement instrument was purified by means of exploratory factor analysis, reliability measurement and confirmatory factor analysis. The hypothesis testing consisted mainly of chi-square tests and multivariate analysis of variance.

The study uncovered four information privacy dimensions among South African consumers, namely concerns about privacy protection, information misuse, solicitation

and government protection. Some of the other findings include the fact that 89 per cent of South African consumers are moderately to very concerned about information privacy; consumers who make use of Internet transactions are more concerned about the misuse of their information than consumers who do not use the Internet for transactions; and the majority of consumers expect the South African government to protect their information privacy.

The implications of the study are that government needs to find a balance between organisations' information needs and consumers' privacy concerns, and that organisations have a responsibility to communicate how they will use consumer information to ensure that privacy is protected. One of the recommendations is that the general premise for South African organisations should be to act as if consumers have joint ownership rights to data collected about them. This should motivate organisations to implement proper privacy practices and to develop visible privacy policies that are easy to understand. Organisations searching for the reward of active consumer participation and strong trusting relationships should treat personal information as a strategic asset.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
BACKGROUND AND OVERVIEW OF THE STUDY

1.1 INTRODUCTION

The right to privacy is an issue that is increasingly raised all around the world. Consumer privacy issues are not new; and many studies report on findings which illustrate consumers' concern about how personal data are used by the government and, more recently, by private organisations (Nowak & Phelps, 1992:28; Wang & Petrison, 1993:7) Culnan, 1993:341; Loro, 1995:32; Petrison & Wang, 1995:19; Louis Harris & Associates & Westin, 1998a:ix; Milne & Boza,1999:5; Phelps, Nowak & Ferrell, 2000:27; Udo, 2001:165; Westin, 2002:16). An increasing number of consumers are expressing a desire to be left alone and a desire to protect their confidentiality (Agre & Rotenberg, 1998:226; Devenish, 1999:146; Hagel & Singer, 1999:7; Longley & Shain, 1988:268; Joshi, Aref, Ghafoor & Spafford, 2001:40). The Internet has grown considerably during the past decade, particularly with respect to its use as a tool for communication, entertainment and market place exchange. This rapid growth has been accompanied by concern regarding the collection, use and dissemination of consumer information by marketers. The consumer privacy issue is becoming more urgent as many consumers are involved in marketing transactions, and, progressively, more marketers rely on technology in their day-to-day operations.

This chapter sets out background which serves as an overview of the topic to be researched. This is followed by the identification of the research problem and a discussion of the identified research objectives. The importance and scope of the study are the presented, whereafter the research design is discussed briefly. Finally, a chapter outline of the study is given, indicating the main discussion areas in each chapter of the thesis.

1.2 BACKGROUND

One of the earliest definitions of privacy was documented by Warren and Brandeis (1890:193) in the 1800s. They argued that the right to life refers to the right to enjoy life, including the right to be 'let alone'. Several definitions on privacy have emerged since the first definition by Warren and Brandeis. In South Africa, privacy has been defined by Neethling, Potgieter and Visser (1996:36) as 'an individual condition of life characterised by exclusion from publicity'. This condition includes all those personal facts which the person himself or herself at the relevant time determines should be excluded from the knowledge of outsiders, and in respect of which (s)he evidences a will for privacy. Violations of privacy can refer to an invasion of a person's private life or relate to the acquisition and disclosure of personal information (Devenish, 1999:145).

Underlying any definition of information privacy is an understanding that an individual's interests need to be balanced with those of society at large. Integrative social contract theory provides a means for understanding the current tensions between organisations and consumers regarding privacy. When marketing transactions are viewed as an implied social contract, consumers provide personal information in exchange for receiving solicitations and other information, based on an expectation that their personal information will be managed and protected in a responsible fashion (Milne & Gordon, 1994:206).

The perceived threats posed by new computerised record-keeping systems have contributed to bringing the issue of privacy to public attention in the United States of America (USA) in the 1960s. During this period, according to Culnan (1993:344), two books were published on the issue, namely Alan Westin's (1967) *Privacy and Freedom*, and Arthur Miller's (1971) *The Assault on Privacy*. In the late 1980s, information privacy again surfaced as a public issue, fuelled by the coming of age of both database marketing and telemarketing. Information technologies that promoted the collection, analysis and exchange of detailed personal information facilitated the compilation of

detailed personal profiles, causing the public once again to focus its attention on privacy (Cohen, 1991:5).

The beginning of the information age has increased the importance of personal data protection to a level where governments and international organisations around the world have been forced to adopt privacy legislation (Holvast, Madsen & Roth, 2001:1). In 2000, the South African Law Commission requested the Minister for Justice and Constitutional Development to introduce privacy and data protection legislation in South Africa as soon as possible. The Minister approved the inclusion of the investigation in the Commission's programme and Project 124 was launched to investigate the privacy and data protection issue with the aim of improving and adding new legislation as soon as possible (Mokgoro, 2000:10-22).

The world economic system's transformation from a dominantly mass-production model to a mass-customisation model is seen as creating an enormous demand for detailed data on consumer behaviour. If goods and services are to be customised, it appears to be necessary for organisations to have access to detailed customer information. Increasing fragmentation of mass audiences has also created a demand for data about the actual and potential users of specialised media channels (Agre & Rotenberg, 1998:277).

Many people perceive there to be a threat to their individual privacy owing to the staggering and increasing power of information-processing technology used to collect a great deal of information about them. Whether this information is accurate, relevant or complete or not, it is stored, analysed, interpreted, compared and exchanged at high speed, and often the individual has no knowledge or control over the information. While organisations may claim that they apply tight security and confidentiality controls over the data, these measures are often instituted mainly for the benefit of the organisation and may provide little protection to the individual who is the subject of the data (Collier, 1995:41). From a marketing perspective, consumer privacy thus revolves around the

buyer's ability to limit the accumulation and dissemination of psychographic and demographic data relating to a specific marketing transaction (Goodwin, 1991:1).

Much of the attention to privacy issues has recently focused on the Internet, and the opportunity that the Internet affords organisations and government to collect extensive information about citizens. The rise of e-commerce, combined with sophisticated data-mining software, has made it easy and affordable to share information across a network or to cross-reference information in a meaningful way (Massey, 2000:19).

An increasing number of consumers are expressing a desire to be 'left alone' and a desire to protect their confidentiality (Agre & Rotenberg, 1998:226; Devenish, 1999:146; Hagel & Singer, 1999:7; Longley & Shain, 1988:268; Joshi *et al.*, 2001:40). Many consumers have experienced quite distinctly and directly the potential dangers of unrestricted gathering, processing and dissemination of personal data, and now desire to keep their personal information more private (Agre & Rotenberg, 1998:225). Another privacy concern of consumers is media intrusiveness, and they state that they would prefer to be left alone. Consumers have little or no control over the prospecting efforts of organisations. The sheer volume of direct mail, phone calls and e-mails they receive relates to the physical intrusion of marketing communications into the daily lives of consumers (Katzenstein & Sachs, 1992:71; O'Malley, Patterson & Evans, 1999:427). As a corollary to these personal experiences, more consumers request individual privacy and data protection rights, above and beyond legislative attempts to control and regulate certain data processing technology.

There has been a well-documented increase in consumer privacy attitudes. There has been a shift from the issue's being a modest concern expressed by a minority of consumers in the 1980s to its being a matter that is intensely debated and desired by more than three quarters of American consumers in 2001 (Nowak & Phelps, 1992:28; Culnan, 1993:341; Loro, 1995:32; Louis Harris & Associates & Westin, 1998:ix; Westin, 2002:16). The increased perception of an erosion of privacy is primarily due to the

proliferation of information technologies, which provides scope for, and the potential ability of, managers to intrude in the private domain of consumers.

The information revolution, moreover, opens up important public policy issues, as organisations are increasingly building comprehensive consumer databases and applying sophisticated data-mining techniques to target consumers. Organisations have good reason to collect information about customers. It enables them to target their most valuable prospects more effectively, to tailor their offerings to individual needs, to improve customer satisfaction and retention, and to identify opportunities for new products or services. However, many consumers have realised that the information they have divulged freely through their commercial transactions, financial arrangements and survey responses has value and that they receive very little in exchange for that value (Hagel & Rayport, 1997:53-4).

More consumers are demanding that their information be used to enhance their experiences and that the information is not used in ways that abuse a privileged relationship (Mabley, 1999:1). Yudelson (1999:63) defines marketing as activities that aim to influence voluntary exchange transactions in a wide range of settings and situations where both parties may look beyond the specific exchange transaction to the development of a mutually beneficial relationship over an extended period of time. If marketers want to look beyond exchange transactions and want to develop long-term relationships, they need to understand the problem areas surrounding information privacy. The next section in this study describes the problem statement that provides the rationale for a deeper investigation into the topic of consumer information privacy.

1.3 PROBLEM STATEMENT

The concept of information privacy has shifted in the space of a generation from a civil and political rights issue to a consumer rights issue underpinned by the principles of data protection (Agre & Rotenberg, 1998:143). There is ample evidence to suggest that consumers world-wide recognise a problem of lack of information privacy and control

over personal information, once such information has been divulged to various organisations. Consumer attitudes about privacy have been researched in various countries and have been addressed in public opinion surveys. Studies have been done from the perspective of a number of disciplines, including law, political science, sociology and psychology. Although some reference is made to some of the most important international studies on information privacy in this section, a detailed discussion can be found in Chapter 5.

Most international studies indicate that information privacy is an important concern to many consumers. The findings of a study by Nowak and Phelps (1992:28) indicate that privacy is an important concern and is affected by the type of practice and the specificity of information. The findings of a study by Wang and Petrison (1993:7) demonstrate that certain consumers (particularly in the older age groups) are more negative about potential threats to their privacy than others. The results of a study by Culnan (1993:341) show that consumers who believe they do not have control over their personal information are more concerned about privacy. Phelps, Gonzenbach and Johnson (1994:9) report that public concern about privacy was high even before increased media coverage in the mid-1980s, and they argue that the dramatic increases in the frequency of media coverage have little relation to public salience. Loro (1995:32) contends that rising consumer concerns about privacy are forcing organisations to utilise the information in their databases to the benefit of consumers. Another study on privacy concerns and consumer choices, done in 1998, analysed privacy attitudes and concerns, concluding that concern over threats to personal privacy remains at very high levels and is increasing (Louis Harris & Associates & Westin, 1998:ix). The findings of a study by Sheehan and Hoy (1999:37) indicate that as privacy concerns increased, respondents reported that they were less likely to provide personal information to organisations.

Various studies have investigated cross-cultural differences with regard to consumer privacy. The findings of a comparative study by Petrison and Wang (1995:19) 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 (1996:34) concluded that Japanese respondents express a stronger concern about privacy issues than United States respondents do. The IBM-Harris 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 & Westin, 2000:5).

Several studies propose ways to decrease high levels of consumer privacy concern. Nowak and Phelps (1997:94) 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'[1] opportunities. Milne and Boza (1999:5) have established that organisations can improve consumer trust by managing their personal information better, which reduces concern about privacy. Phelps *et al.* (2000:27) suggest that privacy concerns can be reduced by providing consumers with more control over the initial gathering and subsequent dissemination of personal information.

Recent international research studies have focused on privacy in an online environment. The results of a study by Udo (2001:165) indicate that privacy and security concerns are the number one reason that web users are not purchasing over the web. Harris Interactive (2001a, 2001b, 2001c) also conducted a series of three surveys on consumer privacy attitudes and behaviours. Their findings are relatively consistent across all three surveys, indicating that consumers are willing to provide both online and offline organisations with basic information, but are more protective of personal information and are less comfortable sharing more sensitive information.

[1] An 'opt-out' opportunity means that an individual can specify that (s)he does not want to receive particular offers at his or her address, or at other contact points.

Four previous studies have measured different aspects of privacy in the South African environment. The first study was conducted to determine whether there is a correlation between the manner in which individuals transact consumer activities, and the acceptance of the use of personal data for marketing purposes (Fowler, 1995:5). However, although research objectives were formulated, no hypothesis testing was done and no results were reported in this study, limiting the conclusions regarding the correlation between consumer activity and use of personal data for marketing purposes. In 1996, another study was conducted by Daya (1996:32), who investigated the secondary use of information within South African banking institutions. On the basis of his findings, he pointed out that banks lack comprehensive policies regulating access to and the distribution of personal data.

In a third South African survey, Mann (1997:49) developed a privacy scale by investigating a variety of factors that might affect consumer concern regarding information privacy. After a refinement process, Mann developed a 19-item scale to measure privacy concerns, dividing consumer concerns into five dimensions: (1) willingness to provide information; (2) perception of the integrity of information provided by sales staff; (3) requirement for product information regarding quality, reputation and value for money; (4) experimental shoppers and early adopters; and (5) willingness to trade information for marketing benefits. Although this study developed a privacy measurement instrument, it did not measure the magnitude of privacy concerns or examine the underlying dimensions of privacy concerns. Sahd (1998:26) conducted a privacy survey in the electronic environment using Mann's privacy scale. Sahd 'tested' Mann's privacy scale and determined that a number of the dimensions in Mann's instrument lacked discriminant validity. Like Mann's study, Sahd's research also focused on the measurement instrument *per se*, and did not measure South African consumers' privacy concerns. In addition to the fact that these four studies did not measure South African consumers' concerns, the samples used were not representative and the findings of these four studies cannot be generalised to the South African population.

While international studies show ample evidence of different dimensions of information privacy concerns, such underlying dimensions have not been researched in South Africa. The research problem can thus be formulated as a **lack of knowledge and understanding of information privacy concerns of South African consumers.** On the basis of this research problem, several research objectives can be formulated, as discussed in the next section.

1.4 RESEARCH OBJECTIVES

The research objectives are divided into primary and secondary objectives. The primary objective is supported by several secondary objectives. These objectives are all discussed more fully below.

1.4.1 Primary objective

Consumers' concern regarding the privacy issue is very real, and any marketer who wishes to achieve long-term success has to take consumers' information privacy concerns into consideration (O'Malley *et al.*, 1999:421). In order to do this effectively, marketers have to understand consumer behaviour in a privacy sensitive environment. The primary objective of this study is **to identify and explore the information privacy concerns of South African consumers in a commercial environment.**

1.4.2 Secondary objectives

In the past decade, many researchers have recognised that consumer attitudes about privacy is a multi-faceted issue (Wang & Petrison, 1993:17; Campbell, 1997:45; Taylor, 2002:20). Therefore, several secondary objectives have been formulated to support the primary objective. The secondary objectives of this study are to establish:

(a) the underlying dimensions of information privacy concerns;

(b) differences between consumers' manifest behaviours to protect their privacy and their privacy concerns;

(c) differences between consumers in terms of their personal experiences of invasions of privacy and their privacy concerns;

(d) the dependency between gender and personal experiences of invasions of privacy;

(e) differences between consumers in terms of their knowledge about information protection practices and their privacy concerns;

(f) the dependency between age and knowledge about information protection practices;

(g) the dependency between level of education and knowledge about information protection practices;

(h) differences between consumers in terms of their Internet usage and their privacy concerns;

(i) differences between consumers in terms of their direct purchasing behaviour and their privacy concerns;

(j) different privacy sensitive segments based on consumers' general privacy concerns; and

(k) differences between consumers in terms of their demographic characteristics and their privacy concerns.

1.5 IMPORTANCE OF THE STUDY

At the start of 2002, the Minister for Justice assigned a committee, as requested by the Law Commission, to investigate the privacy and data protection issue with the aim of improving and adding new legislation in South Africa. Since information privacy is currently on the public agenda in South Africa, this study will provide information to all organisations and associations concerned with managing their customer information processes and the results will make a contribution to the body of knowledge. The knowledge of understanding consumers' privacy concerns will be the provision of the ability to develop policies that align organisations' information handling practices with customers' concerns. Identifying the underlying dimensions of information privacy concerns will indicate the dimensions of information privacy that cause most concern.

This will enable organisations to address the appropriate concerns during relational exchange processes.

1.6 SCOPE AND DEMARCATION OF THE STUDY

This is a study aimed at identifying and exploring the information privacy concerns of South African consumers. Information privacy should be distinguished clearly from physical privacy, which is concerned with physical access to a person. It also differs from trade secrecy, which addresses the ownership of intellectual corporate assets. The focus of both the theory and the empirical investigation in this study is on information privacy in a commercial environment, mainly addressing the use of consumer data for marketing purposes. This excludes other areas of concern such as medical privacy, identity theft, workplace monitoring, intelligence systems and biometrics. Although privacy is a multi-faceted concept encompassing a number of specific issues, the study mainly addresses the privacy issues affecting consumers during data collection, data storage, data use, data disclosure and solicitation. The empirical investigation was conducted among South African consumers above the age of 18 years whose household telephone number is listed in a telephone directory. One adult per chosen household was interviewed telephonically.

1.7 LIMITATIONS OF THE STUDY

The sample was limited to South African households with telephone numbers listed in the various Telkom telephone directories. The sample thus excluded households whose telephone numbers are not listed in a Telkom telephone directory, as well as households which do not have a landline.

1.8 RESEARCH DESIGN

The main aspects of the research design are discussed briefly in this section, and are discussed in detail in Chapter 6. An extensive literature review on information privacy

was conducted, consulting a wide range of relevant scientific journals, research publications and media articles. The empirical survey used national telephonic interviews. The questionnaire was developed on the basis of the literature, and pre-tested among consumers in the selected survey population. A probability sampling design was used in this study to draw a representative sample of households with listed telephone numbers in the Telkom telephone directories. The sample units were randomly selected, whereafter the telephone interviews were conducted with the adult in the household who had most recently celebrated his or her birthday. Data was captured and verified to ensure that no data capturing mistakes were made. Data analyses were done using the SAS programme for processing purposes. Several data analysis procedures were used, including cross-tabulation, frequency distribution, factor analysis, multiple analysis of variance, and confirmatory factor analysis. Reliability and validity testing were also performed.

1.9 PLAN OF THE STUDY

The current chapter has provided an overview of the literature, described the problem statement, research objectives, the importance and scope of the study as well as the research design. The remaining chapters address the following issues:

Chapter 2: Privacy in a legislative environment

This chapter provides a theoretical discussion on privacy in a legislative environment and deals with South Africa's Constitution, as well as with the most recent and proposed data protection legislative actions. The chapter also provides an overview of the history of the development of international legislation since the advent of the information age has increased the free flow of personal information across international borders.

Chapter 3: Consumer information privacy

Chapter 3 reviews the literature pertaining to the main area of study, namely consumer information privacy. It discusses information privacy in a commercial environment from a consumer perspective. Because of the information revolution, many consumers' right

to privacy focuses on two desires, namely, the desire to be left alone, and the desire to protect the consumer's confidentiality. The main discussion addresses these two desires in an information-driven environment that focuses particularly on the collection, storage, control, use and dissemination of personal information, leading to consumers' desiring to conceal information about themselves.

Chapter 4: Relational exchange processes and privacy

This chapter is devoted to the role of privacy in relational exchange processes and addresses the key elements in buyer-seller relationships. The role of organisations in relationship-building is discussed, whereafter information privacy related consumer behaviour is addressed. The discussion on consumer behaviour focuses on the behaviour patterns and activities that precede, determine and follow a consumer's decision-making. Finally, the impact of external influences on a consumer's decision-making processes, as well as on organisations, is investigated.

Chapter 5: Problem statement and formulation of research hypotheses

Chapter 5 elaborates on the problem statement and research objectives as discussed in the first chapter (Sections 1.3 and 1.4). The research hypotheses as well as their link with the identified primary and secondary objectives are also discussed in detail in Chapter 5.

Chapter 6: Research design and methodology

The research methodology is the focus of this chapter, with special reference to the population, sample frame and selection and the development of the measurement instrument. It also provides insight into the statistical techniques used for the data analyses.

Chapter 7: Research results and interpretation

Chapter 7 presents the findings of the empirical research ranging from the general research findings to the more detailed results and hypothesis testing. The results are

presented, interpreted and discussed. The findings of the hypothesis testing and other statistical analyses are presented and interpreted to enable appropriate conclusions.

Chapter 8: Conclusions, implications and recommendations for future research
In this final chapter, the study summarises the main findings and draws conclusions. The chapter also identifies the limitations and presents recommendations for future research.

1.10 SUMMARY

The dynamic nature of today's market imposes a responsibility on marketers to anticipate, plan and respond effectively to consumer needs. Within the current privacy sensitive environment, an understanding of consumers' information privacy concerns can be critical to any organisation's profitability and sustainable competitive advantage. Therefore, this study investigates the magnitude and underlying dimensions of consumers' information privacy concerns in a commercial environment.

The next chapter provides a theoretical background on **privacy** as a concept and presents an overview of how privacy has evolved, both nationally and internationally, in a legislative environment.

CHAPTER 2
PRIVACY IN A LEGISLATIVE ENVIRONMENT

2.1 INTRODUCTION

Privacy is a basic human need essential for the development and maintenance of both a free society and a mature and stable personality in an individual (Agre & Rotenberg, 1998:193). The right to privacy has become widely recognised and has developed in recent times. It is expressly guaranteed in the Universal Declaration of Human Rights of 1948, the European Convention on Human Rights of 1950, the International Covenant on Civil and Political Rights of 1966, and the American Convention on Human Rights of 1969 (Devenish, 1999:135-136). It is not explicitly mentioned in the African Charter on Human and People's Rights of 1981, but is found in most domestic bills of rights, as is the case in South Africa. The South African Constitution guarantees a number of rights of every South African citizen, including the right to privacy, as described in the Bill of Rights (Constitutional Assembly, 1996).

Since privacy, but more specifically information privacy, is currently on the public agenda in South Africa, with a Committee assigned to improve and add new legislation, this chapter addresses privacy from a legislative perspective to serve as a background for Chapters 3 and 4. It is important for all organisations and associations concerned with managing their customer information process to understand privacy. Any organisation that wants to understand consumers' privacy concerns will have to align its information handling practices and privacy policies with privacy legislation. The purpose of this chapter is to clarify the concept of general privacy before specific privacy issues, such as information privacy, are addressed. The rapid growth and increasing use of information technology (especially the Internet and other electronic means of communication) give rise to many complex privacy and data protection issues. Legislation regulating the data processing industry is essential in view of the threat and potential threat that this industry poses to the personal information of the individual.

This chapter addresses privacy from a constitutional perspective and deals with South Africa's most recent and proposed data protection legislative actions, apart from what is contained in the Constitution. Another important issue discussed in the legislative environment is the increasing perception that adequate privacy protection is a necessary condition for being on the global information highway (Agre & Rotenberg, 1998:112). Since the globalisation of markets has forced governments and international organisations to adopt privacy legislation and actions. Finally, the chapter provides an overview of the history of international legislation since the dawn of the information era has increased the free-flow of personal information across international borders.

2.2 THE CONSTITUTION OF THE REPUBLIC OF SOUTH AFRICA

At the beginning of the twentieth century the Cape of Good Hope, Natal, the Orange Free State, and the Transvaal were joined to become the Union of South Africa (Van Wyk, Dugard, De Villiers & Davis, 1996:131). The 1910 Constitution of South Africa gave no rights to the majority of the population and failed to provide for an inclusive democracy. The 1961 Constitution which declared South Africa to be a Republic still denied the majority of the population certain rights. The 1983 Constitution attempted to co-opt the coloured and Indian people as participants in the white-controlled Tri-cameral Parliament, but still excluded black South Africans (African National Congress, 1990:i-iii).

The global political changes of the late 1980s and pressure on South Africa to ban apartheid led to an acknowledgement of the ignored protests of generations of black people in South Africa. The process of developing a constitution for all South Africans started on 2 February 1990, and finally an interim Constitution came into force on 27 April 1994 (Van Wyk *et al.*, 1996:131). Its effect on the South African legal system can justifiably be described as revolutionary. Basically, the interim Constitution brought about three fundamental changes (De Waal, Currie & Erasmus, 2000:2):

- For the first time in South Africa's history, the franchise and associated political and civil rights were accorded to all citizens without racial qualification.
- The doctrine of parliamentary sovereignty was replaced by the doctrine of constitutional supremacy. The Bill of Rights was put in place to safeguard human rights. The courts were empowered to declare invalid any laws and conduct that were inconsistent with the Bill of Rights and the Constitution.
- The strong central government of the past was replaced by a system of government with federal elements. Significant powers were devolved to the provinces and local government.

The 1996 Constitution was drafted and adopted by the Constitutional Assembly and completed South Africa's negotiated political transformation. The Constitutional Assembly was given two years to produce a constitution that conformed to the 34 Constitutional Principles that had been agreed on during the political negotiations from 1991 to 1993. The initial draft of the Constitution was adopted by the Constitutional Assembly on 8 May 1996 and amended on 11 October 1996. Finally, the Constitution was signed into law by President Nelson Mandela at Sharpeville on 4 February 1997 (De Waal *et al.*, 2000:5-6).

The Constitution is an extensive document, numbering 227 pages of print, in the English and Afrikaans versions. Its 251 sections in fifteen chapters, and seven schedules must rank it amongst the longest constitutions in the world (Van Wyk *et al.*, 1996:158). Chapter 2 of the Constitution contains the Bill of Rights. Section 7 in the Constitution declares that the Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in South Africa and affirms the democratic values of human dignity, equality and freedom (Constitutional Assembly, 1996).

2.3 THE BILL OF RIGHTS

The 1996 Bill of Rights follows the format of its 1993 Bill of Rights predecessor, and most of the legal changes made in terms of the 1993 Bill of Rights are unaffected by its

replacement by the new Constitution (Jeffery, 1996/97:1). Traditionally, a bill of rights regulates the relationship between an individual and the state. However, the 1996 Bill of Rights goes further than the individual-state relationship – it recognises that private abuse of human rights may be as harmful as a failure to protect individuals from violations against them by the state. For this reason, the Bill of Rights is not confined to the protection of individuals from the state. In certain circumstances, the Bill of Rights also protects individuals against abuses of their rights by other individuals. Section 8(1) in the Constitution describes the circumstances under which the conduct of the **state** may be challenged for being inconsistent with the Bill of Rights. Section 8(2), on the other hand, deals with the circumstances in which the conduct of **private individuals** may be attacked for being inconsistent with the Bill of Rights (De Waal *et al.*, 2000:41). It is clear from Section 8(1) and 8(2) of the Constitution that the Bill of Rights applies both vertically, that is in relation to the state, and horizontally, that is in relation to private persons (Devenish, 1999:24).

Section 7 in the Constitution states that 'the state is obliged to respect, protect, promote and fulfil' the rights in the Bill of Rights (Constitutional Assembly, 1996). This makes the Bill of Rights not just a negative enforcement mechanism shielding subjects against the abuse of government power, but it also imposes a positive duty on the state to protect, promote and fulfil the entrenched rights (Devenish, 1999:8). The Constitution guarantees every South African citizen a number of rights as described in the Bill of Rights. Among these rights are **the right to privacy and the right to access of information**. These two rights are contained in Section 14 (the right to privacy) and Section 32 (the right to access of information) of the Constitution and are discussed below. It is, however, important to mention that Section 36 in the Constitution limits certain rights (including the privacy rights in the Bill of Rights), to the extent that the limitation is reasonable and justifiable in an open and democratic society (Constitutional Assembly, 1996).

2.4 THE RIGHT TO PRIVACY

2.4.1 Privacy defined

Privacy is a basic human need essential for the development and maintenance both of a free society and of a mature and stable personality in an individual. A logical first step in an evaluation of the law as a mechanism for regulating privacy is to define the scope of privacy law and what is meant by privacy (Agre & Rotenberg, 1998:193). The main problem with regard to privacy is the formulation of a proper definition, since there are different views of this concept. One constant element throughout the history of privacy is the difficulty of defining the concept of privacy. To make matters more problematic, some separate privacy issues such as identity theft and credit card fraud are actually criminal offences unrelated to legitimate uses of information, while telemarketing and unsolicited e-mail marketing are better characterised as sources of annoyance and inconvenience (Loyle, 2002:51). One result of this unsatisfactory situation is the gap between the technical concept of data protection on the one hand, and the legal and moral concept of privacy on the other (Agre & Rotenberg, 1998:6).

The term 'privacy' is widely used to refer to a group of related rights that are accepted nationally and internationally. In an attempt to grasp the scope of the term privacy, some popular privacy definitions are listed below:

- One of the earliest definitions of privacy was documented by Boston attorney Samual Warren and future Supreme Court Justice Louis Brandeis (Warren & Brandeis, 1890:193). They reasoned that the right to life has come to mean the right to enjoy life and that this improved the right to be left alone.
- Konvitz (in McQuoid-Mason, 1978:4) elaborates on the right to be left alone and stated: 'A person may claim the right to be let alone when he acts publicly as when he acts privately. Its essence is the claim that there is a sphere of space that has not been dedicated to the public use or control. It is a kind of space that a man may carry with him into his bedroom or into the street.'

- Fried (in McQuoid-Mason, 1978:5) defines privacy 'not merely as an absence of information about an individual in the minds of others, but rather the individual's control over the information he has about himself'.
- Ruebhausen and Brim (in McQuoid-Mason, 1978:5) argued that the essence of privacy is no more, and certainly no less, than the freedom of the individual to pick and choose for himself of herself the time and circumstances under which, and most importantly, the extent to which, his or her attitudes, beliefs, behaviour and opinions are to be shared with or withheld from others. They therefore define privacy as 'a positive claim to a status of personal dignity, a claim for freedom of a very special kind'.
- In the Guide to American Law of 1984 (in Devenish, 1999:135), the right to privacy is described as a right based on human dignity and has as its objective the preservation for each individual of 'the choice of when and how much he or she will allow others to know about his or her personal affairs or interfere with his or her mind, or body, or private activities'.
- Longley and Shain (1988:268) provide two definitions of privacy from a data and computer security angle: 'The right of an individual to self-determination as to the degree which an individual is willing to share with others information about himself that may be compromised by unauthorized exchange of such information among other individuals or organizations; and the right of individuals and organisations to control the collection, storage and dissemination of their information or information about themselves.'
- In Europe, the right to privacy has been said to consist of 'essentially the right to live one's own life with a minimum of interference. It concerns private family and home life, physical and moral integrity, honour and reputation, avoidance of being placed in a false light, non-revelation of irrelevant and embarrassing facts, unauthorised publication of private photographs, protection from disclosure of information given or received by the individual confidentially' (Devenish, 1999:137).
- The Royal Bank of Canada defines privacy as 'the right of customers to have their personal information safeguarded and to determine for themselves how, and to what

extent, information about them is collected, used and communicated to others' (Jayson, 2002:3).

- In Australia, privacy is defined as 'people's right to the privacy of their own body, private space, privacy of communications, information privacy, and freedom from surveillance' (Collier, 1995:44).
- Privacy is defined in South Africa by Neethling *et al.* (1996:36) as 'an individual condition of life characterised by exclusion from publicity'. This condition includes all those personal facts which the person himself or herself at the relevant time determines should be excluded from the knowledge of outsiders and in respect of which (s)he evidences a will for privacy.

Westin (in Agre & Rotenberg, 1998:194) contends that no final and absolute definition of privacy is possible because privacy issues are fundamentally matters of values, interests, and power. Privacy itself is an intangible commodity and is often mentioned in a negative context. For example, privacy is 'invaded', a confidence is 'breached', or a trust is 'broken' (Pounder & Kosten, 1992:1). Violations of privacy can constitute an invasion of a person's private life or relate to the acquisition and disclosure of personal information. The invasion of privacy has been defined as 'an international and wrongful interference with another's right to seclusion in his or her private life' (Devenish, 1999:145). Because of invasions of privacy, the Constitution addresses the right to privacy in Section 14 of the Bill of Rights.

For the purposes of this study, two definitions were developed (based on the above discussion) to define **privacy** and **information privacy** as they relate to the issues addressed in Chapters 2, 3 and 4.

Privacy is defined **as the right of an individual to isolate his or her private life (personal facts, time, circumstances, values and interests) from the knowledge of others, to be able to control what is withheld from others, and to be free from wrongful interference in his or her private life.**

Information privacy is defined **as the right of an individual to safeguard information about himself or herself from the use or control by others.**

2.4.2 Section 14 on the right to privacy

Section 14 in the Bill of Rights of the Constitution of the Republic of South Africa, which embodies the right to privacy, states (Constitutional Assembly, 1996):

> Everyone has the right to privacy, which includes the right not to have:
> - Their person or home searched;
> - Their property searched;
> - Their possessions seized; or
> - The privacy of their communications infringed.

Section 14 in the Bill of Rights has two parts. The first guarantees a general right to privacy (discussed in Section 2.4.2.1 of this study), and the second protects people against specific infringements of privacy, namely searches and seizures, and infringements of the privacy of communications (discussed in Section 2.4.2.2 of this study). Usually, the two parts are dealt with in separate sections of a bill of rights. In South Africa, however, the specific areas of protection form part of the general right to privacy. In most cases, when one's person, home or property is searched, or when one's possessions are seized or communications intercepted, Section 14 would be infringed upon. However, because the right against searches and seizures is a subordinate element of the right to privacy, the Constitution's protection is triggered only when an applicant shows that a search, seizure or interception of communication has infringed the general right to privacy (De Waal *et al.*, 2000:242-3).

2.4.2.1 The general right to privacy

An individual's general right to privacy is protected by common law as well as by the Constitution. Common law recognises the right to privacy as an independent personality

right and the Constitution recognises the right to privacy as a human right. This section of the study provides a brief description of the general right to privacy as protected by South African law.

(a) The common law right to privacy

The same considerations that have led to the entrenchment of a right to privacy in the Bill of Rights have long been recognised by common law as important reasons for protecting privacy. Common law recognises the right to privacy as an independent personality right which the courts consider to be part of the concept of a person's 'dignitas'. In common law, the breach of a person's privacy constitutes an *iniuria*. This occurs when there is an unlawful intrusion on someone's personal privacy or an unlawful disclosure of private facts about a person. Some examples of breaches of privacy recognised by the common law include entering a private residence; reading private documents; listening in on private conversations; shadowing a person; disclosing private facts which have been acquired by a wrongful act of intrusion; and disclosing private facts in breach of the relationship of confidentiality. The courts have also held that the common law right to privacy is invaded by publishing a person's photograph as part of an advertisement without the consent of that person, by a doctor's informing third parties that his or her patient had HIV (human immune deficiency virus), by wire-tapping private premises, and by peeping at a woman while she is undressing (De Waal *et al.*, 2000:243).

Because the South African legal system has entered the human rights arena, the relationship between fundamental human rights and personality rights must be considered briefly. The Bill of Rights recognises certain personality interests such as privacy. Many human rights relate to interests of personality. Personality rights which are enshrined in a bill of rights generally remain subjective rights, but receive stronger protection because the legislature and the executive of the state may not pass any law or take any action which infringes upon or unreasonably limits such rights. Thus, in addition to the normal delictual remedies available in the case of the infringement of a

personality right, these rights receive constitutional guarantees and protection (Neethling *et al.*, 1996:19).

(b) The constitutional right to privacy

The Constitutional Court has cautioned against a straightforward use of common law principles to interpret fundamental rights and their limitations. The determination of whether an invasion of the common law right to privacy has taken place is a single enquiry, and involves an assessment as to whether the invasion is unlawful. Under the Constitution, by contrast, a two-stage analysis must be employed in deciding whether there is a violation of the right to privacy. First, the scope of the right must be assessed to determine whether law or conduct has infringed upon the right. Second, if there has been an infringement, it must be determined whether it is justifiable under the limitation clause (De Waal *et al.*, 2000:243-4).

Although privacy is a right, some limitations with regard to it may be essential for the administration of justice and the reasonable maintenance of law and order. The courts should endeavour to find a balance between the public's right to know and the individual's right to privacy (Devenish, 1999:157). The scope of a person's privacy right extends only to aspects of his or her life or conduct where a legitimate expectation of privacy can be harboured. A legitimate expectation means that one must have a 'subjective expectation' of privacy that society recognises as 'objectively reasonable'. The subjective expectation component simply recognises that a person cannot complain about an infringement of privacy if (s)he has consented explicitly or implicitly to having his or her privacy invaded. At the same time, it is rather difficult to assess the kinds of privacy expectations that society would regard as objectively reasonable (De Waal *et al.*, 2000:244).

In modern society, the right to privacy seeks to protect three related concerns. An individual's subjective expectation of privacy in respect of these three concerns is usually regarded by society as objectively reasonable (De Waal *et al.*, 2000:244).

- First, the right to privacy seeks to protect certain aspects of one's life in respect of which one is entitled to be left alone: one's body, certain places and certain relationships. The rationale behind this right is that the state and other people should have nothing to do with an individual's intimate affairs.
- Second, the right to privacy aims to protect the opportunities for an individual to develop his or her personality and therefore extends to certain forms of individual and personal self-realisation or self-fulfilment. The implication is that the state may not compel individuals to conform to a stereotypical view of what a model citizen is. This right to privacy dictates that the state and society should be tolerant towards non-conformists. In this regard, the right to privacy involves issues such as the right to choose the kind of lifestyle one wants to lead.
- Third, the right to privacy seeks to protect the ability of individuals to control the use of private information about themselves. This right is closely related to the right to dignity, since the publication of embarrassing information, or information that places a person in a false light, is often damaging to the dignity of the person. But the right to privacy guarantees control over all private information and it is immaterial whether the information is potentially damaging to a person's dignity or not. The use of a person's name or identity without his or her consent would, for instance, constitute a violation of the right to privacy.

2.4.2.2 Infringements of privacy

In the field of the protection of privacy, the convictions of the community regarding right and wrong are of particular importance as a criterion of wrongfulness in all countries. This view is also apparent in South African case law. Privacy can be infringed upon only by knowledge of personal facts by outsiders contrary to the determination and will of the person whose right is infringed upon (Neethling *et al.*, 1996:243). The second part of Section 14 of the Bill of Rights protects individuals against specific infringements of privacy, namely searches and seizures, and infringements of the privacy of communications.

(a) Searches and seizures

The right to privacy includes the right not to have one's person, home or property searched or one's possessions seized. A violation of privacy by means of an act of intrusion takes place where an outsider acquires knowledge of private and personal facts relating to an individual, contrary to that individual's determination and wishes (Neethling *et al.*, 1996:243). Searches and seizures that invade privacy must be conducted in terms of legislation clearly defining the power to search and seize. There are laws that authorise searches and seizures, the most important of which is the Criminal Procedure Act 51 of 1977. The implication of the right to privacy is that the state or private individuals cannot search private property, the person or the home of others, or seize their possessions unless authorised to do so by statute or by the common law. When a search or a seizure is authorised by law, it is lawful, but the constitutionality of the enabling statute or common law may be attacked for violating the right to privacy (De Waal *et al.*, 2000:256).

(b) Privacy of communications

According to South African law, the infringement of private communications constitutes an invasion of privacy. The invasion can be committed by electronic means or by eavesdropping (Devenish, 1999:153). The infringement of privacy through an act of disclosure arises where, contrary to the determination and will of the individual, an outsider reveals to third parties personal facts regarding that individual, which, although known to the outsider, nonetheless remain private. For the sake of convenience, three types of disclosure of private facts can be distinguished, namely, first private facts acquired by a wrongful act of intrusion; second, disclosure of private facts contrary to a confidential relationship; and third, the disclosure of private facts through mass publication.

(i) Wrongful act of intrusion:

If a person acquires knowledge of private facts through a wrongful act of intrusion, any disclosure of those facts by such a person, or by any other person, in principle constitutes an infringement of the right to privacy (Neethling *et al.*, 1996:244). The

embodiment of private facts, for example by photography, photocopying and tape recording, contrary to the determination and will of the individual, constitutes a threat to the right to privacy. Although these acts in themselves do not violate the right to privacy because a wrongful act of intrusion or disclosure of private facts is not present, this interest is exposed to the danger or risk of a wrongful act of intrusion or exposure (Neethling *et al.*, 1996:260).

(ii) Confidential relationships:

Where only selected persons acquire knowledge of private facts in accordance with the determination and will of the plaintiff, and these persons disclose the information, contrary to this determination and will of the person, to a single person (or a small group of persons, as opposed to the mass publication thereof), the wrongfulness of their conduct is more problematic. It is submitted that as a rule, the disclosure is not contrary to the convictions of the community. Giesker (in Neethling *et al.*, 1996:243) suggests that 'the more necessary it is for a person to impart the private facts of the outsider, the more pressing the protection against the disclosure of those facts to third parties by the outsider'. In certain instances the relationship is such that persons are compelled to disclose certain facts about themselves to other parties, such as relationships between doctor and patient, banker and client, direct marketer and consumer. A confidential relationship may also arise where there is an agreement between the parties that private facts disclosed will be confidential or secret (*Geheimhaltungsvertrag*). In such instances disclosure of the private facts involved apart from the breach of contract also constitute an infringement of the right of privacy (Neethling *et al.*, 1996:249-54).

(iii) Mass publication:

The mass publication of facts (disclosure to an unlimited or limited number of persons) is characterised by an element of confidentiality, and the publication thereof in principle infringes on the right to privacy (Neethling *et al.*, 1996:254). The question that must be asked here is to what extent the newspapers may publish truthful – albeit painfully intrusive information – about a person. Newspapers are entitled to publish certain truthful information, although private in nature, about public figures. This is because 'the

candidate who vaunts his spotless record and sterling integrity cannot convincingly cry "foul" when an opponent or an industrious reporter attempts to demonstrate the contrary' (Devenish, 1999:155). Private persons are in an entirely different position, and should enjoy far greater protection. However, it could be argued that the newsworthiness of a particular subject could in practice diminish the extent of such protection. Here the courts have to endeavour to find a balance between the public's right to know and the individual's right to privacy (Devenish, 1999:154).

It is important to note that in all the above-mentioned instances, the question of an infringement of privacy arises only if the individual is identified with the disclosed facts. If this element of identification is absent, the disclosure does not relate to a specific person in his or her state of privacy.

Apart from giving the right to personal privacy a benevolent interpretation, Section 14 must also be read together with similar rights protected in other sections in Chapter 2 of the Bill of Rights, such as the right of access to information provided for in Section 32. The right to personal privacy (Section 14), read with the right of access to information (Section 32), should therefore be interpreted as guaranteeing each citizen a privacy of personal information. The section below addresses the right of access to information as contained in Section 32 of the Constitution.

2.5 THE RIGHT OF ACCESS TO INFORMATION

The objective of the Constitution and the Bill of Rights is to create an open and democratic society. By providing a right to freedom of information, the Constitution has recognised the importance of access to official information in the modern era. Freedom of information is based on two levels: first, at an individual level, where freedom of information is closely connected to freedom of expression and the right to privacy; and second, at a level where freedom of information operates at a political level. In an open and democratic society, government should be accountable for its actions and decisions. Public access to information is fundamental to encouraging transparency and

accountability in the way government and public authorities operate. In addition, the Constitution provides a right of access to information in private hands, where that information relates to the exercise or protection of the rights of the information seeker. This provision recognises that information in private hands, such as those of employers, credit bureaux, insurance companies, banks and direct marketers, can have a considerable impact on an individual who should be able to have access to that information in order to ensure its accuracy or to challenge decisions made on the basis of the information (De Waal *et al.*, 2000:41-2).

2.5.1 Section 32 on the right of access to information

Section 32 of the Constitution states (Constitutional Assembly, 1996):

> Section 32(1): Everyone has the right of access to:
> (a) Any information held by the state; and
> (b) Any information that is held by another person and that is required for the exercise or protection of any rights.
>
> Section 32(2): National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

Section 32(1) sets out the right of access to information in the hands of the state, but also expands the reach of the right of access to information held by private persons. The second part of Section 32(1), stating the access to information held by 'another person', reflects the horizontal nature of the Constitution. This means that it applies not only vertically between citizens and the state, but also between people, among themselves (Brand, 2000b:3). Regarding the access to information held by the state [Section 32(1)(a)], there are no restrictions, thus providing for a rather wider right. Section 32(1)(b) contains the term 'required', and the right has to be interpreted in such a way that one may exercise the right when the information is reasonably required for

the protection of one's rights. The term 'rights' is not defined in the above context and could be taken to refer to the fundamental rights of a person, private law rights or both legislative and private law rights for which the state is responsible, as well as a private individual. This does not, however, provide for a blanket right to accessing information (Judin & Kisch, 2001:1-2). The Constitution is quite clear about the kind of information that may be requested. In the case of the state, there is access to 'any information'. In the case of private bodies, that access is restricted to information that may be needed to exercise or protect other rights (Brand, 2000d:6). It may be possible to refuse such a request on the basis that it would result in an invasion of the privacy of an identifiable person other than the person requesting the information. Further grounds for refusal may be that the records sought to be attained disclose confidential information about a third party, for example, trade secrets (Judin & Kisch, 2001:1-2).

Important limitations are placed on the type and quantity of information that may be claimed under the rights by the proviso that such information must be made available to an applicant only 'in so far as such information is required for the exercise or protection of any of his or her rights' (De Waal *et al.*, 2000:442). Justifiable limitations can arise in relation to law enforcement and criminal procedure, state secrets and foreign affairs, national security, privacy, trade secrets or confidential business information, and legal professional privilege (Devenish, 1999:447-8). The right of access to information therefore includes a number of exemptions. First, the right applies only to 'records' – that is information recorded either in written or electronic form. This excludes information documents of the cabinet, courts and members of parliament or provincial legislatures. Requests for information may also be refused if they would constitute an unreasonable invasion of third-party privacy. Several further exemptions relate to security, military and economic matters, law enforcement and foreign relations. In the case of privately held information, further exemptions are made to protect commercial interests and trade secrets (Brand, 2000d:6). The right of access to information is thus a balancing process to be used between the right to access and other fundamental rights, such as one's right to privacy (Judin & Kisch, 2001:2).

The **right of access to information** (Section 32) could be beneficial in relation to a judicial review of administrative actions, which provides for the **right to just administrative action** (Section 33). Therefore, where the policies and criteria used by administrative bodies are inaccessible to the public, Section 32 could be invoked to secure the required information, subject to the restrictions sanctioned by the limitation clause (Devenish, 1999:451). The Promotion of Administrative Justice Act 3 of 2000 was instituted to give effect to one's right to administrative action that is lawful, reasonable and procedurally fair, and to the right to written reasons for administrative action as contemplated in Section 33 of the Constitution (Hoexter, Lyster & Currie, 2002:13). The Promotion of Administrative Justice Act 3 of 2000 applies to both the state and to persons other than the state (Lambrechts, 2000:90).

Item 23 of Schedule 6 in the 1996 Constitution suspended the operation of the access to information rights until freedom of information legislation was enacted, or for a maximum period of three years (to the end of January 2000). This means that the right in Section 32(1) could not take effect until the enactment of the required national legislation required by Section 32(2) of the 1996 Constitution. Legislation to give effect to the rights enshrined in Section 32 was addressed via the drafting of the Open Democracy Bill that was promulgated as the Promotion of Access to Information Act (De Waal *et al.*, 2000:42). A description of the development process of the Open Democracy Bill is given below.

2.5.2 Promotion of Access to Information Act 2 of 2000

There is a significant difference between the USA and Europe in their approach to privacy. Legislation in the USA is mainly based upon its Bill of Rights, which primarily serves to protect the individual from the state. Legislation to protect the individual from undue invasion of privacy by other legal persons is minimal and fragmented. Legislation in Europe, on the other hand, is more concerned about the protection of the individual from other individuals. In South Africa, the first draft of the Open Democracy Bill conformed more closely to the United States pattern (Department of Communications,

2000b:70). The Open Democracy Bill, which dealt with the constitutionally-guaranteed right of access to information, was introduced in Parliament in 1998 (Brand, 2000a:3). This Bill, ostensibly proposed as a means to entrench these rights particularly in the governmental sector, was extended to include a chapter relating specifically to the rights of privacy and information access in the private sector. The memorandum on the objects of the draft Open Democracy Bill stated, among other things, that the principal objects of the Bill are to provide for 'access by individuals to information about themselves held by private persons, the correction of personal information held by the state or private persons, and the protection of individuals against abuse of their personal information by the state or other private persons' (Direct Marketing Association, 2001a:8).

The above Bill placed stringent and onerous privacy requirements on private organisations. Several industry bodies lobbied for amendments to the Bill. They argued that the initial legislative proposals were inappropriate and that the conditions and limitations would be detrimental to the industry. The Open Democracy Bill was subsequently withdrawn and reintroduced towards the end of 1999. After the private sector portions and data protection provisions of the Open Democracy Bill had been removed, the Bill was approved with 254 votes to 82, and promulgated as the Promotion of Access to Information Act 2 of 2000 (Brand, 2000c:3; Ludski, 2000:1; Direct Marketing Association, 2001a:8). The objective of Act 2 of 2000 is to give effect to the constitutional right contained in Section 32 of the Constitution of access to any information held by the state, as well as any information that is held by another person and that is required for the exercise or protection of any rights (Lambrecths, 2000:86).

In terms of the Promotion of Access to Information Act, all organisations have to produce manuals of information held by the organisation. The South African Human Rights Commission has published a 'blueprint' of what a manual could look like and the information it should contain. The Minister for the Department of Justice has, after several requests, approved an extension to the deadline for the publication of manuals from 15 August 2002 to 28 February 2003 (Ivans & Duval, 2002). The current Promotion

of Access to Information Act thus emphasises the obligations of the state in the protection of personal data held by it more than the collection, use and dissemination of personal data by the private sector.

However, the exclusion of the private sector portions of the Open Democracy Bill was accompanied by a strong plea by the Chair of the Parliamentary Portfolio Committee (Advocate De Lange) to the Law Commission to pass a Data Privacy Law with urgency (Direct Marketing Association, 2001a:8). The constitutional recognition and protection of the right to privacy (Section 14) as a fundamental human right provides some indication of the importance of this right and may possibly place a duty on the state to adopt proper legislation for the regulation of the data industry and the protection of an individual's personal data. Moreover, Section 32 in the Constitution gives individuals access to information held by the state, but also access to any information held by another person (Neethling *et al.*, 1996:292). This highlights the fact that it is important to regulate the data industry. Therefore, the next section of this chapter addresses data protection as related to privacy and freedom of information. Data protection is a descriptive term referring to rules about the collection, use and dissemination of personal information. One important policy objective of data protection is the application of fair information practices, an organised set of values and standards regarding personal information and defining the rights of record subjects and the responsibilities of record keepers (Agre & Rotenberg, 1998:194).

2.6 PRIVACY AND DATA PROTECTION

Data protection entails the legal protection of persons (the data subjects) with regard to the processing of data concerning themselves by other persons or institutions (the data media). Since the seventies, the individual's need for protection in this field, which especially concerns his or her privacy as a personality object, has progressively received more attention in industrialised countries (Neethling *et al.*, 1996:291). The processing of private and public data can pose a potential threat to an individual and is briefly discussed below.

2.6.1 Private and public data

Private data about an individual can be held by credit bureaux, banks, employers, insurance companies, the medical profession, voluntary associations and mailing list companies. These data media often collect personal information about individuals with regard to various activities such as drinking habits, health, reputation, political and religious convictions, criminal records, race and creditworthiness. Although the data stored by these institutions are often available only to its clients, the possibility exists that other individuals, private institutions or even the state may have access to such information (Neethling *et al.*, 1996:292-4). Mr Johnny de Lange, chairman of the Parliament's justice portfolio committee, claims that the absence of relevant legislation has exposed South Africans to widespread abuses of privacy (Ludski, 2000:1). When people apply for an account at a bank, the personal information obtained by the bank can be shared with other institutions without the consent of customers. Unless it is properly regulated, information technology is capable of eroding, if not eliminating, the concept of privacy. People around the world are increasingly recognising that they and their personal information are subjected to unfair control and manipulation on a daily basis. Therefore, countries around the world are passing legislation on personal data protection (Holvast *et al.*, 2001:14). Data protection is no longer seen as a purely functional construct to be used to directly shape and influence the use of information-processing technology. Instead, the focus has shifted to the individual, as can be seen in citizen's rights featured prominently in all European data-protection systems (Agre & Rotenberg, 1998:235).

The state, with all its departments, agencies and other offices, personifies the public data media. On account of the state's numerous activities and functions, the personal data processed covers a wide range, for example information on civil servants as employees, on pupils and students at educational institutions, on taxpayers at the receiver of revenue, and on all individuals in terms of census reports, voters' rolls and registration of the population. The processing of this data is usually justified by its public

importance. The storage and use of the information is generally essential for the proper functioning of state administration and effective state planning. Since individuals may be compelled by legislation to furnish information on themselves to the state, the state controls this unique source of information directly. To illustrate the danger that the processing of data by the state poses to the privacy of the individual, the Identification Act 72 or 1986 is discussed below. This statute permits the Director-General of Internal Affairs to supply personal information without the consent of the data subject to any other state department, local authority or statutory body for any of their purposes, or even to any other person who makes application and pays the prescribed fees, if the Director-General is of the opinion that furnishing such information is in the interests of the person concerned or in the public interest (Neethling *et al.*, 1996:294-5).

The processing of information by private or public data media threatens individuals in two ways. First, the compilation and distribution of personal information creates a direct threat to the individual's privacy. When information relating to a person is collected, the total picture represented by the record of such facts is usually of such a nature that the person in question would like to restrict others from having knowledge thereof, despite the fact that some of the data, viewed in isolation, are not necessarily 'private'. Second, the acquisition and disclosure of false or misleading data may lead to an infringement of the individual's right to his or her identity. A processing of incorrect or misleading personal data through the data media also poses a threat to an individual's identity because the information is used in a manner which is not in accordance with his or her true personal image (Neethling *et al.*, 1996:295-6).

Unless data legislation controls the private sector in South Africa, the public is justified in being concerned about its personal data privacy. Hence, given the limitations of the Promotion to Access of Information Act, the Law Commission instituted a Project Committee consisting of various experts to investigate the privacy and data protection issue.

2.6.2 Project 124 Committee

The Ad Hoc Joint Committee on the Open Democracy Bill submitted its report on the Promotion of Access to Information Bill to Parliament on 24 January 2000. The Committee noted that the Bill only deals with the aspect of access to private information about an individual, be it access by that individual or another person, and did not regulate other aspects of the right to privacy, such as the correction of and control over personal information. Foreign jurisdictions with freedom of information regimes have enacted separate legislation which, as an important component of democracy legislation, regulates aspects such as the correction of and control over personal information. Privacy legislation generally provides for more detailed mechanisms and provisions dealing with personal information in the hands of another person by empowering that individual, among others, to demand the rectification of incorrect information.

The Committee requested the Minister for Justice and Constitutional Development to introduce privacy and data protection legislation in Parliament as soon as possible. Since the preparation of this type of legislation will require extensive research, the Minister requested the Law Commission to consider the possible inclusion of such an investigation in its programme. The Minister then approved the inclusion of the investigation in the Commission's programme on 8 December 2000. At the start of 2002, the Minister of Justice assigned ten members to the Project 124 Committee under the chairmanship of Judge Craig Howie, with Prof. Neethling as the project leader. The Project 124 Committee is currently investigating the privacy and data protection issue with the aim of improving existing legislations and adding new legislation as soon as possible (Mokgoro, 2000:10-22).

Consumers' expectations and concerns regarding possible legislation and government protection are of specific importance to this study and will be one of the aspects measured in the empirical survey.

Due to the multifaceted nature of the data industry, it may be necessary for the Project 124 Committee to develop codes of conduct, enforced by legal sanctions, for the data activities for each sector of the data industry. However, this method is likely to be cumbersome and too extensive, and may also prove to be too rigid. Consequently, a more flexible approach seems to be required by means of which general principles may be developed for the protection of data. According to traditional principles, it can be accepted that the unauthorised collection or storage of personal information, or the processing of false or misleading data are in principle wrongful and that the communication thereof to third parties should also be regarded as unlawful (Neethling *et al.*, 1996:297-9). Traditional principles of protection are of little value if a data subject is not legally empowered to exercise direct control over his or her data records.

It is obvious that legislation regulating the data processing industry is essential in view of existing threats and potential threats to the personal information of the individual. Neethling *et al.* (1996:306) stressed the fact that when drafting legislation, a proper balance must be found between competing interests. First, the individual's personality merits proper protection. Second, the Constitution recognises every person's right to engage freely in economic activity. In order to exercise this right properly, an individual needs personal information about others. Third, the state can fulfil its functions properly only if it also keeps a record of sufficient personal information regarding its subjects. Future legislation will have to accommodate all these rights and interests in a balanced manner.

The complexities of modern society have produced more reasons why the state or an individual has an interest in, and need of information regarding another person. In order to obtain this data and satisfy these needs, a new industry has developed, the practices of which pose a potential threat to the individual due to the use of electronic means (computers) for storing data (known as a data bank). In particular, integrated data banks create a greater possibility of disclosure of an individual's private life (including computer privacy) than ever before (Neethling *et al.*, 1996:291). Various role players in South Africa are also aware of the effect of the electronic commerce environment on

information privacy. The section below addresses some of the current issues on the matter.

2.6.3 Electronic communications and transactions

Rapid growth in Internet usage has fuelled the privacy issue. In every electronic communication, an Internet user discloses some form of personal information. Every e-mail message contains a header with information about the sender and the recipient. Virtually every electronic transaction involves the transfer of personal data such as identity numbers, credit card numbers, telephone numbers, physical addresses and e-mail addresses. The key to further Internet growth, especially as far as electronic commerce is concerned, is the attainment of privacy through technology and law (Buys, 2002). Buys (2002) contends that it would be risky to regulate the technology that threatens privacy. He believes that the legislature and the courts should rather be interested in giving Internet users control over their own information and to provide measures to enable every user to make an informed decision on the question of how private and confidential personal information should be in the digital age.

In May 1998, the Department of Communications received a mandate to establish an information technology investment cluster. The main objective of this cluster was to develop coherent legislation on information society-related issues (Groenewald & Lehlokoe, 1999). The right to privacy and data protection was a key issue taken up by the Department of Communication in the e-Commerce Green Paper. The Minister of Communications, Dr Ivy Matsepe-Casaburri, launched the government's Green Paper on e-Commerce on 20 November 2000. The launch concluded the first phase of government's initiative to develop an appropriate legal foundation for electronic business in South Africa. The Green Paper invites comments which, when considered and compiled, will direct the formulation of government policy in a White Paper (Department of Communications, 2000a). In the electronic commerce (also called e-commerce or e-business for short) environment, unsolicited commercial e-mail, international sharing of data, automatic collection of information, and tracking of

individuals when they go online are contentious issues. Legislation aimed at preventing any abuse of information and an invasion of privacy is expected to give individuals the right to demand the correction of information that is on record about themselves. It is also expected to stop organisations from using information provided by customers for purposes other than those for which it was supplied (Ludski, 2000:1).

The Electronic Communications and Transactions (ECT) Bill was tabled before Parliament recently and South Africa became the first country in Africa to join more than 20 other countries that have introduced electronic commerce legislation in the past four years (Temkin, 2002:2). The Bill reads *inter alia* as follows:

- to provide for the facilitation and regulation of electronic communications and transactions;
- to provide for the development of a national e-strategy for the Republic;
- to promote universal access to electronic communications and transactions and the use of electronic transactions by small, micro and medium sized enterprises;
- to provide for human resource development in electronic transactions;
- to prevent abuse of information systems;
- to encourage the use of e-Government services; and
- to provide for matters connected therewith (Minister of Communications, 2002).

The Bill will affect all organisations, even if they do not consider themselves e-commerce players. This is because it also deals with issues that go beyond electronic transactions such as the registration of cryptography providers, proper control of critical databases, consumer protection, domain name administration and cyber crime (Temkin, 2002:2). The act aims to give legal effect to and regulate a wide range of electronic communications. These include electronically stored records, e-mail, websites, short message services (SMS), pre-recorded telephone messages, automated teller machine (ATM) transactions and online contracting (Grealy, 2002:21). Any organisation that encrypts documents or messages will be affected by clauses allowing government to determine which technologies can be used and when messages can be intercepted. A proposal that gives government the right to know what kind of critical information is

stored on corporate databases will also affect organisations. Traders selling goods or services online face onerous new rules. Retailers who do not give full details about their company and give consumers sufficient opportunity to review and modify an order would be obliged to take the goods back if the buyers changed their minds within 14 days (Stones, 2002:3; Temkin, 2002:2).

Using a smart card, a fingerprint and a password, President Thabo Mbeki signed into law the Electronic Communications and Transactions (ECT) Bill in July 2002. The ECT Act makes this advanced electronic signature legal. At the signing ceremony, Communications Minister Ivy Matsepe-Casaburri said the Act allowed for data messages to be legally recognised. It would ease the conclusion of deals and transactions online. The most controversial part of the Act is Chapter 10, which allows for a non-profit organisation to control the '.za domain'. This organisation's nine directors will be nominated by the Minister, following a process of public nomination and selection by an independent panel (Anon, 2002c:2).

Because of the ubiquity, ease of use, speed and decentralisation of electronic technology, privacy is unequivocally an international issue on the international agenda. South Africa's policy-makers will have to pay attention to agreements reached at the international level with regard to privacy and data protection (Agre & Rotenberg, 1998:112). Therefore, the final section of Chapter 2 provides a broad outline of the development of international privacy issues, highlighting some of the most important privacy legislation in other countries which might have a bearing on the South African scenario.

2.7 INTERNATIONAL PRIVACY AND DATA PROTECTION

The dawn of the information age has increased the importance of personal data protection to a level where governments and international organisations around the world have been forced to adopt privacy legislation and multilateral instruments. At the same time, various organisations and governmental interests have attempted to stem

the tide of public demands for the privacy of an individual's most sensitive private information (Holvast *et al.*, 2001:1). A discussion on the historical development of privacy and data protection in the international arena follows.

2.7.1 Before 1970

The first privacy law was created by Warren and Brandeis in the USA in 1890, although it was not until 1970 that the Privacy Act was enacted (Schwartz, 1998:48). On 10 December 1948, the General Assembly of the United Nations adopted and proclaimed the Universal Declaration of Human Rights. The Declaration sets forth a comprehensive list of the rights to which all people are entitled. Article 12 of the Universal Declaration recognises the right to privacy (Rotenberg, 2001:256). Shortly after the Universal Declaration of Human Rights of the United Nations, the Council of Europe Convention for the Protection of Human Rights was adopted, in 1950. Article 8 in the Council of Europe Convention addresses the right to respect private and family life (Rotenberg, 2001:262). Many believe that the Nazis behaviour was the impetus for the 1950 European Convention on Human Rights, drawn up shortly after World War II. Europeans viewed privacy as a human right partly as a reaction to the Nazis use of personal records to identify 'undesirables' (Williams, 1999:5). In 1969 the Organisation for Economic Cooperation and Development (OECD), an international body of 29 countries, became the first international organisation to recognise the privacy implications of the transborder data flow of personal information when its Data Bank Panel examined the privacy issues associated with digital personal information (Holvast *et al.*, 2001:1).

2.7.2 The 1970s

In 1970 the United States Congress passed the Fair Credit Reporting Act to protect individuals from any misuse of personal information by Credit Reporting Agencies (Rotenberg, 2001:1).

Sweden introduced its Data Act in 1973 to prevent undue encroachment on individual privacy. This Act requires registration and licensing of databases with personal information (Hussain & Hussain, 1992:153). Four years after the USA passed the Fair Credit Reporting Act, the Privacy Act and the Freedom to Information Act were passed by the United States Congress in 1974. Whereas the Privacy Act of 1974 grants citizens access to their own personal files kept by the government, the Freedom of Information Act allows citizens to access all federal agency records (Rotenberg, 2001:39,60). This was followed by the Right to Financial Privacy Act of 1978 that sought to regulate the disclosure of personal financial information to federal agencies in the USA. This Act also recognises individuals' privacy interests in their bank records, and gives them rights regarding the disclosure of these records (Rotenberg, 2001:79). In 1977, the Federal Data Protection Act was introduced in Germany to guard against any misuse of personal data during storage, communication, modification and erasure, and to prevent harm to any personal interest of the person concerned (Hussain & Hussain, 1992:153).

2.7.3 The early 1980s

In 1980 the Privacy Protection Act was passed in the USA. This Act establishes procedures for law enforcement seeking access to records and other information from the offices and employees of a media organisation (Rotenberg, 2001:101). On 23 September 1980, the OECD issued guidelines for privacy protection in the transfer of personal information across national borders. In developing the guidelines, the OECD worked closely with the Council of Europe, which was at that time drafting its own Convention on Privacy (Rotenberg, 2001:268). Canada passed its Privacy Act in 1982. This Act establishes rules applying to any information collected and used by government and introduces a fair information code to regulate government's handling of personal records (Holvast *et al.*, 2001:2). The United Kingdom's Data Protection Act was put in place in 1984, preventing the international transfer of personal information if it considered that information to be inadequately protected in the receiving country (Collier, 1995:42). In 1984, the USA passed the Cable Communication Policy Act to provide a strong statutory framework for the protection of television cable subscribers'

personal information. The Act incorporates the privacy principles set out in the OECD Privacy Guidelines of 1980 (Rotenberg, 2001:107).

2.7.4 The mid- to late 1980s

In 1985, the OECD extended its guidelines to cover transborder data flow. The Council of Europe had concluded the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data in 1981, and it came into effect in 1985. The Council negotiated the Convention in response to the rapid rise of automated data processing, and advances in computer technology that were allowing more and more records to be stored and transferred digitally (Rotenberg, 2001:297). Although there are many similarities between the OECD Guidelines and the Council of Europe Convention, the OECD Guidelines are advisory in nature and not legally binding on its members, whereas the Council of Europe Convention is legally binding on any Member State that ratifies it (Holvast *et al.*, 2001:2).

The Electronic Communications Privacy Act was enacted in the USA in 1986 as an amendment to the Omnibus Crime Control Act of 1968, to address technological advancements in communication networks and to bring electronic communication within the ambit of federal law regarding wiretapping and bugging (Rotenberg, 2001:111). Under this law, neither private entities nor government can gain unauthorised access to stored messages such as e-mail, nor can they intercept these messages (Schwartz, 1998:49). During 1988, the USA amended the Federal Criminal Code to prohibit the disclosure of video rental records containing personally identifiable information by enacting the Video Privacy Protection Act of 1988 (Rotenberg, 2001:165). In Australia, the Privacy Act of 1988 details Information Privacy Principles based on the OECD Guidelines, covering the Commonwealth (federal) public sector. Australia's Privacy Act also applies to the private sector in that it includes provisions and guidelines governing the consumer credit industry and restricts the use of tax file number information (Rotenberg, 2001:413).

At the end of the 1980s, three important areas of divergence were observed in the world's data-protection policies. The first concerned the scope: most of the European countries applied the same statutory principles to both the public and private sector. The USA, Canada, Australia and Japan, however, rejected an 'omnibus' approach, preferring to regulate only the public sector's practices and to leave the private sector governed by a few sectoral laws and voluntary codes of practice. The second difference was a disagreement about whether these laws should apply only to computerised personal data and/or also to manual record-keeping systems. Most countries chose to make no distinction, except for Sweden, the United Kingdom and Austria. The third and principal difference concerned the choice of policy instruments to enforce, oversee, and administer the implementation of the legislation. These powers range from the stricter licensing and registration regimes in force in Sweden and Britain to the more advisory and less regulatory systems headed by privacy or data-protection 'commissioners' in Germany, Canada, and Australia (Agre & Rotenberg, 1998:101).

2.7.5 The early 1990s

The United Nations provided ten principle guidelines for the Regulation of Computerised Personal Files concerning the minimum privacy guarantees that ought to be reflected in national privacy laws These guidelines were adopted on 14 December 1990. These guidelines mirror the OECD's eight guidelines, but set them out in slightly different ways (Rotenberg, 2001:307). The Telephone Consumer Protection Act of 1991 amended the Communications Act of 1937 in the USA. The purpose of this amendment was to prohibit any person within the USA from using an automatic telephone dialing system to make a call to any emergency telephone line or to any telephone number for which the called party was charged for the call without the consent of the called party, with specified exceptions. The Act also prohibits the use of a telephone facsimile machine, computer or other device to send an unsolicited advertisement to a fax machine (Rotenberg, 2001:178). New Zealand introduced a Privacy Act in 1993 with the object of promoting and protecting individual privacy in respect of information about individuals in accordance with the OECD Guidelines (Holvast *et al.*, 2001:1). In 1994, the Driver's

Privacy Protection Act was enacted. It requires all the States in the USA to protect the privacy of personal information contained in an individual's motor vehicle record, excluding traffic violations, license status and accidents in which the driver was involved (Collier, 1995:42; Rotenberg, 2001:188).

2.7.6 The mid 1990s

The Personal Data (Privacy) Bill was signed into law in Hong Kong on 3 August 1995. This resulted in a Personal Data (Privacy) Ordinance. The main international effect of the ordinance is the restriction it places on the transfer of personal data outside Hong Kong. Such a transfer of personal data that are collected, held, processed or used either in Hong Kong or by a data user whose principal place of business is in Hong Kong is prohibited unless one or more specified conditions are met (Holvast *et al.*, 2001:9).

In 1995, the European Union's Directive on the 'Protection of Personal Data' and on the 'Free Movement of Personal Data' finally emerged from the European Union's complex and drawn-out legislative process (Agre & Rotenberg, 1998:105). The European Union Data Protection Directive of 1995 establishes common rules for data protection among Member States of the European Union in order to facilitate the free flow of personal data within the European Union (Rotenberg, 2001:311). Many organisations that rely on an unimpeded flow of personal data between themselves and Europe have been particularly alarmed by the European Union's Privacy Directive (Holvast *et al.*, 2001:2). The Data Protection Directive has had, and will continue to have, an impact on the data-protection policies of countries (or states) that have not yet passed such legislation, including those outside the European Union.

The pressure on non-European Union countries stems principally from the stipulation in Article 25 that data transfers to a 'third country' may take place only if that country ensures an 'adequate level of protection'. Article 26 lists a number of derogations, among which is the provision that data may be sent to countries with 'inadequate'

protection if the data controller enters into a contract that 'adduces sufficient guarantees with respect to the protection of the privacy and fundamental rights and freedoms of individuals' (Agre & Rotenberg, 1998:109). An implementation of Articles 25 and 26 can have vast economic consequences for credit-granting and financial institutions, hotel and airline reservation systems, the direct marketing sector, life and property insurance, and for any other sector that relies on the flow of personal data across international borders (Agre & Rotenberg, 1998:109).

In 1996, the International Labour Office in Geneva compiled a Code of Practice on the Protection of Workers' Personal Data. The purpose of this Code of Practice is to provide guidance on the protection of workers' personal data when developing legislation, regulations, collective agreements, work rules, policies and practical measures. This Code does not have binding force and does not replace national laws, regulations and international labour standards (Rotenberg, 2001:364).

In the same year, the USA amended the 1934 Communications Act to the Telecommunications Act of 1996. Section 222 of the Act provides that telecommunications carriers must protect the confidentiality of Consumer Proprietary Network Information (CPNI). CPNI includes the calling patterns, billing records, unlisted telephone numbers and home addresses of service subscribers (Rotenberg, 2001:192). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was passed by the United States Congress to combat fraud by standardising the format, use and security of electronically transmitted healthcare information. HIPAA's security and privacy standards are an important step toward building consumer confidence enabling increased electronic transactions in the healthcare industry in the USA (Hanks, 2002:1).

The unprecedented growth of communication networks and associated technologies for privacy and security has created a need for an international policy framework to harmonise national policies and promote techniques to safeguard communication networks. In 1997, the OECD adopted the Guidelines for Cryptography Policy. The Guidelines are a non-binding agreement identifying the policy goals that countries

should implement when drawing up cryptography policies at national and international levels (Rotenberg, 2001:351).

In December 1997, the European Union adopted the Directive of the European Parliament and of the Council concerning the processing of personal data and protection of privacy in the telecommunications sector (Rotenberg, 2001:339).

2.7.7 The late 1990s

In 1998 the Children's Online Privacy Protection Act was introduced in the USA. It prohibits an operator of a website or online service directed at children, or any operator who has actual knowledge that it is doing so, from collecting personal information from a child in a manner that violates regulations required under this title which are designed to protect such children from unlawful and deceptive practices in the collection of personal information (Rotenberg, 2001:196).

In 1999 the Financial Modernisation and Privacy Act, also known as the Gramm-Leach-Bliley Act (GLB Act) was introduced. This Act is regarded as the most sweeping legislation in the USA affecting banks and other financial institutions since the Depression in the early 1930s. The passage of the GLB Act permits banks, insurance companies and brokerage firms to operate as one entity, enabling them to offer a wider range of products and services, but with great implications for consumer privacy rights. To regulate the disclosure of consumer data among affiliates, the GLB Act requires financial institutions to give customers a Privacy Policy notice informing them of the kind of information it collects about them and how it uses that information. It also requires financial institutions to give consumers the right to 'opt out' or prevent the sale of personal data to third parties, and to develop policies to prevent fraudulent access to confidential financial information (Rotenberg, 2001:205). In brief, institutions will have to comply with standards governing how non-public personal customer information can be shared with affiliates and third parties and how disclosure of their privacy policies is carried out (Stein, 2000:121).

2.7.8 The 21st Century

On 23 March 2000, the Personal Data Protection Law was proclaimed by the President of Latvia. The purpose of this Law is to protect the fundamental human rights and freedoms of natural persons, in particular the inviolability of private life, with respect to the processing of data regarding natural persons (Rotenberg, 2001:371). In the same year, the Czech Parliament enacted the Protection of the Personal Data Act of 2000 of the Czech Republic. This Act regulates the protection of personal data of natural persons and the rights and obligations arising within the data processing and it specifies the conditions under which personal data may be transferred to other countries (Rotenberg, 2001:382).

In Australia, the Privacy Amendment (Private Sector) Bill 2000 was passed by the Australian Parliament on 6 December 2000 and received Royal Assent on 21 December 2000. The new legislation, effective from 21 December 2001, contains amendments to the Commonwealth Privacy Act of 1988 and will regulate the handling of personal information by private sector organisations (Rotenberg, 2001:413).

On 21 July 2000, the United States Department of Commerce, responding to possible restrictions of personal data from Europe to the USA as a result of the European Union Data Privacy Directive, issued what is known as its 'Safe Harbor Privacy Principles'. The Safe Harbor programme was agreed to after the USA insisted that a voluntary approach to data privacy was better than a legislative approach. It took more than two years for the European Commission and the Department of Commerce to negotiate the contents of the Safe Harbor programme (Bureau of National Affairs, 2002h:191). Organisations in the USA acceding to the 'safe harbor' principles are seen by the USA as fulfilling the adequate protection requirement of the European Union Directive. It is interesting that the 'Safe Harbor' principles only apply to automated data and this is, in itself, a clear violation of the European Union Directive, which covers automated and manual types of data (Holvast *et al.*, 2001:14).

The Personal Information Protection and Electronic Documents Act of 2000 came into force in Canada on 1 January 2001. The Act establishes rules that govern the collection, use and disclosure of personal information in the private sector (Kirwin, 2002). The third stage of the Act will enter into force on 1 January 2004, when the law will extend to every organisation that collects, uses or discloses personal information in the course of a commercial activity within a province (Pitcher & Oorloff, 2002:1-2).

On 26 October 2001, President George W. Bush signed into law the USA Patriot Act of 2001. This Act, which arguably opens the door to invasion of privacy by the state, was introduced only days after the 11 September 2001 terrorist attacks on the World Trade Centre and the Pentagon. This anti-terrorism legislation is intended to expand the intelligence and law enforcement capability to identify and disrupt terrorist activities. The changes brought by the enactment of the USA Patriot Act will not only substantially affect individual privacy rights, but will also have broad ramifications for organisations, particularly those engaged in the provision of communications and financial services (Raul & Tyler, 2001:21).

The new European Union Directive on the protection of personal data and privacy in the electronic communications sector took effect on 31 July 2002. This new Directive introduces new rules on data retention and unsolicited commercial communications (Mason, 2002).

Thus, in today's information age, it is evident that protection of personal data transfers varies from nation to nation, as does the regulatory framework governing them. There has been marked shift in the direction of a global standard for information privacy modelled on the provisions of the European Union (Rudraswamy & Vance, 2001:133). It is clear that the European Union's 1995 Data Protection Directive constitutes the rules for the increasingly global character of data-processing operations. Its effect on countries outside the European Union is principally a penetrative one. The increasing global interdependence means possible consequences for those organisations that rely

upon the unimpeded flow of personal information, and which cannot claim to protect the data of consumers, clients and employees in ways that match the European standard (Agre & Rotenberg, 1998:111). In an interdependent world, the policy efforts of the Europeans carry externalities that force other countries to pursue policies that they would otherwise oppose or avoid. The alternative is to bear the costs of maintaining a different public policy. In addition, the general pressures to conform have increased as more and more countries have joined the 'data-protection club'. There is an increasing perception that adequate privacy protection is a necessary condition for being on the global information highway (Agre & Rotenberg, 1998:112).

As the global marketplace continues to expand, organisations face increasingly strict privacy and data protection regulations in a growing number or countries around the world. Many governments are following the lead of the European Union by developing omnibus privacy legislation to address public concerns about the protection of personal information (Pitcher & Oorloff, 2002:1). Regulatory frameworks with laws or a lack of laws in different countries can pose serious problems for transnational and multi-national organisations conducting business world-wide. This may have far-reaching social and ethical implications, particularly when those organisations fail to comply with the existing regulations that protect the privacy of the individuals or the entities involved. It is therefore important for multi-national organisations to understand the regulatory environment in different countries. This is also relevant when multi-national organisations focus on globalisation in order to diversify and expand potentially new markets to gain competitive advantage (Rudraswamy & Vance, 2001:128). Obviously South Africa can draw on the experience of Western countries. Whatever privacy laws the international community adopt, there will be strong and perhaps irresistible pressure on South Africa to follow suit.

2.8 SUMMARY

This chapter has introduced the concept of privacy from a constitutional perspective. In the Bill of Rights, Chapter 2 of the Constitution, South African citizens are guaranteed

(among other things) the right to privacy and the right to access of information. The Promotion of Access to Information Act 2 of 2000 was promulgated to give effect to the constitutional right of access to any information held by the state, as well as any information that is held by another person and that is required for the exercise or protection of any rights. However, this Act excluded private sector portions and data protection provisions. This led to a request from the Minister for Justice to form a Committee (Project 124) to investigate the privacy and data protection issue with the aim of improving existing legislation and adding new legislation. Because of the marked shift toward a global standard for information privacy, the chapter has also provided a brief historic overview of privacy and data protection in the international environment.

Several forces are working toward a global convergence of the conceptual content and legal instruments of privacy policies. These forces include shared technology and a well-networked global policy community. One problem in dealing with privacy issues is that not everybody is concerned with the same issues, at the same time, to the same extent, or in the same way, making legislation to protect privacy very problematic. Legislating this area is even more difficult in an international situation, and when one attempts to regulate the issue across different countries, as is currently the case.

The chapter concluded that South Africa has to adopt privacy and data protection legislation because of pressure from the international community and the fact that data privacy is becoming a global concern with transnational implications. South African organisations cannot ignore European Union privacy laws, since these laws have an impact outside the European Union, affecting South Africa as well.

The next chapter focuses on data protection as a privacy issue. Chapter 3 will addresses the information privacy issues surrounding the collection, use and dissemination of consumers' personal information in a commercial environment, as well as the responsibility of organisations to limit media intrusion and develop privacy practices and policies.

CHAPTER 3
CONSUMER INFORMATION PRIVACY

3.1 INTRODUCTION

One of the consequences of today's information society is the ease with which it has become possible to invade an individual's privacy. This has led to data privacy becoming a global concern with transnational implications. As mentioned in the previous chapter, the OECD has issued guidelines for privacy protection during the transfer of personal information across national borders for both the public and private sectors. Following the release of the OECD Guidelines, the Council of Europe opened for signature its Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, which latches on to the key principles in the OECD Guidelines. Not only have the European Union states nearly completed the process of adopting legislation to comply with the European Union's Data Privacy Directive, but other countries are also following these guidelines, including Canada, Mexico, Japan and Australia. Since there has been a notable shift toward a global standard for information privacy, modelled on the provisions of the OECD Guidelines, these directives guide the privacy discussion in this chapter. As a general rule, European countries approach privacy in an 'omnibus' fashion by passing privacy bills that address all the processes of data collection, use and sharing throughout society.

South Africa, on the other hand, has moved slowly toward establishing formal privacy mechanisms and to standardise privacy practices. The globalisation of markets, the growing pervasiveness of the Internet and the implementation of the Data Protection Directive bring new pressures to South Africa to align with global standards. The economic cost of comprehensive privacy regulation may be steep, but the same price could be exacted if there are no regulations at all, as growing sentiment abroad regarding strict privacy rules threatens to create barriers to global trade.

Although the Law Commission in South Africa has implemented Project 124 to consider the development of data privacy legislation, there is at present no separate Data Privacy Act in South Africa dealing with all the relevant data matters. As was discussed in Chapter 2, South Africa's Promotion of Access to Information Act emphasises the obligations of the state in the protection of personal data held by the state. It does not address the collection, use and dissemination of personal data by the private sector. This creates a need which this chapter will attempt to meet by focusing on the data protection aspect of privacy, as it relates to consumers' control over their personal data in the private sector.

Privacy is a multi-faceted concept encompassing a number of specific issues. 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 US, and 'data protection' in Europe is addressed as 'information privacy' in this chapter. Information privacy is viewed as the right to control information about oneself and should be distinguished from physical privacy, which is concerned with physical access to a person. It also differs from trade secrecy, which addresses ownership of intellectual corporate assets.

This chapter attempts to balance the information privacy issues of consumers in commercial activities with the advancement of a free international flow of personal data between countries, as stipulated in the OECD's Guidelines. The focus is thus 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. The underlying premise of information privacy in this discussion is that marketing organisations that collect personal information about individuals have certain responsibilities, and that individuals have a right to protect themselves from

organisations in possession of their personal information. The rise of the Internet, which permits organisations to obtain information about customers more easily than before, has brought privacy to the centre stage. Consumers have become more aware of their constitutional right to privacy as marketers and organisations continue to gather more personal information to gain a better understanding of consumers' spending habits.

3.2 INFORMATION PRIVACY AS A CONSUMER ISSUE

The concept of privacy has shifted from a civil and political rights issue motivated by polemic ideology to a consumer rights issue underpinned by the principles of data protection and by the law of trading standards. Privacy advocacy has been recast as a legal and a consumer rights issue. In the present-day context, privacy protection is widely perceived as constituting a set of technical rules governing the handling of data. While there are consequently more codes, conventions and laws in place than before, more data on more people is being collected by more powerful systems and for more purposes than at any other time in history. Many traditional rights have been put on a commercial footing, thus converting privacy rights into consumer issues (Agre & Rotenberg, 1998:143-4).

Consumers, to a greater extent than legislators, are forcing privacy onto the marketing agenda (Mazur, 2001:20). Many citizens have experienced quite distinctly and personally the potential dangers of unrestricted gathering and processing of personal data by others. As a corollary to these personal experiences, more and more citizens request individual privacy and data protection rights, above and beyond legislative attempts to control and regulate certain data processing technology (Agre & Rotenberg, 1998:225). Consumers' awareness of privacy issues has increased sharply as a result of the growth of the Internet. First, the Internet has prompted a huge increase in the number of people using computers. Second, several privacy-related incidents have resulted in considerable negative press coverage for organisations that invaded people's privacy improperly. Third, many organisations are using the Internet for marketing, sales or information dissemination. Finally, the Internet's international nature

presents new challenges to governments, technology developers and providers, enterprises and consumers (Loyle, 2002:50).

There are three potential areas for privacy abuse on the Internet. First, an increase in the ease with which people can be monitored; second, the potential use of database information distinctly different from its intended application; and third, a significant reduction in the cost of sending solicitations to prospective customers (Morris-Lee, 1996:40).

Blattberg and Deighton (1991:12) have noted the following information privacy issues that affect consumers: there is concern that much of the information is gathered without consent; consumers are not given the right to prevent transaction information from being sold or used; there is opposition to the proliferation of direct mail marketing and telemarketing to households; and the assumption is often made that better databases will lead to more solicitation. Some fear that information may fall into the wrong hands. There is also concern that personal information might be used in fraudulent schemes against naïve or unsuspecting people. More generally, there is a fear of the unfamiliar. Information that strangers are not supposed to know, used in ways that buyers never expected, gives an undue advantage to sellers in adversarial marketplace relationships. In order to identify and maintain socially responsible behaviour, an organisation continually has to monitor trends in the values held by society, because, as consumers are exposed to and gain a greater understanding of organisational practices, their values and expectations may change. Consumer's concerns regarding the privacy issue are very real, and any marketer that wants to achieve long-term success has to take these concerns into account. In reality, consumers have different thresholds of information privacy which are determined largely by the kind of information being collected, the organisation responsible, how the data is collected and the subsequent uses to which that information will be put (O'Malley *et al.*, 426).

Many believe that information is the true heart of the 21st century information revolution, just as electricity was the true heart of the 20th century's technological revolution.

Information is both a commodity to be bought and sold on an open market and an asset bestowing enormous competitive advantages on those with early or more complete access to it (Turner, 2002:1). Because of the information revolution, many consumers' right to privacy embodies two desires, namely the desire to be left alone and the desire to protect their confidentiality (Agre & Rotenberg, 1998:226; Devenish, 1999:146; Hagel & Singer, 1999:7; Longley & Shain, 1988:268; Joshi *et al.*, 2001:40). These two desires are of specific importance and relevance to this study. The empirical study aimed to measure consumers' concerns regarding the confidentiality of their information and their concerns regarding media intrusiveness (see Chapter 7).

The next section reviews the literature pertaining to the main area of study, namely consumer information privacy. Most of this chapter addresses consumers' desire to be left alone and their desire of confidentiality protection in an information-driven environment that places a renewed focus on the collection, storage, control, use and dissemination of personal information leading to consumers' desire to conceal information about themselves.

3.3 DESIRE TO BE LEFT ALONE

Privacy can generally be defined as the right to be left alone, free from intrusion or interruption (Department of Communications, 2000b:68). One of the privacy concerns of individuals and legislators is media intrusiveness. It is estimated that the average American consumer is buffeted by roughly a million marketing messages a year across all communications media (Hagel & Singer, 1999:7). Although legislators in various countries are addressing this threat, many consumers are acting on their own behalf by requesting marketers to remove their names from mailing lists. In the USA, some consumers take their right to be left alone a step further and participate in activities such as 'buy nothing day' or 'TV turnoff week' in an attempt to demonstrate that they are dissatisfied with the media's intrusiveness on their daily activities (Hagel & Singer, 1999:8).

3.3.1 Media intrusiveness

Much of the direct communication received by consumers is from organisations prospecting for new business. New business is the lifeblood of any organisation and consequently marketers are constantly trying to acquire new customers. Unfortunately, consumers have little or no control over the prospecting efforts of organisations (O'Malley *et al.*, 1999:427). **The issue of media intrusiveness is of specific importance to this study and was measured in the empirical survey as discussed in Chapter 6**. The sheer volume of direct mail, telemarketing and e-mail relates to the physical intrusion of marketing communications into the daily lives of consumers (Katzenstein & Sachs, 1992:71).

Unfortunately, most marketers believe in the 'law of big numbers'. This law states that the more interactions marketers have with many consumers, the more they can learn from their buying patterns (Bhatia, 2001:110). This point of view leads to media intrusiveness. Ten years ago, many consumers responded politely to telemarketers who called them at home during dinner. Today, people resent the imposition and many simply hang up. Consumers may soon demand that telemarketers reward them, just as people now routinely receive compensation for participating in focus groups (Hagel & Singer, 1999:11). Consumers' privacy can be intruded upon by unsolicited communication through media such as postal mail, telephone, fax, e-mail or short message systems (SMS).

3.3.1.1 Unsolicited mail, telephone and fax advertising

Unsolicited mail is sent by organisations that market their products and services by means of postal mail. Many consumers refer to these types of communication as 'junk mail'. Marketers need to be more protective of their consumer lists. Over-use of consumer lists can contribute to problems associated with unwanted and unsolicited postal mail communications such as the 'junk mail' image (O'Malley *et al.*, 1999:442).

Unsolicited commercial faxes are banned in the USA under the Telephone Consumer Protection Act, under which the Federal Communications Commission regulates marketing. Many writers have argued that unsolicited fax advertising unfairly transfers the cost of such advertising on consumers who did not want to receive this advertising (Hovanyetz, 2002f).

A special concern to marketers is the perception that the telephone is an especially intrusive marketing medium (Roberts & Berger, 1989:441). Many consumers are annoyed by telephone sales pitches interrupting their dinner. The rise of telemarketing over the past decade has motivated many consumers to end this media intrusiveness. **This situation is relevant to the research, and the empirical study aimed to measure South African consumers' concerns regarding telemarketing and this medium's possible intrusiveness.**

Consumers in the USA have signed 'do-not-call' lists in 28 states that have enacted or implemented their own registries to stop telemarketers from calling (Smith, 2002:3; Hovanyetz, 2002e). The rest of the states have legislation pending for similar laws, with many expected to enact ordinances during 2002 and 2003 (Odell, 2002b). The Federal Trade Commission (FTC) proposed a national do-not-call system, where consumers could call a toll-free number to place their phone number on a national do-not-call registry (Direct Marketing Association, 2002b). The proposal for the registry was first announced in October 2001 as a key component of the Commission's privacy initiative. The proposed amendments are designed to prevent deceptive telemarketing practices and to enable consumers to exert greater control over when and whether to receive telemarketing calls in their homes (Schultz, 2002a). The 2002 deadline for comments on the proposed national do-not-call list has been extended due to a large response from Americans. The FTC has received more than 21 000 e-mail comments on the national do-not-call list. This issue has generated the second highest response of any issue put forth by the FTC, with only smokeless tobacco receiving more comments in the early 1990s (Hovanyetz, 2002d).

The reason for a uniform national do-not-call list is to ensure that marketers and consumers are not disadvantaged by a costly patchwork of differing state laws. The national do-not-call list should be in place by the end of 2002 or early 2003 (Hovanyetz, 2002a). The national proposal would allow consumers to place a call to the FTC and ask to place them on the national do-not-call list (Gruenwald, 2002). Consumers will also be able to allow access to certain organisations or block calls only during certain hours (Campanelli, 2002). After consumers' contact details have been listed, it will be illegal for a telemarketer to call that number. Telemarketers will be able to access the do-not-call lists via the Web and will be required to remove the numbers of all consumers who have placed themselves on the national suppression list from their own databases (Stern, 2002). Illinois, one of the states in the USA, is the first state that signed a bill into law that bans unsolicited calls to cellular phones. According to Alberta (2002b) the ban was due to take effect on 1 January 2003. Illinois residents are charged $5 to have their names and phone numbers placed on the do-not-call list maintained by the Commerce Commission at an annual cost of $1 million. The programme is partially funded by telemarketers who are charged up to $1 000 for a copy of the state's do-not-call list.

The Direct Marketing Association (DMA) in the USA opposes national do-not-call lists because it argues that this legislation punishes reputable marketers for the sins of fly-by-night scammers. The DMA points out that the private sector has been self-regulating the telemarketing industry since 1985 through the DMA's Telephone Preference Service (TPS), Mail Preference Service (MPS), and other industry guidelines. They believe that their TPS covers about 80 per cent of national outbound telemarketing calls, a service to which 4.1 million Americans subscribe (Direct Marketing Association, 2002b). However, Winston (1999:65), a specialist in direct marketing law, believes that do-not-call lists are proliferating in the USA due to the inadequacy of the DMA's Media Preference Services. The DMA is concerned that the new national do-not-call lists will especially hurt employment in the industry and cripple the ability of non-profit organisations to raise funds (Direct Marketing Association, 2002a). They have urged the FTC to be careful in weighing the merits of the proposed registry because more than six

million jobs and $668 billion in telesales in the USA (Direct Marketing Association, 2002b). The FTC says that the public's overwhelming reaction to state do-not-call lists indicates consumers' concern about their privacy, and that includes unwanted intrusions and unwanted phone calls at the dinner hour (Mayer, 2002:7). Unfortunately, the FTC does not have the authority to regulate banks, financial services and telephone companies, the latter being one of the biggest telemarketing industries in America (Oldenburg, 2002:1; Hovanyetz, 2002c).

If a consumer's name appears on a state's do-not-call list and a telemarketer calls that individual on the list, the organisation could face fines up to $25 000 (Alberta, 2002a). Some consumers feel so strongly about media intrusiveness, especially telemarketing, that they have created there own ways to stop unwanted calls. One American citizen created a website to guide laymen on how to prosecute telemarketers. Other websites are less serious, for example a website selling anti-telemarketer T-shirts and caps. This has been followed by various anti-telemarketing products, such as the TeleZapper, which is a device that plugs into a phone, and when a telemarketer's computer dials the consumer's number, the phone emits the same tone as a disconnected line (Oldenburg, 2002:1). Other electronic devices designed to screen telephone solicitation calls include the Phone Butler which screens calls and informs telemarketers to put the number on their do-not-call list; the Call Screener which can send messages to telemarketers as well as emit dialer-discouraging tones; and the TriVOC unit which creates an extension number that can be attached to its own answering device and can be used for screening (Hovanyetz, 2002b).

In South Africa, there are no special laws restricting access to customers via the telephone, mail or fax. Therefore, the South African Direct Marketing Association's (DMA) Code of Practice, which regulates direct marketing conduct, covers largely unlegislated territory. If South African consumers want to eliminate unwanted calls or stop receiving mail solicitations, they can register with the DMA's Media Preference Services. The Media Preference Service (MPS) of the DMA comprises three distinct areas of consumer preference. First, there is the MPS option, which allows consumers

to opt out of receiving unwanted direct mail. Second, there is the Telephone Preference Service, which allows consumers to restrict unwanted telemarketing calls. Third, there is the Fax Preference Service, which provides for the suppression of fax marketing. Since the DMA has enhanced a culture of respect for consumer choice, all members are subjected to an adherence of the Code's mandatory privacy guidelines (Direct Marketing Association, 2001a:13).

The MPS is a database of information about individuals who have asked to be excluded from mail, telephone and fax marketing. The service is managed and administered by the DMA and is provided at no cost to DMA members. Each quarter a copy of the database is made available to subscribers. This file copy is used by organisations to flag the records on their own databases of consumers who have registered with the MPS. The flagging enables organisations to prevent the use or disclosure of these individuals' information for marketing purposes. The facility is provided at no cost to consumers and details are retained on the MPS file for five years. To ensure the accuracy of information and protect the interest of consumers, the registration process must be in writing. From a consumer perspective, the MPS affords consumers the right to marketing privacy at a national level. Marketers, on the other hand, are able to use the MPS to demonstrate their commitment to consumer privacy and to remove consumers who do not wish to be contacted from their lists.

3.3.1.2 Unsolicited e-mail advertising

The number of electronic mailboxes world-wide was estimated at 569 million in the year 2000, an average of 1.8 mailboxes per Internet user. Every day, these inboxes are inundated with hundreds of commercial messages, underscoring the fact that e-mail is not only a means of interpersonal communication, but is also a powerful and cost-effective business tool (Gauthronet & Drouard, 2001:5). People who screen their bulging e-mail inbox probably have a dire need for a law regulating unsolicited electronic messages, known as 'spam'. Spam refers to the bulk sending of unsolicited e-mail advertisements to large numbers of Internet and e-mail users. The term 'spam'

was derived from a Monty Python sketch set in a cafeteria, where the word 'spam' takes over each item on the menu until the entire dialogue consists of the word 'spam'. As this situation so closely resembles what happens when mass unsolicited mail takes over mailing lists, the term has subsequently come into common use (Judin, 2000:35). The first spam was sent in 1997, but has now become a part of everyday life for computer users (Gay, 2002). With all the efficiency and speed of communication that e-mail brings into consumers' social and business lives, spam is an unavoidable side-effect which is here to stay for the foreseeable future. It is a sacrifice of privacy that every e-mail user makes when connecting to and enjoying the benefits of the Internet (Judin, 2000:37).

There are many signs of a growing shift in expenditure from direct marketing to the Internet, particularly e-mail marketing. There are three main reasons for this. The first is the fact that the cost of launching an advertising campaign on the Internet is a fraction of the cost of using traditional media. The second reason is the sales conversion ratios for e-mail marketing are 5 to 15 per cent, compared to half a per cent to two per cent for conventional mailings. Third, there is a trend towards e-mail marketing at the expense of banner advertising on the Internet (Gauthronet & Drouard, 2001:13). The popularity of e-mail marketing for organisations has, consequently, resulted in mass mailings to consumers' e-mail addresses.

As e-mail addresses can be obtained from a number of sources on the Internet, a lucrative trade has developed in compiling and selling mailing lists. E-mail addresses are extracted from the Internet, compiled into mailing lists and sold to marketers, who then use such lists to send unsolicited e-mails to large numbers of Internet users (Judin, 2000:35). Spammers often hide their return e-mail addresses so that the recipients cannot reply to the spammer. Other unscrupulous tactics include spamming through a legitimate organisation's e-mail server so that the message appears to be originating from an employee of that organisation (Roberts, Feit & Bly, 2001:144).

Surveys show that the spam plague is worsening. Jupiter Media Metrix, a United States company that monitors Internet business trends, predicts that spam levels will treble by

2006, with the average e-mail recipient receiving 1 400 messages a year (Gay, 2002). EarthLink Inc, the third-largest Internet service provider in the USA, has won a $25 million lawsuit against a spammer that used the company's network to send an estimated 1.25 billion junk e-mails since the year 2000. This is believed to be the largest fraudulent spam judgement since the Internet was created (Credeur, 2002).

In the USA, 22 states have laws governing the distribution of commercial e-mail to individuals and organisations (Colker, 2002; Nethaway, 2002). California's anti-spam law, for example, prohibits marketers from sending e-mail to anyone who has not 'opted-in' (consented to receiving future offers) to receive messages, or to anyone they do not have a prior business relationship with. Unsolicited commercial e-mails also clearly have to designate the content of the messages in the subject lines. A subject line has to contain the legally required characters 'ADV:' to indicate that it is a commercial mail message, or 'ADV:ADLT' for e-mail messages of an adult nature (Tomasula, 2002a). Filters on e-mail programmes can be set to detect those characters and delete the messages before they appear in an inbox.

The Japanese government is moving toward similar measures and plans to implement a revised ordinance regulating the transmission of unsolicited commercial advertisements via mobile phone and computer by the end of 2002. This law will also require marketers to positively indicate their e-mail addresses, identifying 'advertisement' in the subject line and give consumers the option of specifying that they do not want to receive future offers ('opt-out') or future communications (Bureau of National Affairs, 2002c).

China's largest Internet companies have formed a coalition intended to crack down on unsolicited e-mail, following reports that many North American and European servers routinely block all e-mail from China because of the inordinate number of spam messages relayed through servers there. In response to the negative attention, several of China's largest Internet Service Providers signed an agreement on 25 March 2002, pledging to crack down on the distribution of spam. They also proposed establishing a

'China Anti Junk Mail Association' to gather and publicise information on servers that accommodate spammers (Lovelock, 2002).

Software companies such as TruSecure, Symantec and McAfee sell products and services to organisations to keep out spam in two ways: by identifying words used frequently in the subject lines of unwanted mail, and by 'blacklisting' the mailbox addresses of frequent spammers (Naraine, 2002; Hirsh, 2002c).

Part of the spam problem is that the anonymous nature of the Internet makes it difficult to track down those who send illegal messages. For computer users to gain true redress, one would have to co-ordinate millions of users to give power to an individual (Colker, 2002). Another problem is the difficulty to distinguish between spam and legitimate e-mails, and between spam and proper marketing activities (Hirsh, 2002b). A survey conducted by the European Commission in 2001 indicates that it costs consumers an estimated $8.8 billion a year in connection costs just to receive the unsolicited e-mails (Colker, 2002). Current technology allows a single cyber-marketing company to send half a billion personalised advertisement mails via the World Wide Web everyday. The study's analysis of e-mail marketing concentrates on the most-developed market, the USA, and details how, in response to the rapid growth of unsolicited mail, the e-mail marketing industry is working with Internet users towards systems of data collection and exchange based on the express permission of the user. The European Union's Directive favours the 'opt-in' approach. This is supported by a study which found that, from the point of view of the industry, 'permission based marketing' is proving a more effective and viable method of data collection (Gauthronet & Drouard, 2001:23).

Seth Godin, a computer scientist and marketing graduate, coined the term 'permission marketing', which has been copyrighted by Yahoo. He believes that an increasing number of advertisers attempt to stand out from the crowd, but only create apathy and confusion. He appeals to advertisers to move away from 'interruption marketing' to permission-based direct marketing, in other words, to communicate with customers and

prospects on a voluntary basis, slowly building first interest and then trust (Godin, 1999:75).

The European Council introduced new rules for unsolicited e-mails in its Electronic Communication and Data Privacy Directive, which apply to all 15 European Union Member states. According to this Directive, there is a European Union-wide opt-in for unsolicited e-mails in cases where there has been no prior customer contact. Once an e-mail address has been acquired in the context of the sale of a product or a service, an organisation may send marketing e-mails for its own products and services without prior consent of the recipient. The Directive is expected to take effect in October 2003 at the latest (Tandberg, 2002).

South Africa's jurisprudence on this topic is virtually non-existent. The Advertising Standards Authority (ASA) regulates advertising in South Africa with the purpose of monitoring and controlling commercial advertising and dealing with complaints from the public. The DMA of Southern Africa has established guidelines in respect of unsolicited marketing e-mail and is working with the International Federation of Direct Marketing Associations (IFDMA) to create an international E-mail Preference Service (Judin, 2000:36; Direct Marketing Association, 2001a:13). The guidelines include the full codes of practice of the DMA, the ASA and the Harmful Business Practices Act, together with other relevant industry laws and codes synthesised to take into account South African realities. These guidelines on information practice stipulate the following regarding unsolicited e-mail marketing (Direct Marketing Association, 2001b):

- E-mail solicitations should be clearly identified, and the e-mail address of the marketer must be stated.
- Irrespective of whether marketers have a previous business relationship with the consumers, they should provide a mechanism for individuals to have their name and address removed from the database for further solicitations, or to have their information suppressed for any purpose they choose.
- Information should be given about e-mail tracking when the consumer opens the solicitation.

- Persons involved in the rental, sale or exchange of lists of data for online solicitations should take reasonable steps to ensure that such sharing adheres to industry principles.
- The opt-out provisions apply to rental, sale or exchange of lists or spaces in chat rooms.

Two important groups have launched programmes to help consumers distinguish between legitimate e-mail pitches from marketers and other unsolicited e-mail, which may be sent by scam artists or pornographers. The website privacy certification organisation TRUSTe and the privacy consultancy ePrivacy group launched a certification and seal programme for commercial e-mail in February 2002. It is called Trusted Sender. The programme places a seal in the top right corner of each e-mail message from a Trusted Sender programme participant. The seal is intended to allow consumers to verify that the message is not spam and that the organisation sending the message is in compliance with the programme's guidelines (Schultz, 2002b). Such e-mail must include the identity of the sender and must provide consumers with a way to opt out of receiving future e-mail from the sender. Many, however, believe that the main problem is not distinguishing between legitimate commercial messages and spam, but rather keeping the spam from getting into a consumer's mailbox at all (Bureau of National Affairs, 2002b:107).

Although mainstream marketers have, by and large, accepted permission e-mail marketing, there is still much debate between marketers and anti-spammers over what are/are not acceptable e-mail address gathering practices (Magill, 2002). In addition, the definition of e-mail is currently still very broad and it also covers 'short message services'. Section 3.3.1.3 addresses unsolicited SMS messages and their effect on consumers' desire to be left alone.

3.3.1.3 *Unsolicited SMS advertising*

The Short Message Service (SMS) revolution can provide a growth opportunity for direct marketers. SMS and location-targeted messaging provide opportunities to send information directly to mobile phone users. Mobile phone network owners have vast customer bases. It is also possible for third-party organisations to build their own lists of mobile numbers via website promotions. They can then use these lists for targeted marketing, if users have opted in by leaving their details on a website. The danger is that some organisations may sell such lists to other organisations, which can then send random messages to mobile users. This situation can potentially be abused.

The advantage of an SMS is that the messages can be timed and personalised. The main barrier is again the intrusion factor. For location-specific services, mobile phones have a unique strength. Since it is a device most users have on them nearly all the time, some people may begin to expect to receive appropriate SMS messages. For example, an airline passenger's phone may ring as (s)he passes a duty free shop, inviting the recipient to take up a special offer (Furber, 2001:23). The Mobile Marketing Association (MMA) in the USA is taking tentative steps to regulate location-based advertisements with the introduction of a set of preliminary standards for wireless advertising to promote consumer privacy. The MMA and other similar groups aim to ward off potential privacy concerns before the technology becomes nationally available. The guidelines include stipulations that members are not allowed to merge information on users' location with private data, unless consumers consent via a double opt-in process. They also specify that members must have consent before sharing subscribers' information with third parties (Saunders, 2002). The new European Union Directive on the protection of personal data and privacy in the electronic communications sector indicates that the use of mobile phone location data should be subject to the explicit consent of phone users (Mason, 2002).

The Marketing Federation of South Africa (MFSA) has recently formed an e-Business Portfolio Committee which has developed a Code of Practice for e-Business and SMS

marketing. One such code is the SMS Code of Practice, which was drafted in 2002 with the participation of Cell-C, MTN, Vodacom and other service providers. The aim of this code is to protect consumers by preventing unsolicited SMS messages, providing a channel for resolution, promoting responsible use of SMS messages as a marketing medium and limiting the use of SMS messages to commercial messages to consumers. The committee has realised that consumers can perceive commercial SMS messages as intrusive, as there are no clear opt-out options and there is often no indication of who has sent the SMS (Marketing Federation of South Africa, 2003).

The use of marketing data does, however, extend far beyond the desire of an individual to avoid receiving too much postal and electronic mail (spam), or too many unsolicited telephone calls. The provision of sensitive information about a person's buying habits could also result in adverse privacy implications for the individual. Nevertheless, despite the current antagonism, marketers and consumers have at least some complementary needs: consumers need the goods and services that marketers sell, and marketers need consumers to buy these goods and services. This raises the issues of how to treat customers, and of how marketers should protect consumers' confidentiality during and after transactions.

3.4 DESIRE TO PROTECT CONFIDENTIALITY

In recent years, the ability to gather and use confidential consumer information in commercially desirable ways has increased substantially. Advances in technology have made collecting, sorting and disseminating this information easier than before. In addition, the growing popularity of e-commerce has led organisations to offer more services over the Internet, leading to an increase in the volume of personal information in circulation (Smith, 1999:8). Many people perceive there to be a threat to their individual privacy owing to the increasing power of the information-processing technology used to collect, store, analyse and exchange vast amounts of information about them. Unfortunately, their information is often used for the benefit of the

organisation and little protection is provided to the individual who is the source of the data (Collier, 1995:41).

South African consumers have recently demonstrated that they have a desire to protect their confidentiality. Early in 2002, EasyInfo.co.za (South Africa's first online telephone directory) launched a directory of 2.5 million names and addresses (including thousands that are unlisted in the white pages of Telkom directories). Soon after, EasyInfo, newspapers and radio stations were bombarded by complaints from consumers about an invasion of privacy. Initially, EasyInfo removed approximately 800 names from the directory, but only weeks later, EasyInfo had to close its information site containing confidential information of Telkom customers. Telkom also ordered EasyInfo to hand over all customer confidential information and disclose all third parties to whom the information had been made available (Marud, 2002:1; Venter, 2002:3).

Perceived invasions of privacy depend on the reputation of the organisation involved, the knowledge which consumers possess about the particular processes of data collection used, and the specific uses of the information. They also depend on the extent to which consumers believe the offer or request to be relevant, the degree of sensitivity they associate with the particular information being collected and any negative consequences likely to result from information collection (O'Malley *et al.*, 1999:433).

The world economic system's transformation from a dominantly mass-production model to a mass-customisation model is seen as creating an enormous demand for detailed data on the behaviour of consumers. If goods and services are to be customised, it follows that organisations must have access to detailed customer information. Increasing fragmentation of mass audiences also creates a demand for data about actual and potential users of specialised media channels (Agre & Rotenberg, 1998:277).

As has been mentioned in Section 2.7.3, the OECD has issued guidelines for data protection in the transfer of personal information across national borders. Since many

global standards for information privacy are modelled on the provisions of the OECD Guidelines and the European Union Directive, these guidelines are incorporated in this chapter. The guidelines can be summarised as eight principles as follows (and are discussed in detail the next section):

- First principle: Collection limitation
- Second principle: Data quality
- Third principle: Purpose specification
- Fourth principle: Use limitation
- Fifth principle: Security
- Sixth principle: Openness
- Seventh principle: Individual participation
- Eighth principle: Accountability

The remainder of this chapter links the consumer's desire to protect his/her confidentiality with the eight guidelines issued by the OECD. Each principle guideline is discussed under the relevant heading. They are not presented chronologically. Instead, the eight guidelines have been incorporated into seven areas pertaining to data collection, data storage, data control, data use, data security, data disclosure and privacy policies. The discussion focuses on the afore-mentioned issues as they relate to consumers' activities during commercial transactions.

3.4.1 Data collection

One of the first principles of the OECD Guidelines is the limitation regarding the collection of personal data. This guideline states that any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge and consent of the data subject (Rotenberg, 2001:268). One problem is that data protection laws do little to prevent or limit the collection of information. Many Acts merely stipulate that information has to be collected by lawful means and for a purpose directly related to a function or activity of the collector. Thus, a virtually unlimited number of information systems can be established without any breach of law (Agre & Rotenberg, 1998:156).

Although record-keeping has always been a part of organised society, the amount of data collected in the past was constrained. Because of access and storage problems and the inability to integrate and correlate data with speed, it was impractical to develop large databases prior to electronic processing. Currently, the ability of computers to process, store and retrieve vast quantities of data at high speed has led to the collection of pools of data that constitute comprehensive personal dossiers (Hussain & Hussain, 1992:151). **This issue is relevant to the study and consumers' concerns regarding the collection of excessive information by organisations are measured in the survey, as discussed in Chapter 6.**

Personal information has a market value. So, for example, marketers can determine from such information where to direct their advertising to optimise value and cost (Hussain & Hussain, 1992:157). An important debatable issue is who has rights to the data generated by an organisation's database. Some argue that, if personal information is so valuable, the individual should be paid for it. As a result, the fight for control over personal data that is electronically collected and digitally manipulated, usually without the permission or knowledge of the person involved, could lead to a new definition of privacy rights in the information age (Massey, 2000:19). **The collection of information from consumers without their permission is important to this study and forms part of the concerns measured in the empirical survey.**

Many consumers and consumer protection groups fear that organisations will use the opportunity which the Internet provides to capture information about unsuspecting people who visit their websites. By merging this information with a wide range of publicly available data, those organisations will accumulate vast databases about their customers (Hagel & Singer, 1999:8). In supplying personal information, consumers should consider the possible consequences of their submitting such information. This is especially true if these consequences are negative. In an effort to minimise such effects, consumers may actively avoid situations in which they would be required to give information, they may refuse to give information, or they may provide incorrect

information (O'Malley *et al.*, 1999:435). If marketers 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 a choice between opting in and opting out.

3.4.1.1 Opt-in versus opt-out

Marketers should start treating consumers as joint owners of data. The authorised uses of the data (both internal and external) must be clearly communicated and negotiated at the time of data collection. Marketing organisations normally offer consumers two choices during data collection: opt-out or opt-in. Opt-out means that an individual specifies that (s)he does not want to receive particular offers at his or her address or other contact points. This option is similar to that chosen by those individuals who write to the DMA and ask to have their names and personal information removed from the circulation of future marketing offers (Schwartz, 1998:51). When consumers choose the opt-out option, they object to the secondary use of their information, which is a way to request that the organisation does not use their information for certain purposes or sell it to others.

Opt-in implies that an address has been approved by the individual residing at that address. This consumer has consented to receiving specific types of offers and customer correspondence from a particular organisation and/or all of its offers. While responsible marketers use opt-in lists where possible, the compilation of these lists can only be done when each consumer expressly indicates that he or she wants to receive future communications (Bureau of National Affairs, 2002a). Some believe that the only way to ensure that a consumer has truly consented to the terms is an opt-in agreement. If the organisation at some future point wishes to renegotiate the 'contract' on new terms, each consumer in the database must be contacted with an offer. Only if a consumer has indicated consent to the revised terms can the new use of the data proceed (Smith, 2001:20). **The opt-out option is of particular relevance to this**

study, and the empirical survey measured consumers' concerns about the opportunity to remove their names from mailing lists.

Many marketing organisations fear the opt-in mechanism, apparently because of concerns that, given full disclosure of data uses, few customers would be convinced that the benefits of allowing such uses outweigh the perceived costs. However, for an organisation that owns a database, the set of consumers who select to opt in, would represent a true treasure: a group of customers who have stated an overt desire to embrace targeted marketing through secondary data use (Smith, 2001:20). Studies have indicated that three in ten consumers opt out of providing consent, but only one in 10 opts in, making the opt-out the preferred consent for marketers (Bureau of National Affairs, 2002a). Cate and Staten (2001) believe that an opt-in system is always more expensive than an opt-out system because the opt-in system fails to harness the efficiency of having customers reveal their own preferences as opposed to explicitly having to ask them. They reason that an opt-out system sets the default to 'free information flow' and lets privacy-sensitive consumers remove their information from the system. By contrast, an opt-in system sets the default rule to 'no information flow', thereby denying to the economy the very lifeblood on which it depends.

The California Chamber of Commerce and other members of the Alliance for Fair Information Practices in the USA have released a report which concludes that opt-in proposals could cost California consumers, employees and taxpayers several billion dollars. The report indicated that an opt-in regime would cost California charities $1.57 billion in revenue lost to programmes that reduce the California tax base by $2.1 billion within several years. The purpose of this report is to urge lawmakers to maintain a balance as they continue to debate this important issue in future (Main, 2002).

The European Union's Directive does not specify that consumers either opt in or opt out, leaving the decision up to the individual countries. Some countries, such as the United Kingdom and South Africa, favour the opt-out system for data for third-party use (implying that an organisation cannot share the customer's information with a third party

if the consumer has barred information sharing), while Italy favours the opt-in system (meaning that an organisation cannot share the data with a third party unless the consumer gives explicit permission). Such permission also varies from country to country, with some requiring written permission and others allowing consent via electronic means (Banham, 2000:60). The European Union's new Directive on the protection of personal data and privacy in the electronic communications sector, however, has changed the current United Kingdom position, requiring unsolicited commercial communications, such as e-mail, text messages, faxes or telephone calls from automated calling systems to be sent only on an opt-in basis. This means that consumers must indicate that they are willing to receive such communications before they can be legally sent (Mason, 2002).

In addition to choices between opting in and opting out during data collection, there is also an international trend to specify the purpose for which the personal information is collected.

3.4.1.2 Purpose of data collection

The third principle of the OECD Guidelines relates to purpose specification. This means that the purposes for which personal data are collected should be specified at the time of collection (Rotenberg, 2001:268). Although several laws regulate privacy issues, and there are different rules for financial, medical and communication information, a global trend is developing, namely to inform consumers when gathering their information about the purpose for which the information is gathered, and then to use it only for that purpose (Floor, 2001:41). Consumers should be able to indicate, at the time when information is supplied, whether they wish that data to be divulged for commercial applications or uses other than those for which they were informed it was originally collected (Wientzen & Weinstein, 1997:89).

In South Africa, marketers are not required to inform consumers about secondary uses of data (that is when personal information is collected for one purpose but used for

another). Nor are marketers required to give consumers the right to stop those uses. **This is relevant to the empirical study and specific items in the measurement instrument addressed the issue of purpose specification.**

Over the past few years, some organisations have provided opt-out capabilities for consumers. Unless a consumer takes overt action to opt out of the secondary data uses, it is assumed that the consumer has assented to these uses. By contrast, with very few exceptions, the use of personal data in Europe is prohibited if the consumer objects to the secondary use. Usually, the consumer is given a clear and overt notification of the intended uses at the time of data collection and is, at that point, given an easy option (often a check-off box) to object to the secondary use. If the organisation later realises that it wanted to use the collected data for a new purpose, it is obliged to contact the consumers and allow them to object, However, some European countries demand that an opt-in approach be used for all secondary uses, and an opt-in provision must be used in any European Union country if the profiles include special categories of data such as those indicating ethnic origin, religious beliefs and data regarding a person's health or sex life. When an opt-in plan is in effect, an organisation cannot assume that the lack of a consumer's objection implies consent. In addition, consumers must be allowed to inspect and correct the information about them (Smith, 2001:10). According to the European Union (EU) Directive, citizens also have the right to prohibit the processing of personal information for the purposes of direct marketing. Further regulations concern the effective enforcement of individual claims and monetary compensation for established violations (Agre & Rotenberg, 1998:234).

The pervasive spread of computer networking has also had numerous effects on data collection (Rotenberg, 1999:3). Computer networking provides an infrastructure for a wide variety of technologies that identify and track the movements of consumers on the Internet. One very controversial data collection device is known as a 'cookie' and is discussed below.

3.4.1.3 *Data collection devices*

Information collection devices embedded in Internet browsers, and known as 'cookies', enable a website to identify users and recognise them when they log on in future. Cookies are small pieces of code used mainly by commercial websites to track Internet users. They may be set to follow Internet users from one website to another, collecting information about the personal browsing habits of the visitor for advertising and marketing purposes (O'Shea, 2000:26). Cookies are downloaded to a person's hard disk by the browser and are used to recognise and authenticate individuals when they return to a website and permit access without logging in every time. Some cookie devices, such as those involved with an online purchase, only last for a short period of time. This type of cookie can serve as a shopping cart for an electronic commerce website for the browser to remember the items a consumer wanted to purchase, even if (s)he leaves the site and returns later. Others cookies can last much longer, potentially creating a record of someone's surfing activities over several years. This type of cookie records the links or advertisements that a consumer clicks on and adds that information to a profile of the consumer's interests located in a cookie file (Roberts *et al.*, 2001:205). Web browsing software can be configured to warn someone when a site tries to install a cookie, and it can even be set to automatically reject the code. However, there are concerns that less technically adept people will not consider using such settings (Wearden, 2002).

The European Parliament is planning to introduce new legislation to ban the use of cookies on websites, unless an opt-in consent has been received from consumers. Members of the European Parliament have passed a Privacy and Electronic Communications bill which requires all websites to request their users for permission before cookies are delivered. The bill still needs approval from each of the 15 European Union governments to become law (Bremner, 2002b).

Critics of the legislation argue that it will add another layer of bureaucracy and potentially rob e-business of a quick and easy way to track their customers' activities.

They believe that the legislation will make shopping online more cumbersome, and that it could have large financial implications for organisations because cookies enable them to track customers in a cost-effective way. This legislative process is strongly opposed by leading representatives of the e-business industry. The Interactive Advertising Bureau (IAB) and the DMA have joined forces to protect the use of cookies. The DMA argues that cookies do not breach anyone's privacy since they cannot be used to identify an individual's actual identity. They further explain that cookies store a unique reference number which allows websites to carry out a number of valuable functions such as tailoring pages to the browser (Anon, 2002b). The DMA's Code of Information Practice states that websites should have a clear policy regarding their use of cookies, which informs consumers that they can set their web browsers to alert them that a cookie is being received (Direct Marketing Association, 2001b).

3.4.2 Data storage

The second principle of the OECD Guidelines is data quality. This embodies the notion that collected data should be relevant to a specific purpose and be accurate, complete and up-to-date (Rotenberg, 2001:268). Every organisation with computerised files containing data of a personal nature has an obligation to ensure that such data are accurate, updated, kept confidential and used for restricted purposes (Hussain & Hussain, 1992:156). If consumers are concerned when organisations utilise their data for commercial purposes, or pass that data on to third parties, then these concerns may be compounded further when their data are inaccurate. Concern in respect of the accuracy of data held may be heightened in certain circumstances. If, for example, the data relates to the credit history of the consumer, then the possibilities of negative consequences of inaccuracies are high. Inaccuracies in financial data may result in the consumer is being turned down for a loan or bond. Some consumers believe that the large amounts of unsolicited and irrelevant direct communications they receive result from inaccurate data (O'Malley *et al.*, 1999:429). Maintaining data accuracy should be of paramount importance to industry participants, since accurate data facilitates the building of consumer relationships. The point is that if organisations intend to utilise the

personal details of consumers for marketing or other purposes, then the onus is on the organisations to ensure that the information they hold is correct (O'Malley *et al.*, 1999:429). Although providing customers with access to their information entails some additional costs for most organisations, these organisations may find themselves in possession of a 'clean' database that can be mined with no fear of backlash (Roberts, 1997:27). **Data accuracy is of specific importance to this study and was addressed in the empirical survey.**

Privacy has become a public issue, as increasingly powerful computers have decreased costs and made possible the management of extremely large volumes of personal information. Even small organisations now have the ability to collect, store, process and disseminate significant amounts of data (McDonald, 1998:107). Technology, in the form of a database, provides marketers with the ability to store customer information and develop interactive relationships with individual customers. The existence of a database enables management to track and evaluate the effectiveness of each customer contact. A customer database can be used by marketers to solicit sales, qualify and track sales leads, provide sales support and customer service and manage customer relationships (Roberts, 1997:27). The assumption is often made that better databases will lead to more solicitation, but some believe that more precisely targeted communications will seem less intrusive than broadcast advertising or indiscriminate junk mailing (Blattberg & Deighton, 1991:5,8).

In order to survive in today's economy, organisations must have access to the most up-to-date customer information possible. Organisations have to be in control of the data disposal issue, rather than allowing it to snowball into an overwhelming problem. Data quality is important when organisations are actively involved in customer relationship management (CRM). Poor data quality significantly impairs the effectiveness of CRM initiatives, hence reducing the return on investment. Data clean-up projects can generate financial benefits, even if those benefits are not immediately visible or directly tied to the bottom line (Hirsh, 2002a).

The age of high-tech sales data collection was supposed to help organisations acquire new customers and retain existing ones. However, having too much information about potential purchasers can be costly, particularly if the information has become outdated while in storage (Hirsh, 2002a). A new law in the USA, called the Data Quality Act, requires the United States government to set standards for the accuracy of scientific information used by federal agencies. The law, which took full effect on 1 October 2002, creates a system under which anyone can point out errors in documents. If an error is confirmed, an agency has to remove the data from government websites and publications (Raney, 2002).

3.4.3 Data control

The seventh principle of the OECD Guidelines is individual participation. An individual should have the right to access, confirm and demand correction of his or her personal data (Rotenberg, 2001:268). As computing systems increasingly support information sharing and communication, it is important for consumers to understand how their information is accessible, when and to whom. They must also be able to control that access easily. Technological trends work in favour of access to information that is electronically stored (Agre & Rotenberg, 1998:68). As with any physical entity, information can be altered, destroyed or removed from the control of its owner. But, unlike physical entities, information has the property of being able to be copied or overheard without leaving a trace of such an activity (Ettinger, 1993:3). Ensuring data integrity gives consumers access to, and the right to request modifications of data records that identify them individually (Smith, 2001:20). **Consumers' right to access of information (also addressed in Chapter 2) is relevant to this study and was measured in the survey.**

However, it is difficult, if not impossible for consumers to know, when they find mistakes, whether these mistakes were circulated prior to correction and, if so, what other databases contain the error. This explains why consumers may be concerned with the growth of computerised databanks and an unmonitored exchange of data. Already in

the 1960s, alarms were sounded about the future of privacy in an age of computer databanks, and over the dehumanisation created when computerised transactions replace face-to-face relations (Hussain & Hussain, 1992:157).

According to Fried (in McQuoid-Mason, 1978: 4), Goffman (in McQuoid-Mason, 1978: 5) and Konvitz (in McQuoid-Mason, 1978: 11) many privacy advocates see the right to privacy as the right to have control over one's information preserve. The control that individuals have to maintain over their personal information has become an international issue with potentially enormous implications in the early 1980s (Prescott, 1999:28). Control has also been defined as empowering people to stipulate what information they protect, and who can get hold of it (Agre & Rotenberg, 1998:70). Neethling *et al.* (1996:303) believe that in order to enable individuals to exercise control over their data records, the following five requirements must be met. The individual has to be:

- aware of the existence of a data record containing the individual's data;
- aware of the purpose for which data is processed;
- legally entitled to have access to his or her data records;
- legally entitled to acquire information as to which persons have or have had access to his or her data records; and
- legally empowered to procure a correction or deletion of certain data.

For many consumers, control over information probably involves an ability to be able to acquire interactive information about products and services they are considering to purchase, to receive targeted solicitations likely to be of interest, to request information they want, and not to be bothered as much by information they find immaterial (Petty, 1998:26). The term 'privacy-enhancing technologies' (PETs) refer to technical and organisational concepts that are aimed at protecting personal identity. PETs seek to eliminate the use of personal data or to give direct control over revelation of personal information to the person concerned (Agre & Rotenberg, 1998:126). Several new technologies will soon permit consumers to challenge marketers regarding control of personal information. Some of these technologies were designed for the online world: anonymisation software allows people to shield their identities as they surf the web;

cookie suppressors stop organisations from planting information in the computers of consumers who access their sites, thus preventing them from identifying and tracking the behaviour of those consumers; e-mail filters permit consumers to protect their computers from spam; anonymous payment mechanisms assist consumers to buy products and services online without revealing their identity; reverse cookies give consumers a way of keeping track and storing records of their own online behaviour. Alone or in combination, these technologies will finally make it possible for consumers to seize control of information about themselves and to choose whether to keep it private or to share it with vendors and other third parties (Hagel & Singer, 1999:11).

3.4.4 Data use

The fourth principle of the OECD Guidelines concerns limitation of use, and is interrelated to the third principle, which deals with purpose specification. It states that the use of personal data ought be limited to specified purposes, and that data required for one purpose ought not be used for others (Rotenberg, 2001:268). **This is relevant to the empirical study and specific items in the measurement instrument addressed the issue of limitation of use.**

The implication of the limitation of use principle for direct marketers is a clamp-down on information sources on which they rely. This means that publicly available information cannot be changed from one of public notification to one of commercial use (Prescott, 1999:28).

Another principle relating to data use is the sixth principle of the OECD Guidelines, which refers to openness. This requires that there should be a general position of transparency in respect of the practices of handling data (Rotenberg, 2001:268). Some believe that consumer anxiety over the collection of personal information has more to do with **how** the information is used rather than **what** data is being collected (Odell, 2002a).

The growth in direct marketing has led to a huge increase in the demand for information that can be used to identify potential consumers of services and products (Smith, 1999:8). One of the most striking areas of difference between the South African and European perspectives is the distinction regarding internal secondary uses of personal data for marketing. The European Directive states that consumers have a legal right to restrict internal uses of personal data for purposes of direct marketing (Smith, 2001:16), whereas the South African perspective places no restriction on internal secondary uses of personal data. For many years direct marketers have emphasised the principle that data collected for direct marketing purposes should be used for no other purpose, and they have succeeded to a great extent. The public is now more concerned that information collected for other purposes may be used for direct marketing or any number of other purposes. While direct marketers have been educated not to use the information they have on file for non-marketing purposes, others now need to be educated not to use the information collected for direct marketing purposes (Nash, 1992:131).

The rise of e-commerce and the Internet, combined with sophisticated data mining software, has resulted in a whole new industry being created where even the tiniest nuggets of personal data have tremendous value (Massey, 2000:19). Data warehousing and data mining are important activities in several marketers' business strategy to deliver better value to customers. Customers can experience increased personalised levels of service from all types of retailers and service providers who are using the data warehousing and data mining capabilities that technology provides (Anon, 2000:16). Unfortunately, data mining techniques can build personal profiles of consumers, leading to an invasion of privacy. IBM is currently researching a technique called 'Privacy-Preserving Data Mining' that explores the notion that one's personal data can be protected by being scrambled or randomised prior to being communicated (Morphy, 2002). By applying this technique, a marketer could generate accurate data models without ever seeing personal information.

Marketers use aggregate information regarding consumers' preferences and buying habits to form groups of consumers with similar interests and tastes. Information used for data mining or direct marketing is used not only for the benefit of organisations that use the information, but also ultimately for the benefit of the consumer. One of the benefits of the information age is the ability to deliver relevant information to individuals depending on their personal preferences (Wientzen & Weinstein, 1997:89). By comparing data on thousands of different information systems, it is possible to create a detailed picture of any one particular person. Cross-referencing these data can, for instance, identify a person's age, income, political party, marital status, number of children, employment history and reading patterns. This process is referred to as databanking, which is computer matching of information in one database with that of another, sometimes resulting in a more detailed database. Many people assume that the details of their private lives will remain confidential, but as more and more of these details are being computerised and made available as sales tools, this assumption loses its validity. The ease of access to a person's file brings up a major disadvantage of large databases and databanking abilities, namely the potential infringement of the right to privacy (Forcht & Thomas, 1994:24). **Consumers' beliefs and attitudes regarding the misuse of their information by organisations are important to this study and formed part of the beliefs and attitudes measured in the empirical survey.**

Cookies are devices that can be used for the purpose of data collection and have been discussed above, in Section 3.4.1.1. Despite negative perceptions of cookies, this technology was built with good intentions. Cookies actually make surfing on the Internet easier, eliminating the need to enter an identification code and password each time a members-only website is visited (Blotzer, 2000:29). Another benefit arises when consumers continue to visit a website, because they can receive personalised information (Allen, Kania & Yeackel, 1998:343). Thus, not all cookies are necessarily bad and raise privacy issues, but when a cookie is used to build an online profile, then it is processing personal data, and as such it can intrude on people's privacy (Wearden, 2002).

Unlike television, radio and the print media, the Internet can record what individuals (not groups) are reading, listening to and shopping for and then build detailed profiles of that behaviour (Green, 1999:48). Toys 'R' Us gathered consumer addresses and credit card numbers from cookies which were placed on online shoppers' hard-drives. After a New Jersey state inquiry into how the toy company protected personal information about its customers, Toys 'R' Us Inc. agreed to pay $50 000 and change its Internet privacy policies. As part of the settlement, Toys 'R' Us agreed to maintain a clear and conspicuous link to its privacy policy on the initial web page consumers are directed to when they enter the web addresses 'www.toysrus.com' and 'www.babiesrus.com' (DeMarrais, 2002).

Relying on techniques such as cookies and web-bugs to track users on the Internet, over the years, DoubleClick, an Internet advertising company, built up profiles on millions of individuals' surfing habits, preferences and past purchases. As a result, it earned considerable notoriety as one of the worst invaders of personal privacy on the Internet. In February 2000, following complaints from the Electronic Privacy Information Center (EPIC) and others, the Federal Trade Commission launched a formal investigation of the company when it was revealed that it planned to link personally identifiable information to these formerly anonymous Internet profiles. The investigation was officially closed in January 2001, consequent to DoubleClick's commitment to abide by self-regulatory guidelines for online profiling. The dismissal of charges (although the case cost DoubleClick $1.8 million in legal fees) required DoubleClick to take action to protect consumer privacy, including an education effort, purging consumer information and adherence to an enhanced privacy policy. DoubleClick agreed to revise its privacy policy to include more easy-to-read explanations of its business. The settlement also required the company to obtain permission (opt-in) from Internet surfers before it can tie personally identifiable information with web surfing history (Silver, 2000:17; Tomasula, 2002b). In addition, DoubleClick must conduct a public information campaign consisting of 300 million banner advertisements that educate consumers on Internet privacy (Mariano, 2002). Some believe it took DoubleClick two years to recover from a public

relations crisis about information that the company had said would remain private, stressing the importance of transparency with respect to the practices of handling consumers' information (Bureau of National Affairs, 2002f).

3.4.5 Data security

The fifth principle of the OECD Guidelines is security safeguards. This means that personal data must be collected and stored in a way reasonably calculated to prevent its loss, theft or modification (Rotenberg, 2001:268). **The safety of consumers' information is of specific relevance to this study. Consumers' concerns regarding the security of their information were addressed in the empirical survey.**

The computer industry is undergoing constant change and growth, and it is only reasonable to assume that security issues are also in constant flux. The period from 1990 to 2001 has introduced new sophisticated, computer-aided crimes. As the need for information grows, so does the criminal's methodology used to manipulate the data and information held by computers. Data security covers a broad landscape of corporate concerns such as integrity, volume and flow of information (Forcht & Pierson, 1994:31). Computer security is the shield that organisations and governments use to protect sensitive and classified information from unauthorised users (Sanderson & Forcht, 1996:32). Data security is the protection of data from unauthorised disclosure, modification and/or destruction – whether accidental or intentional.

It is beneficial to develop an understanding of the fundamentals of data security before planning, designing, or reviewing any information system. 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 security and confidentiality against any anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience or unfairness to any individual about whom such information is maintained (Longley & Shain, 1988:268). 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 (Sanderson & Forcht, 1996:33). Although data security is an important issue for the protection of privacy and personal data, awareness of the fact that it is even more important to keep personal data to a strict minimum is growing, based on the fact that non-existing data cannot be misused (European Union, 1997:1).

With the emergence of computers as an integral part of doing business, and within the computer industry itself, security threats to secured information come from different sources. The best way to keep data on a system almost completely secure would be to disconnect the system from networks. This removal of computers from networks, in today's business environment, is neither feasible nor efficient. Possibly the most frequent method used in efforts to secure data transmission over networks is encryption and cryptography. Encrypting a file scrambles the data into unreadable, garbled characters. All cryptography is based on the concept that only the users of the encrypted information should have the keys needed to decrypt it into something understandable (Sanderson & Forcht, 1996:34).

In May 2001, Visa issued its own security rules to merchants covering the storage, encryption and access of credit card data. As part of its security plan, the top 100 e-commerce merchants, who account for about 70 per cent of Internet commerce using the Visa system, are required to have their online security systems validated by a third party (Thibodeau, 2002).

Information systems security refers to the protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit, and against denial of service to authorised users, including measures necessary to detect, document and counter such threats. The main goals of information security are confidentiality or secrecy, integrity, availability, accountability and assurance. The goal of confidentiality refers to the need to ensure that the information is not accessed by an unauthorised person. The goal of information integrity is to protect information from unauthorised modification. Information availability ensures that the information is

available when needed and is not made inaccessible by malicious data-denial activities. Information accountability ensures that every action of an entity can be uniquely traced back to the entity. Security assurance is the degree of confidence in the security of the system with respect to predefined security goals (Joshi *et al.*, 2001:40).

Two classes of services are crucial for a secure Internet infrastructure. These include access control services and communication security services. Access control services protect Internet resources from unauthorised use, whereas communication security services ensure confidentiality and integrity of data transmitted over the network, in addition to non-repudiation of services to the communicating entities (Joshi *et al.*, 2001:38).

A study in the USA revealed that about 90 per cent of respondents detected computer security attacks in 2001. The annual survey polled 503 corporations, government agencies, financial and medical institutions and universities. Most organisations did not report the attacks for fear of bad publicity about computer security. The results of the survey indicate a continued upward trend in the total number and cost of computer security incidents. The cost of the computer security incidents in 2001 is estimated at $456 million (Costello, 2002). Dan Clements, a fraud investigator in the United States, found that it takes only 15 minutes for stolen credit card numbers to be posted on the Internet. He posted faked credit card data on a web page to track how quickly the information could find a path around the security system. In 15 minutes, 74 visitors from 31 different countries came to view the data and by the end of the weekend, 1 600 potential thieves from 75 countries had visited the page with Indonesia, the United States and Romania leading the pack (Sullivan, 2002:6).

On 23 November 2001, 30 nations, including most European countries, Canada, Japan, South Africa and the United States, signed the Council of Europe's Convention on Cybercrime at an official ceremony in Budapest, Hungary. The Convention, which has been under negotiation since 1997, is the first international treaty to address crimes

committed in 'cyberspace', including breach of copyright, computer-related fraud, child pornography and hacking (Electronic Privacy Information Center, 2001:2).

The United States Chamber of Commerce and the National Cyber Security Alliance joined forces in early 2002 to launch a campaign to inform consumers about how to arm themselves against the potential hazards of the Internet. The focus of the Stay Safe Online Campaign is to educate those who venture to use the Internet on how to protect themselves from computer viruses and potential hackers trying to obtain their personal information (Bureau of National Affairs, 2002d). Another group, the Better Business Bureau (BBB) launched a new Internet site, the Safe Shopping Site, to help consumers locate online retailers that have met BBB standards for privacy in e-commerce. The site also provides information for consumers to learn how to protect their personally identifiable information online (Bureau of National Affairs, 2002g:148). IBM has formed the Privacy Institute and the Privacy Management Council, two initiatives designed to promote secure data management and to protect consumer information. The Privacy Institute does research and develops technologies to help ensure privacy in the areas of e-commerce, mobile computing, knowledge management, and intrusion detection. The Privacy Management Council plans to leverage knowledge of experts in key industries such as finance, health care, government and travel (Garretson, 2001).

3.4.6 Data disclosure and dissemination

Consumers are becoming more concerned about privacy and how their information is being sold (Grant, 2002). It is important for individuals to know when and what information about them is being captured and to whom the information is being made available (Agre & Rotenberg, 1998:70). Information technology is increasing the ability of organisations to share and exchange data with third-party sources. This creates concerns about individual privacy, particularly the ethical issues associated with the collection and dissemination of personal information for direct marketing purposes. Today, most personal information is obtained from secondary data sources, where information is accessible without the individual's knowledge. This type of data originates

from database publishers who transform the data into useful marketing information (McDonald, 1998:107). **Data disclosure and dissemination are of specific importance to this study. The empirical survey measured consumers' concerns regarding data disclosure without their permission, as well as data disclosure to third parties in return for the offering of products and services.**

A particularly critical area covered by the EU's privacy laws is the transfer of data to countries outside the EU. As was mentioned in Chapter 2, pressures from the international community and the fact that data privacy is becoming a global concern with transnational implications dictate that South African organisations cannot ignore EU privacy laws.

There are several ways to accomplish international data transfers legally, but none of them are easy. For example, if a French organisation wants to transfer data of its customers in France to South Africa, they will have to request the French data privacy authorities for approval of the transfer. Alternatively, they have to obtain each customer's consent before transferring the information (Eisner, 2002). The European Union Directive states that personal information may extend outside the European Union only if the destination country ensures an 'adequate level of protection' for the data, or unless one of a number of exceptions applies. A few exceptions to the European Union prohibition are when an individual gives 'unambiguous consent', when it is necessary to fulfil a contract or to comply with law, or if adequate protection can be provided contractually (Prescott, 1999:28). The European Commission has approved standardised contract clauses on privacy protection in cases of cross-border data transmissions to non-European Union countries (Mazumdar, 2002). The clauses are voluntarily, but provide European countries with a sense of security in protecting their privacy rights in other countries. These clauses can be inserted into contracts with non-European Union countries whose own legislation does not offer enough protection, as is the case with South Africa. These clauses do not apply to countries whose own data protection laws are considered to comply with the Commission's standard, such as

Switzerland, Hungary, Canada and United States organisations adhering to the Safe Harbor principles (McMahon, 2002).

Under the federal standard in the USA, an organisation can share customer information within its family of organisations, or with another organisation under a joint-marketing agreement, without obtaining the permission of the consumer. The only instance where an organisation is required to give customers an opportunity to deny permission to release their information (or opt out), is when the data is transferred to a third party marketer (Direct Marketing Association, 2002c). Air Canada is an example of a company who violated the principles of federal privacy legislation in its use of personal information collected through its Aeroplan frequent flyer programme. The airline has improperly shared with third parties the information it has collected from Aeroplan members. The complaint against Air Canada focused on its June 2001 distribution of a brochure entitled 'all about your privacy', to 60 000 of the Aeroplan programme's 6 million members. The brochure outlined five situations in which the airline and its partners share personal information on Aeroplan members internally and with outside parties. Members were instructed to check off boxes if they did not want Air Canada to collect, use, or disclose personal information. But even before distributing the brochure, Air Canada used and disclosed personal information about Aeroplan members in the form of mailing lists and basic membership data (Bureau of National Affairs, 2002i:317).

The Mobile Marketing Association in America (MMA) have set guidelines that include stipulations that its members must have consent before sharing subscribers' information with third parties. Marketers must also fully disclose whether they are using or selling anonymous or aggregate location information for marketing purposes, and should provide ways for subscribers to opt out of all programmes and information sharing (Saunders, 2002). In 2001 in the United Kingdom, about 8 000 investigations were conducted into alleged breaches of their 1998 Data Protection Act, mostly involving organisations wrongly disclosing confidential data to third parties (Bureau of National Affairs, 2002e:61).

In South Africa, citizens' personal details are currently being sold, exchanged and shared in a R3-billion industry. All kinds of organisations, from big businesses to charities and religious groups are earning revenue from selling customers' names, addresses, ages, gender, language preference and an indication of their incomes. South African organisations can tap into a list of 300 000 home-owners nationwide, and they can select names according to the size of the property, the suburb, the recency of purchase, the value of the property and the value of the bond. Some of the purchasers of the lists make assumptions about income based on the suburb in which a person lives. There are, for example, lists containing the personal details of fifty thousand Jewish people and 120 000 Muslims residing in South Africa that can be sold to marketers who have identified Jews or Muslims as their market (Cameron, 1997:1).

Thus far, this chapter has addressed consumers' desire to be free from media intrusion, as well as their desire to protect their confidentiality during data collection, storage, control, use, security and disclosure and dissemination. The final part of Chapter 3 addresses consumer information privacy from an organisational perspective by discussing organisations' responsibility to develop privacy practices and policies.

3.5 PRIVACY PRACTICES AND POLICIES

The eighth principle of the OECD Guidelines is the principle of accountability. One of the first steps an organisation needs to take to ensure customer privacy is to develop a privacy policy and make it visible. **Consumers' expectations regarding organisations' privacy policies are of specific relevance to the study and were measured in the empirical survey.**

The organisation should appoint a data controller to be responsible for complying with the principles of the privacy guidelines (Rotenberg, 2001:268). Two types of expenditures are involved when implementing corporate privacy policies: one-time development costs and recurring operational disbursements. Development costs include analysis and design of procedures for privacy protection, and the acquisition of

equipment and software dedicated for that purpose. The main component of operations is salaries, primarily for administrative assistants handling notification, access, correction and erasures. Other operational costs include computer time, data storage, data transmission, rental of maintenance of security equipment and supplies (Hussain & Hussain, 1992:159).

The pressure for comprehensive, effective privacy policies are rising. Creating a written policy can be a first step in the privacy process. IBM has created a Tivoli Privacy Wizard to help organisations formulate privacy policies by defining the privacy policy, and translate it into an electronic language that different software applications can understand and apply. Policies created by the Wizard can be exported to P3P format, the current industry standard (Anon, 2002a). Privacy wizards are also available from organisations such as TRUSTe, Microsoft, and the DMA. Most of these privacy generators request organisations to answer a series of questions online and in return they receive a customised privacy policy which they can then submit to a lawyer to adapt to their own particular needs (Wazeka, 2000:64).

Many privacy advocates are trying to achieve a balance between providing the public with privacy-protecting technologies and passing legislation to support the use of those technologies. A handful of organisations are not waiting for privacy legislation, but are working on privacy-enhancing technologies that can be used immediately (Pruitt, 2002). P3P is one example of how privacy proponents are moving ahead with stand-alone privacy-enhancing technologies. The World Wide Web Consortium (W3C) has approved the platform for privacy preferences (known as P3P), as the new standard for online privacy. P3P is a technology that allows web users to set their privacy standards and then alerts them when they are visiting a site that does not meet their requirements (Pruitt, 2002).

P3P covers nine aspects of online privacy. Five topics detail the data tracked by the site: who is collecting the data; what information is being collected; for what purposes; which information is being shared with others; and who the data recipients are. The

remaining four topics explain the site's internal privacy policies: whether users can change the way their data are used; how disputes are resolved; what the policy for retaining data is; and where the detailed policies can be found in human readable form (http://www.w3.org/P3P). This technology is viewed as a landmark development because it paves the way for the standardisation of privacy policies (Neethling, 2000:35). Whether or not a site uses P3P, the system will not stop sites from gathering data or sharing information with marketers. Some privacy supporters have campaigned actively against P3P, stating that it will not do anything to protect users' privacy (Kane, 2002).

The Privacy Leadership Initiative (PLI) and the United States Chamber of Commerce have announced a partnership to provide a resource for small and medium-sized organisations with step-by-step instructions on becoming privacy smart. The free online resource, Privacy Made Simple, is a one-stop shop designed primarily for small or medium-sized organisations that want to develop or upgrade their privacy policies and notices. Bill Kovacs (2002), vice president of the Chamber in charge of technology policy says that 'meeting the privacy expectations of consumers is a critical component of doing business in the e-commerce environment and it is also good for the bottom line, because privacy policies are shown to increase consumer confidence and boost sales'.

Privacy and social responsibility issues, for organisations, customers and legislators may be alleviated by increased attempts by the industry to police itself. Self-regulation goes beyond the minimum requirements of legislation and has to be adhered to in spirit as well as to the letter (O'Malley *et al.*, 1999:441). In an effort to build consumer trust, direct marketers abide by certain information practices to honour consumers' privacy. The DMA of South Africa provides guidelines that must form the basis of privacy policies of member organisations. Member organisations also have to meet nine basic privacy requirements, namely:

- The purpose of collection has to be explicit and legitimate.
- The collection of personal information has to be fair and lawful.

- Only relevant information can be collected, and it should be adequate for the purpose for which it was collected.
- The information may not be used for any purpose without the data subject's knowledge, and every data subject has to be offered the right to opt out of disclosure of the information to third parties.
- Organisations have to make all attempts to ensure accuracy of data, and the data subject has the right to access, object, and correct data.
- The organisation has to treat information with sensitivity, as well as implement security measures to prevent unauthorised access to the information.
- The organisation has to subscribe to the Media Preference Service (Direct Marketing Association, 2001a).

The DMA's privacy guidelines are an important step in creating meaningful self-regulation to protect consumer privacy in the information age. Private sector leadership of this magnitude is critical in building consumer confidence in the marketplace by ensuring that personal information will be treated fairly and responsibly. Consumer acceptance is crucial, particularly with the promise of interactive marketing in the future (Anon, 1999:6). However, the success of self-regulation depends upon consumers' using the facilities provided to them, and registering complaints about offending organisations. To this end, consumers and direct marketers will need to be better educated as to what is acceptable and what is not acceptable in the future. At an industry level, it is important that consumers are made aware of their rights. Given that consumer knowledge of direct marketing practices is a factor of how they perceive the industry, direct marketers need to allow the consumer greater access to information. Consumers should be made aware of what constitutes acceptable and unacceptable behaviour in terms of data collection and utilisation by organisations. They also need to know how to protect their information, how to query information held in an organisation's database, and how to remove their information if they so desire (O'Malley *et al.*, 1999:441). **This is of importance to the study which aimed to measure, *inter alia*, consumers' knowledge of options to remove their information.**

Unfortunately, self-regulation has limitations. First, most consumer groups lodge complaints to government agencies instead of to the industry. Second, the interests of organisations are diverse and a single industry solution is unlikely to be possible. Third, not all organisations are associated with the DMA, especially those most likely to act in unethical ways. Finally, industry boards have no power to enforce compliance. Perhaps co-operation between organisations, consumer advocates and government would be a more effective way of treating privacy issues (Katzenstein & Sachs, 1992:73).

For a direct marketing industry whose heart is a database and whose lifeblood is marketing data, the privacy and security issues are potentially life-threatening. To marketers, the personal information which is provided by their customers is a treasure that should be handled with caution, as this is their greatest asset (Wientzen, 2000:77).

3.6 SUMMARY

More and more consumers are concerned about their information privacy. Over the last few years a large number of countries have issued privacy laws in which the cross-border transfers of data is regulated. In response to the technological advances of the last decade, which allowed organisations to collect, process and transfer personal data on a far greater level than before, many countries and regions have started to develop detailed regulatory provisions to ensure the protection and privacy of data relating mainly to individuals. The European Union ensures the highest standard of protection, providing what is probably the most extensive set of rights mainly for individuals, and obligations for organisations using personal data. As more countries around the world implement data protection legislation, consumers' awareness and sensitivity continue to grow in respect of information privacy issues.

While European laws provide extensive data protection, in South Africa such protection is only provided to a limited extent. The most obvious route for South African managers in all industries is voluntarily (without being required to do so by law) to embrace certain principles that are implemented in European organisations. This is important because

organisations that do not voluntarily embrace more expansive sets of consumer information privacy protection are likely to be forced to do so through future legislation.

This chapter has focused on consumers' desire to be free from intrusion by marketers, and their desire to protect their confidentiality. This was addressed against the backdrop of data collection, storage, control, use, security, disclosure and dissemination. The general premise for South African managers should be to act as if consumers have joint ownership rights to data about themselves. This should motivate organisations to implement proper privacy practices and to develop visible privacy policies. In order to do this effectively, marketers have to understand consumer behaviour in a privacy sensitive environment, which is the focus of the next chapter.

CHAPTER 4
RELATIONAL EXCHANGE PROCESSES AND PRIVACY

4.1 INTRODUCTION

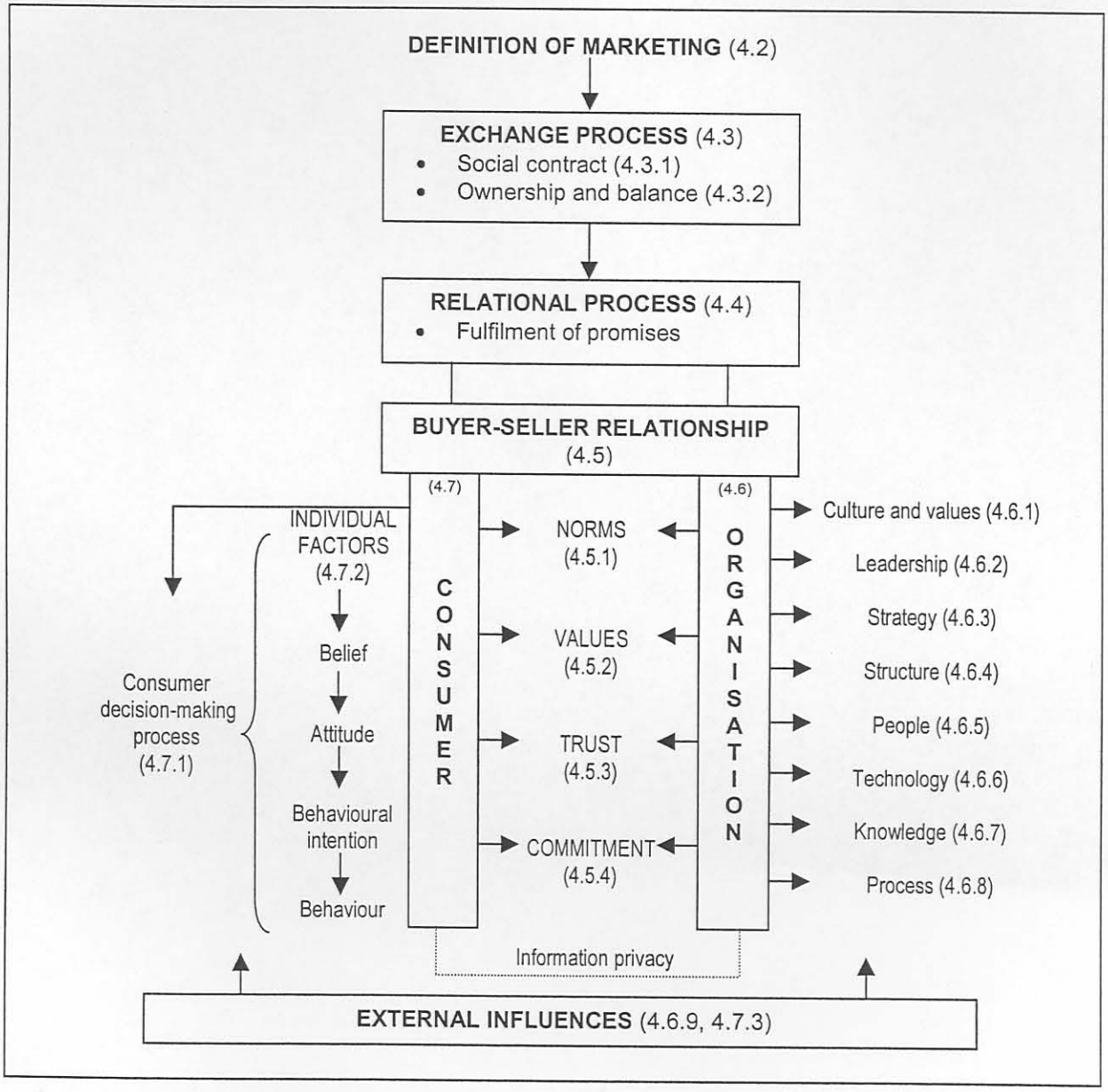
The chapter starts with a focus on the development of marketing definitions, indicating one central theme to all the definitions, namely the concept of exchange. In this exchange process, there is an implied social contract between consumers and marketers, where consumers provide personal information, amongst other things, in exchange for products, services or information. Extensive use of consumer information has become part of everyday exchange processes; hence, the issue of who owns consumer information is raised, since control of consumer information is a valuable commodity in the market and it is therefore a source of power.

As marketing developed, the exchange process developed a more relational character. An integral element of the relationship marketing approach is the promise concept. This concept implies that the fulfilment of promises is vital as a means to achieve customer satisfaction, to retain the customer base, and to attain long-term profitability. If promises are not kept, the evolving relationship cannot be maintained and enhanced. Given the relational exchange processes between organisations and consumers, the chapter also addresses norms, values, trust and commitment as key virtues in building a relationship between these two parties.

Finally, the chapter focuses on the dual nature of the information privacy issue in relational exchange processes. On the one hand, it explains the role of organisations in relationship-building, as well as external influences on its marketing activities. On the other hand, it discusses the consumer decision-making process and how it is influenced by individual factors and external factors. Figure 4.1 provides an outline that will serve as the basis of discussion for this chapter. It is important to note that the aim is not to question current consumer behaviour models, but rather to develop a framework to

serve as a platform for explaining interrelationships in exchange processes. The figure also indicates in which section(s) of the chapter the different matters are discussed.

Figure 4.1 Relational exchange processes*



* The relationships and/or influences indicated are used merely for illustrative purposes and do not imply tested theoretical and empirical relationships.

4.2 THE DEVELOPMENT OF MARKETING AS A BODY OF KNOWLEDGE

The term 'marketing' comes from the word 'market', which refers to a group of potential customers with similar needs who are willing to exchange something of value with sellers offering various goods and/or services (Perreault & McCarthy, 2002:14). In 1948, the American Marketing Association (AMA) defined marketing as the performance of business activities directed toward and incident to the flow of goods and services from producer to consumer or user (Webster, 1992:2). The articulation of the marketing concept in the mid- to late 1950s posited that marketing was one of the principal functions of the organisation because the main purpose of any organisation was to create a satisfied customer (Webster, 1992:2). The marketing mix, known as product, price, place and promotion, was introduced to marketing education by McCarthy in 1960 (Yudelson, 1999:60).

Throughout the 1970s, the marketing literature emphasised transactions as a central construct and as the basic unit of analysis for the marketing discipline (Webster, 1992:6). Some authors even advocated a definition of a transaction that included any exchange of value between two parties, thus broadening the concept of marketing to include virtually all human interaction (Kotler & Levy, 1969:10). In the late 1970s and early 1980s, a new exchange paradigm was suggested where the focus was on understanding the relationship dimensions of the exchange (Pels, 1999:19). During the 1980s, marketing literature began to recognise the importance of managing buyer-seller relationships as strategic assets (Webster, 1992:7). In 1985, the AMA produced an updated definition of marketing which identified marketing as the process of planning and executing the conception, pricing, promotion and distribution of ideas, goods and services to create exchange and satisfy individual and organisational objectives (Grönroos, 1990:5).

The 1990s have seen a strong move away from the transaction perspective to a recognition of the role of relationships in the marketing activities of the organisation (Webster, 1992:14). Yudelson (1999:63) referred to marketing as those activities that

seek to influence voluntary exchange transactions in a wide range of settings and situations where both parties may look beyond the specific exchange transaction to the development of a mutually beneficial relationship during an extended period. The marketing process may be said to be enhanced by the fact that exchange parties have different goals. While these goals may or may not in fact be independent, the means for satisfying them is very often interdependent. This highlights the importance of the social system within which shared values and relationships are developed or it is because these needs may be satisfied differently that both parties in the marketing exchange are able to experience an increase in potency (Peters, 1997:220).

Kotler (in Grönroos, 1994:355) concluded that organisations have to move from a short-term transaction-oriented goal to a long-term relationship-building goal. The objective was no longer to make a sale, but to develop a customer relationship in which the sale is only the beginning of the relational process. As customer relationships replaced transactions as the focus of marketing activity, a new definition emerged and the customer became a long-term strategic business asset (Webster, 1994:26). Grönroos (1990:8) established a new definition of marketing which described marketing as a process to establish, maintain and enhance long-term customer relationships at a profit, so that the objectives of the parties involved are met. He believed the main objective of marketing was to create enduring relationships with customers through mutual exchange and fulfilment of promises. Here marketing is viewed as an interactive process in a social context where relationship-building and management are the cornerstones (Grönroos, 1994:353).

The above definitions all suggest that the concept of exchange has been central to marketing from the beginning. The literature indicates that marketing, as a body of knowledge, has always been concerned with understanding relationships between buyers and sellers (Kavali, Tzokas & Saren, 1999:576). Marketing thus revolves around customer relationships whereby the objectives of the parties involved are achieved through various kinds of exchange. Moreover, exchanges take place in order to establish and maintain these relationships (Grönroos, 1990:7). The definitions suggest

that the core of marketplace behaviour is the exchange of values within different relationships. The above definitions suggest that marketing has developed from 'transactions that included any exchange of value' to 'relationship dimensions of the exchange'. The next section focuses on the two key issues identified in most marketing definitions, namely the exchange process and the relational nature of these exchanges.

4.3 THE EXCHANGE PROCESS

Every exchange requires having two or more parties where the one party offers something, and another party obtains that which is given by offering something in return. Exchange is a value-creating process because it normally leaves both parties better off (Kotler, 2000:12). In the commercial world, this 'sacrifice' by the consumer is usually money, or something of monetary value, whereas the marketer offers products or services in return for value. In addition, the consumer may have to give up time, effort or comfort, may have to take on some risk or has to pay other forms of costs to obtain the item or service from the marketer. The growing emphasis on the exchange transaction between two parties has shifted the focus of marketing management from activities to influence consumers to activities designed to facilitate a mutually advantageous exchange (Yudelson, 1999:61, 63).

Exchange may be viewed either from the perspective of economic exchange or the perspective of social exchange. In economic exchange models, social interaction is viewed as an exchange of mutually rewarding activities in which the receipt of a needed valuable is contingent on the supply of a favour in return. According to social exchange theory, social relationships are based on each partner's motivational investment and anticipated social gain (Takala & Uusitalo, 1996:47). Underlying any definition of information privacy is an implicit understanding that the individual's interests are balanced with those of society at large. Individuals surrender a measure of privacy in exchange for some economic or social benefit (Culnan, 1993:10).

It is important to realise that there can be no transaction or exchange without the flow of information. The information does not need to be complete, or even accurate, but at the very least, the two parties must acknowledge each other's existence and have some idea of what will be exchanged, as well as what the respective benefits and costs may be (Yudelson, 1999:63). In particular, consumers must perceive that the economic or social benefits derived from the relationship with the marketer outweigh the personal information privacy costs (Davis, 1997:33).

Concern about privacy has focused on two different theoretical concepts of privacy. The first is a social relationship view, in which privacy is understood to act as a balance to the development of social relationships. This concept of privacy on the Internet would be manifested in anonymous interactions and assumed identities, like in chat rooms, where social relationships between members of various Internet communities evolve. A second concept of privacy is the better-known property view, in which individuals see privacy as the extent to which they control their own information in all types of exchanges. The property view manifests itself in willing exchanges of personal information in exchange for valued services such as free e-mail or special discounts from organisations (George, 2002:166).

Besides money and other costs, consumers invest their personal information in an exchange process. Close, long-term relationships can be achieved through the exchange of information, the exchange of goods and services and a social contract. In their turn these exchanges lead to certain benefits or gains (Grönroos, 1990:7). It has been suggested that transactions are more likely to be morally defensible if both parties enter into them freely and fully informed. This necessitates an investigation into social contracts between buyers and sellers, as set out below. Assuming that marketing and marketers want to be part of morally defensible transactions, the goal of marketing should be to increase the likelihood and frequency of free and informed transactions in the market (Kavali *et al.*, 1999:578).

4.3.1 Social contracts

The belief that information control is a key mediator of consumer privacy concerns has led many to suggest that marketers should view consumers' exchange of personal information as an implied social contract (Culnan, 1995:11; Milne, 1997:299). A social contract is defined as a fundamental compact that consists of the rules imposing basic duties, assigning rights and distributing the benefits of political, social and economic co-operation, unanimously agreed to by reasonable people in a state of perfect equality and absolute impartiality (Grant, 2000:20). In a marketing context, a social contract is established when a customer provides a marketer with personal information at the point of purchase with the intention that the marketer will use this information to serve the customer better (Milne, 1997:299). When marketing is viewed as an implied social contract of this nature, consumers are seen to provide personal information in exchange for products or services, receiving solicitations and other information, based on an expectation that their personal information will be managed responsibly.

Integrative social contract theory provides a means for understanding the current tensions between marketers and consumers regarding privacy. Integrative social contract theory posits that members of a given community or industry behave fairly if their practices are governed by shared norms (Donaldson & Dunfee, 1994:254). According to Phelps *et al.* (2000:29) the implied social contract is considered to have been breached if consumers are unaware that information is being collected, if the marketer rents the consumer's personal information to a third party without permission, or if consumers are not given an opportunity to remove their names from lists or otherwise restrict the dissemination of personal data about them.

It is important that the dual nature of the information privacy issue should be highlighted. On the one hand, it is concerned with the right of individuals to privacy. On the other hand, information protection negatively affects organisations in their right to full disclosure and a free flow of information (Walczuch & Steeghs, 2001:142). The tension between information access and information control has been presented as a problem

of striking a fair balance between the privacy interests of individuals and the financial interests of organisations. The effective utilisation of consumer data is essential to the development of a meaningful dialogue between organisations and consumers, and in many ways, the interests of consumers and organisations about the use of consumer information are similar (Campbell, 1997:47). One issue pertaining to the dual nature of information privacy is the ownership of information. This is addressed in the next section.

4.3.2 Ownership and balance in the exchange process

As the extensive use of consumer information has become part of the fabric of the modern market, the issue of who owns consumer information has been raised (Davis, 1997:35). The control of consumer information has been a valuable commodity in the market and is therefore a source of power (Prabhaker, 2000:164). Information technology is now having a vast impact in this area, changing the nature of relationships and the balance of power between the parties involved (Fletcher & Peters, 1996:145). In practice, consumers and organisations often disagree about who owns the information and what kinds of trade-off are acceptable in different situations (Campbell, 1997:48). Several perspectives on ownership have been offered, placing ownership rights either in the hands of consumers or in those of organisations.

Organisations have good reason to collect information about consumers. It enables them to target their most valuable prospects more effectively, to tailor their offerings to individual needs, to improve customer satisfaction and retention and to identify opportunities for new products or services (Hagel & Rayport, 1997:53-4). One view suggests that the organisation which has gathered such information through the expenditure of time, effort and money for the purposes of its business should control its use and dissemination (Davis, 1997:35). This view is supported by Taylor, Vassar and Vaught (1995:44), who suggest that marketers who have created databases posit that the information contained in the databases belongs to these marketers and that

therefore the marketers feel justified in using, selling or renting the information to others without the consumers' consent.

Personal information privacy rights could have a significant impact on information-trading practices. Many consumers vent their concern about their privacy by refusing to provide permission to disclose their information to third parties, diminishing the marketing opportunities of the organisation which is dependent upon the availability of lists. Others believe that placing ownership in the hands of consumers could improve consumer targeting and solicitation response rates, if consumer consent for contact was obtained. A consumer who granted permission would be better qualified and more interested in having contact with the organisation (Davis, 1997:39).

Foxman and Kilcoyne (in Davis, 1997:34) argue, on ethical grounds, that marketers should recognise consumer ownership rights to personal information because consumers perceive these rights to exist and resent their violation. If personal information can be defined as property, the original owner could control its use and dissemination, an idea consistent with the notions held by Westin and Miller (in Davis, 1997:35). In the late 1960s, they argued that property rights should be attached to personal information so that individuals could control its dissemination better and could safeguard their personal privacy. Consumers must perceive that the economic and social benefits derived from the relationship with the marketer outweigh the personal privacy costs; otherwise consumers will take ownership of information about themselves and demand value in exchange for it. Many consumers have now realised that the information they have divulged so freely through their commercial transactions, financial arrangements and survey responses has value and that they get very little in exchange for that value (Hagel & Rayport, 1997:53-4).

A consumer-controlled information market could offer advantages, as well as disadvantages from a social and economic perspective. One advantage can be the protection that personal information privacy rights can provide against unwanted mail and telephone solicitations. A social disadvantage to information privacy is the situation

where consumers cut themselves off from valuable marketing information by failing to provide consent to information use and dissemination (Davis, 1997:39).

Research in the Internet environment has revealed that consumers do not trust most Internet providers enough to engage in relationship exchanges involving money and personal information. This lack of trust arises from the fact the consumers feel that they lack control over the access that Web merchants have to their personal information during the online navigation process. Trust is best achieved by allowing the balance of power to shift toward more co-operative interaction between an organisation and its customers (Hoffman, Novak & Peralta, 1999:80). Westin (in Davis, 1997:36) provides a very workable solution to the above problem when he suggests that marketers merely hold the consumer's information and should thus be regarded as trustees of the consumer data.

Online businesses have to negotiate a delicate balance between strong consumer demand for privacy protection and a real consumer desire for personalised treatment. Successful organisations must collect relevant information and use it properly as a competitive tool. As consumers become more comfortable online, they are increasingly open to providing personal information to their favourite websites. However, they are stridently demanding that this information be used to enhance their experience and that the information is not used in ways that abuse a privileged relationship, or even be subject to a perception of abuse (Mabley, 1999:1).

The above discussion highlights the need for exchange processes with a more relational nature. The social system within which shared values and relationships are developed will only satisfy the needs of the different parties involved if the benefits they receive outweigh their costs; resulting in a beneficial trade-off.

The next section discusses critical elements in creating a mutually beneficial relationship against the backdrop of information privacy.

4.4 THE RELATIONAL NATURE OF EXCHANGES

The evolution of relationship marketing and the advocacy to extend relationship marketing into the management of the exchange processes within consumer markets have resulted in a growing interest in responding to every customer on an individual basis. The search for improved techniques for winning and keeping customers (considerably enhanced by the increasing availability, sophistication and cost-effectiveness of computer-based systems) has been paralleled by an increasing concern among consumers of the impact of these new marketing management techniques on their private rights (Long, Hogg, Hartley & Angold, 1999:5).

One of the most controversial aspects of relationship marketing in consumer markets centres on information privacy. A fundamental tenet of relationship marketing is that the role of the consumer has changed from a passive recipient of marketing practices to an interactive co-producer of marketing practices. It is implicit in this philosophy that marketers and consumers are partners in business. However, it may be difficult for organisations interested in relationship marketing to pursue customer partnerships if consumers and organisations do not share a common set of values or understanding about privacy (Campbell, 1997:45).

Morgan and Hunt (1994:22) define relationship marketing as all marketing activities directed toward establishing, developing and maintaining successful relationship exchanges. The concept of a relationship implies at least two essential conditions. First, a relationship is a rewarding connection between the provider and the customer, where both parties expect to obtain benefits from the contact. Second, the parties have some kind of commitment to the relationship over time, and they are therefore willing to make adaptations to their own production processes (Takala & Uusitalo, 1996:48).

Customer relationships lie at the core of marketing and are developed so that individual and organisational objectives are met. Each party in a relationship has certain expectations and objectives. Sellers, for instance, want continuing relationships

because they assume that these relationships are more profitable. An integral element of the relationship marketing approach is the promise concept. In establishing and maintaining customer relations, the seller gives a set of promises relating to goods, services, financial solutions, material administration, transfer of information, social contracts and future commitments. On the other hand, the buyer gives a set of promises concerning his or her commitments to the relationship (Grönroos, 1990:8). Relationship marketing demands the establishment of mutually accepted norms of redress. The buyer expects the seller or supplier to act responsibly in unforeseen and unplanned events (Selnes, 1998:310). The promise concept is important to both sides in order to ensure profitable business operations (Takala & Uusitalo, 1996:48).

Takala and Uusitalo (1996:49) present a number of issues which are critical in respect of long-term customer relationships (some of these have already been addressed and the rest are addressed in the remainder of the chapter). According to these authors, the following are relevant to a relationship marketing philosophy:

- Customers and their needs are the starting point of marketing.
- The objectives of the seller and the customer influence their mutual relations.
- Exchange, which is a focal issue in relationship marketing, includes continuous struggle for power of balance.
- There are various means of establishing relationships.
- Promises must be kept in order to maintain relationships.
- Mutual trust is a main factor in long-term relationships.
- Relationships imply dependence and commitment.
- Communication is essential.

Kavali *et al.* (1999:576) define relationship marketing as the process of planning, developing and nurturing a relationship climate that will promote a dialogue between an organisation and its customers which aims to imbue an understanding of, confidence in and respect for each others' capabilities and concerns when enacting their role in the market and society. This definition highlights the core issues addressed in the remainder of this chapter. First, the key elements in developing a relational climate are

discussed. This is addressed from both the buyer and the seller's perspective, since the concept of relationship marketing may be seen either from the sellers' perspective – as a means to tie customers into closer relationship with them – or from the buyers' point of view – as a way to obtain a group of preferred suppliers (Takala & Uusitalo, 1996:48). Second, there will be a focus on the role of organisations in the building of relationships within a privacy sensitive environment. The chapter concludes with a discussion on consumer behaviour in relational exchanges, with a focus on consumers decision-making processes and how these change when information privacy becomes an important driving force. It is important to note that, for the purposes of this study, relational exchange processes include transactional and relational marketing (Coviello, Brodie & Munro, 1997:506).

4.5 KEY ELEMENTS IN A BUYER-SELLER RELATIONSHIP

Kavali *et al.* (1999:576) have identified the following key elements in relationship marketing: equity, benevolence, norms, reliability, responsibility, commitment, diligence and trust. Selnes (1998:310) believes that relationship marketing is about healthy relationships characterised by trust, equity, responsibility and commitment, which proactively set the conditions that may influence ethical behaviour. Zineldin (2000:10) has identified personal relationships, interactions and social exchange as the most important core elements of relationship marketing, while Ravald and Grönroos (1996:19) consider value to be an important constituent of relationship marketing. Some of the key elements of relational exchanges that have an impact on information privacy are discussed below, namely norms, values, trust and commitment.

4.5.1 Norms

Norms are expectations about behaviour that are at least partially shared by a group of decision-makers. Norms may apply at different levels, but for the purposes of this study, the focus is on norms that govern individual exchange relationships between buyers and sellers. Norms differ in their general orientation content. So, for instance, norms

have been found to differ significantly in the extent to which they prescribe behaviours directed toward collective as opposed to individual goals. Macneil's (in Heide & George, 1992:34) typology of discrete versus relational norms reflects this difference. Basically, discrete exchange norms contain expectations about an individual or competitive interaction between exchange partners. The individual parties are expected to remain autonomous and pursue strategies aimed toward the attainment of their individual goals. By contrast, relational exchange norms are based on the expectation of mutuality of interest, essentially prescribing stewardship behaviour, and are designed to enhance the well-being of the relationship as a whole (Heide & George, 1992:34).

Kavali *et al*. (1999:579) report that inadequate basic norms and the absence of ethics are the biggest obstacles to success in relationship marketing. Strategic uses of information technology based on personal information may raise privacy concerns among consumers if these applications do not reflect a common set of values (Culnan, 1993:341). Long-term relationship-building efforts provide an effective way for marketers to build trust and loyalty among targeted consumers. One of the ways to achieve such affinities among consumers is to interact with targeted segments from ethical perspectives that are consistent with the segments' expectations, values and norms (Rawwas, Strutton & Johnson, 1996:58). There has been a movement toward thinking of marketing less as a function and more as a set of values and processes where all functions participate in the implementation (Moorman & Rust, 1999:180).

4.5.2 Values

Value is considered to be an important constituent of relationship marketing (Ravald & Grönroos, 1996:19). The success of a relationship that is a mutually profitable relationship for supplier and buyer depends on the ability to provide episode value and relationship value continuously (a discussion of the meaning of these two values is set out below).

Episode value is improved by increasing the benefits and/or reducing the sacrifice to the buyer. The benefits and the sacrifice can be viewed as two elements that are mutually dependent. Increasing the benefits should lead to a reduction in the customer's perception of sacrifice by minimisating the costs involved in a discrete episode and in the relationship as a whole. Reducing the sacrifice or effort the customer has to undertake in order to purchase a product at an episode level involves activities such as lowering the actual price or increasing the convenience of the purchase. Consumers can also feel that they are making a psychological sacrifice when they worry about whether a supplier will fulfil its promises. The perceived sacrifice thus includes all the costs which the buyer faces when making a purchase, such as purchase price, acquisition costs, transportation, installation, repairs and maintenance, risk of failure or poor performance. The perceived benefits are a combination of physical attributes, service attributes and the technical support available in relation to the particular use of the product, as well as the purchase price and other indicators of perceived quality.

Research has indicated that buyers tend to be more sensitive to loss than to gain, and this constitutes an opportunity for an organisation to improve the customer-perceived value and thereby establish and maintain a long-term relationship. If the organisation can provide value in terms of reducing the customer's perceived sacrifice, so that the relationship costs are minimised and customer performance is improved, the chances of becoming successful are evident. But to be able to provide this kind of value, organisations have to understand the elements of customer-perceived value and how the organisation's activities influence customer performance (Ravald & Grönroos, 1996:21-26).

Information is increasingly emerging as an asset, with a market value and associated acquisition and handling costs. As an asset, information can have the property of increasing in value through use (Glazer, 1991:6). Records of customer purchase behaviour, held and accessed on a database system, can become the primary marketing resource of many organisations. Therefore, the focus for customers is likely to be the value they receive from the demonstrated use of their information by

organisations. By contrast, it is likely that for the organisation, customer information value may be sought from the anticipated use of such information (Peters, 1997:218). However, where the collection of customer data is not seen by the customer as resulting in greater value, difficulties may arise.

This distinction between anticipated and realised information value on the part of organisations can lead to problems of goal incompatibility with customers, and may well raise issues of privacy and a perception on the part of customers that organisations do not really need or appropriately use the information they collect from customers (Peters, 1997:219). To some, the value dimension of personal information implies that some type of compensation is due for such information. Compensation is a controversial topic and is a salient issue for some consumers. It has been proposed that consumers be compensated via coupons, discounts or rebates. Compensation, however, does not seem to be the driving issue for most consumers today. Instead, consumers are more likely to be interested in acquiring some control of, and enhancing the benefits associated with, the marketing relationship, while minimising potential abuse of their personal information (Davis, 1997:37).

Relationship value has a deeper meaning than the episode value (discussed above). As a relationship evolves, a buyer starts to feel safe with the supplier, and trust develops. Trust through safety, credibility and security reduces the sacrifices for the buyer and is assumed to be of value in itself (Selnes, 1998:305). The next section addresses trust as a key element in a buyer-seller relationship.

4.5.3 Trust

In order to establish long-term relationships with customers, organisations need to win consumers' trust on a continuous basis (Kandampully & Duddy, 1999:52). Trust has been defined as a willingness to rely on an exchange partner in whom one has confidence (Grönroos, 1997:327). Trust thus exists when one party has confidence in an exchange partner's reliability and integrity. This trust extends beyond the provision of

the actual goods or services to all aspects of the organisation-consumer interaction. The manner in which the information is obtained, stored and used is likely to affect consumer's trust in marketers. Thus, consumer privacy concerns related to collection, errors and secondary use of their information are all expected to have a negatively effect a consumers' willingness to respond to direct response advertising media (Campbell, 1997:47).

Trust is an important concept in relationship exchange, since it allows exchange partners to look beyond short-term inequities or risks and to concentrate on long-term gains. The role of trust in relationships and exchange is to stimulate co-operation and to create goodwill, which helps to preserve the relationship. There is general consensus that trust is critical in exchanges involving interdependence, uncertainty and risk (Milne & Boza, 1999:316).

Perceived risk in a relationship enhancement decision may be reduced by trust alone or trust in combination with a number of mechanisms. Anderson and Narus (in Selnes, 1998:308) found a close connection between co-operation and trust. They suggest an iterative process where co-operation leads to trust, which in turn leads to greater willingness to co-operate in future, which then generates trust, and so on. Trust can be an important antecedent of relationship enhancement to the degree that it reduces perceived risk more efficiently than other available mechanisms. Satisfaction is a manifestation of the other party's ability to meet relational norms, and is an important source of trust (Selnes, 1998:309). Interviewees from multi-national corporations in Germany and the Netherlands argued that customers were more likely to trust an organisation if they knew that their private information was well protected (Walczuch & Steeghs, 2001:156).

Honest and timely communication with consumers has a strong effect on both trust and satisfaction (Selnes, 1998:317). Hunt (in Harker, 1999:15) identifies relational trust and commitment as critical elements in relationship development. To gain the loyalty of customers, the organisation must first gain their trust. When customers trust an online

vendor, for instance, they are much more likely to share personal information. That information enables the organisation to form a more intimate relationship with customers, offering products and services tailored to the consumers' individual preferences, which in turn increases trust and strengthens loyalty (Reichheld & Schefter, 2000:106).

Thoughtful organisations realise the value of becoming the 'consumer's advocate'. They can also promote that value to other organisations to build a powerful network of associates, each of which espouses guardianship for the consumer. The promotional value of revealing the latest method to collect information that compromises the consumer's privacy and the latest response to protect that privacy would position the advocate as an organisation of trust. While some organisations strive to find new ways to ferret out information and use it to gain a marketing advantage, others will find new ways to use that information while keeping it private. The value is consumer co-operation, even if it entails a price. The price is likely to be very small compared to the efficiency benefits of knowing exactly what the consumer wants. However, paying for consumers' private information would help the organisation to arrive at the value of that information. It would also encourage more technological developments to protect information (Franzak, Pitta & Fritsche, 2001:640).

As the relationship between two parties develops over time, and as they gain experience and learn to trust each other, they will gradually increase their commitment through transaction-specific investments in products, processes or people dedicated to the particular relationship (Selnes, 1998:307). Commitment is discussed in detail in Section 4.5.4.

4.5.4 Commitment

Relationship commitment is central to relationship marketing, and has long been central in social exchange literature. Social exchange theory explains the causal relationship between trust and commitment and that trust is an important determinant of relationship

commitment (Morgan & Hunt, 1994:24). Relationship commitment refers to a situation where an exchange partner believes that an ongoing relationship with the other partner(s) is so important as to warrant maximum efforts at maintaining it. When that happens, the committed party believes that the relationship is worth working on to ensure that it endures indefinitely. As the practice of relationship marketing develops, consumer-organisation relationships may well develop along more rigidly defined lines, even if this involves limiting entanglements and introducing more contractual elements into the interaction. The benefits of such actions would be a clearer understanding of the motivations and expectations of the parties involved (Peters, 1997:220). The next section focuses on the organisation and its role in developing and maintaining long-term relationships.

4.6 THE ROLE OF ORGANISATIONS IN RELATIONAL EXCHANGES

The goal of relationship marketing is to align all the aspects of an organisation with the needs of its chosen customers and stakeholders. Gordon (1998:22) has identified eight components of relationship marketing which are needed to obtain the above-mentioned goal, vis-à-vis culture and values, leadership, strategy, structure, people, technology, knowledge and process. Each component is discussed briefly below, relating it to relational exchanges and information privacy. Thereafter, the different external influences affecting organisations' marketing activities are discussed, because developing these influences allows organisations to serve as sources to protect consumers.

4.6.1 Culture and values

Organisational culture is the basic set of values and beliefs that are shared throughout the organisation. These values and beliefs help employees understand how the organisation functions and dictate behavioural norms (Webster, 1994:29). At the basis of all organisational functioning there is a core of values and beliefs, the culture shared by members of the organisation (Webster, 1988:37). Management must develop a

broad concept of organisational culture that focuses the organisation outward – on its customers and competitors – and creates on overwhelming predisposition toward entrepreneurial and innovative responsiveness to a changing market.

Shared values and the development of commitment, trust and long-term orientation between the organisation and its customers become key factors in facilitating an expectation of positive gain in future dealings between customers and organisations (Peters, 1997:215-221).

4.6.2 Leadership

The leaders within an organisation must be prepared to focus on the value that can be unlocked through relationship marketing. No organisation can successfully implement a relationship marketing initiative as long as the leadership in the organisation is focused on winning at the expense of others. Organisations with greater bargaining power than their customers and suppliers must play a role in leading their own organisation and their customers to a higher state of relating, one in which value can be created and shared. The leadership must regard sharing as a virtue and understand the real meaning of a relationship before committing the organisation to relationship marketing (Gordon, 1998:24).

The findings of an online survey conducted among corporate privacy officers in October 2001 indicated that 86 per cent of organisations had a Privacy Notice and Privacy Policy on the organisation's website, while 65 per cent had in place a Consumer Privacy Policy for the organisation's offline activities that collect and use personal information. A total of 49 per cent said that their organisation's top management was strongly behind a pro-active, leadership-oriented privacy policy. Of the privacy officers surveyed, 30 per cent believed that while management sees privacy as an important issue, management preferred not to take a leadership role. According to 21 per cent of the respondents, senior management sometimes view privacy issues as an annoyance, but managers do

recognise the need to comply effectively with laws and regulations (Opinion Research Corporation International & Westin, 2001:6-7).

Privacy leadership involves setting the highest possible standard of respect for personal information, applying it to all customers, promoting the standard as a competitive edge and making sure compliance is seamless (Privacy Council, 2002). Setting privacy standards has to be part of an organisation's strategy and is discussed in the next section.

4.6.3 Strategy

At the corporate strategy level, the role of marketing is threefold (Webster, 1992:11):

- to assess marketing attractiveness by analysing customer needs and requirements and competitive offerings in the markets potentially available to the organisation, and to assess its potential competitive effectiveness;
- to promote a customer orientation by being a strong advocate for the customer's point of view versus that of other constituencies in management decision-making, as called for by the marketing concept; and
- to develop the organisation's overall value proposition (as a reflection of its distinctive competence, in terms reflecting customer needs and wants) and to articulate it to the market and throughout the organisation.

Organisational strategies include customer strategies to develop an understanding of the capabilities needed to advance the customer relationship. The customer must be central to the business strategy if the organisation is to implement relationship marketing effectively. Strategy needs to be aligned between the organisation and its customers to ensure that each understands the direction of the other, enabling each to assess the other in its role as long-term partner, and to create the value each wants. Thus, strategy needs to be customer-centric, with relationship objectives and strategies geared to individual customers (Gordon, 1998:25). In a traditional economy, value was typically a result of scarcity, while in the new digital economy value comes from

plenitude. This important observation points to the foundation for business strategies of the future. Managing supply and demand for products is not as important as managing networked relationships of products (Prabhaker, 2000:164). A structured approach to the utilisation of customer information is needed if organisations are to exploit its value and use it effectively to build customer relationships. Such an approach must begin with an understanding of how the value created between organisations and their customers may be characterised (Peters, 1997:214). An organisation's long-term success in a market is essentially determined by its ability to expand and maintain a large and loyal customer base (Kandampully & Duddy, 1999:51) and the issue of privacy can be an important element in this strategy.

4.6.4 Structure

Gordon (1998:25) believes that organisations that organise according to relationship marketing should go beyond considering traditional organisational structures such as business units organised by product or market and should consider organising by relationship and capability. Interactive databases are making relational marketing a reality for consumer goods (Webster, 1992:6). An organisation that applies a relationship-type strategy can monitor customer satisfaction by directly managing its customer base. In a relationship marketing situation, the organisation can build up an information system to provide management with a continuously updated database of its customers and continuous information about customers (Grönroos, 1997:331). An important role for marketing management is to ensure that information about customer service and satisfaction is gathered and distributed to all parts of the organisation on a regular basis (Webster, 1988:39).

A customer orientation is more than a set of beliefs. It must be supported by up-to-date and accurate information about the needs, wants, preferences and buying habits of customers obtained through direct contact with them. The central question that should guide all information gathering is 'how does the customer define value and how well are we providing it? (Webster, 1994:30). As was mentioned in Section 4.3.2, information

has emerged as an asset with a market value. A structure approach to the utilisation of customer information is therefore needed if organisations are to exploit this value and use it effectively to build customer relationships. Value adding marketing activities should provide benefits for both consumers and organisations, thus increasing their goal satisfaction and alignment (Peters, 1997:215). The creation of value for both organisations and customers relies increasingly on the co-ordination of business activities and individual customer information and is addressed in Section 4.6.5.

4.6.5 People

People are the key to any relationship and people have to be supported by technologies and processes to multiply their capabilities and make them even more effective. However, the findings of a study among United States and European organisations indicate that only six in 10 organisations have implemented employee training programmes to lower their technology risk (Green, 2001:57; Kelly, 2001:18). Organisations should train, develop and grow people into owners of a process which seeks to build customer relationships (Gordon, 1998:27). Skill and effectiveness in the use of information can be seen as critical to becoming market-oriented and gaining success in an intensely competitive business environment (Peters, 1997:225). Employees' future role in relational exchange processes lies in protecting consumer privacy and being accountable for their processes for collecting and using personal information, including e-mail addresses. Indiscriminate use and careless trading of information should be eliminated (Schwartz, 1998:51).

Internationally, many organisations have appointed chief privacy officers (CPOs) to help organisations reassure customers that their privacy will be protected. In general, the job description of a CPO is to train employees with regard to privacy, to align the organisation's privacy policies to avoid potential risks, to manage customer privacy disputes and to inform senior executives of how the organisation should deal with privacy issues (Nash, 2000:62).

Marketing can no longer be the sole responsibility of a few specialists. Everyone in the organisation must be charged with the responsibility for understanding customers and contributing to developing and delivering value for them. It must be part of everyone's job description and part of the organisation culture, as previously discussed in Section 4.6.1 (Webster, 1992:14). The ability to deliver on commitments made to customers by the organisation rests at least in part on internal co-ordination within the organisation. This co-ordination may foster co-operative interdependence between the organisation and its customers, whereby each party views its goals as being linked to that of other parties, and recognises that as one party moves towards its goal, this in turn helps the other party to achieve its own goal (Peters, 1997:221).

4.6.6 Technology

Technology can serve multiple roles within an organisation, and can mediate between an organisation and its customers. Information technology changes the role of the customer and the patterns of market communication, relations and interactions. Marketers and managers must be aware of new developments in the relevant technology and the possible effects thereof because technology can and does affect business activities and relationships in many different ways (Zineldin, 2000:11). Technology provides an invisible, automatic means of collecting and analysing consumer data and can construct consumer profiles. This very invisibility compromises consumer privacy. Most consumers do not realise that their information is being collected and used to construct profiles. Most have not consented to divulge the information nor to be the target of promotion (Franzak *et al.*, 2001:637).

The Internet and World Wide Web will dramatically alter the way organisations conduct business and establish business or customer relationships, changing both the market opportunities and the information technology and network infrastructure. Information technology and other technologies present opportunities to develop new relationships with end users (Zineldin, 2000:13,15). Information technology, through the appropriate use of customer information, can facilitate goal satisfaction and compatibility between

the organisation and its customers, and provide ways in which to recognise and enhance the long-term value of customers.

One of the most profound implications of information-processing technology is the realisation that traditional strategic trade-offs may be obsolete. This can be illustrated by the withdrawal of a proposed customer profile database by the Lotus Development Corporation and Equifax in the USA. In 1991, the Lotus Development Corporation intended to produce and sell a CD-ROM called Lotus Marketplace: Households. Using data from the Equifax credit bureau, the CD-ROM contained information on the buying patterns and estimated incomes of more than 120 million Americans. While the product did not contain information which was not already publicly available, consumers perceived the aggregation and availability of this information as a threat to their privacy and the ensuing outcry caused the organisations concerned to abandon the project (Peters, 1997:225).

A survey among 1 500 companies in the USA and Europe has indicated that organisations do not adequately understand the risks posed by technology, have difficulty identifying potential risks, and lack the tools to manage them effectively (Veysey, 2001:1; Zinkewicz, 2001:50). As the use of the Internet develops further, an organisation's capability to collect information from customers and the potential to create value from such information also increases. Apart from having the capability to leverage such information, organisations likewise need to build a level of trust so their customers can comfortably provide sometimes highly personal and confidential information. Technology must enable marketers to develop new knowledge and insight about the customer relationship and facilitate action on the information. In essence, knowledge is what employees know about customers, products, processes and past successes and failures. Knowledge creates value in use and is discussed below, in Section 4.6.7.

4.6.7 Knowledge

Relational marketing theory holds that social and structural ties between organisations and customers can be established and leveraged to stimulate mutually beneficial economic exchanges. Directly related to and underlying customer relationship management (CRM), is the emerging discipline of knowledge management. In a marketing context, knowledge is defined as information that is relevant, actionable and based at least partially on experience. Customer profile information is crucial for relationship building. It provides an advantage in a competitive marketplace, where knowledge about the target buyer needs to be more detailed, more personal, increasingly timely and preferably exclusive. For relationship marketing, rich descriptions of personal behaviour that indicate wants and needs are more valuable than estimates of characteristics based on large samples. Ongoing developments in information technology facilitate the gathering, processing and analysis of the information required to forge close buyer-seller relationships. Information helps organisations overcome barriers to transactions by guiding judicious allocation of resources to strategic marketing variables. Private information, with its restricted distribution, can produce the type of knowledge that provides a competitive advantage (Franzak *et al.*, 2001:634).

Personal information moves through a complex web and access to personal information is enabled by the availability of large commercial databases compiled from public records or from responses supplied by consumers. Organisations seeking information on consumers may tap into this network in two ways. First, organisations can use their own data to profile their existing customers. Second, to enable better targeting of their existing customers, organisations may have their customer files overlaid with additional personal information by obtaining a list compiler or list broker to match the customer file against a third-party marketing database (Culnan, 1993:347).

As the dynamics of the global marketplace and the requirements for competition success have changed, the need for managing the customer relationship has grown.

CRM involves attracting, developing and maintaining successful customer relationships over time. At the core of CRM is the development of a 'learning relationship' that engages customers in a two-way dialogue that is effective and efficient for both customers and the organisation. Interactions are no longer discrete transactions; rather, they reflect an ongoing knowledge-based process. A key challenge in the application of knowledge is transferring it from where it was created or captured to where it is needed and should be used (Massey *et al.*, 2001:157).

4.6.8 Process

Organisations should focus processes around existing customers, giving each the value (s)he wants by communicating with the customer as an individual. There is a need to be market-oriented in customer information use, in other words to understand and address consumer needs through the information collected in a way which is perceived as valuable by customers themselves (Peters, 1997:226). Electronic information is the lifeblood of an organisation and the value of information being stored and transmitted across organisational networks is growing (D'Aversa-Williams, 1999:6). Information is a valuable corporate asset, but many organisations are still unaware of how much at risk information can be from Internet technologies. Organisations can commit to spending on the physical security of their buildings and contents, but neglect the security of their information; the loss of which may be more damaging financially than the loss of actual physical assets (Woodward, 2000:22).

Managing information systems involves two fundamental but interdependent dimensions. First, a sophisticated technological infrastructure that enables the design and construction of high quality systems needs to be implemented. Second, organisation-wide quality-oriented behaviour needs to be established (Ravichandran, 2000:119).

In addition to hardware and software solutions, the establishment and enforcement of security policies are also critical (Gunst, 1999:62). The current data avarice, which is

leading marketers to seek out and capture more personal information, has a definite downside. The more effective the information gathering, storage and retrieval process becomes, the greater the tendency to encroach on individual privacy. At some point, marketers are likely to bump into an effectiveness ceiling, where responsiveness increases no further without the addition of personal sensitive data to the analysis process. Maintaining the balance between information and individual privacy will be one of the important challenges in the future (Fletcher & Peters, 1996:148). The cost of building a quality marketing database is high, but the return on that investment is directly related to the marketer's ability to manage, maintain, grow and use it (Williams, 1991:59).

The above section discussed the eight components of relationship marketing needed by an organisation to align its activities with the needs of its chosen customers and stakeholders. Apart from these eight components, organisations also have to be aware of the influence of external activities on their marketing strategies, as discussed below.

4.6.9 External influences on organisations' marketing activities

In exchange processes, a number of constraints or external influences on marketing activities have developed to serve as sources of consumer protection. These include legal influences, political influences, competitive influences and ethical influences (Peter & Olson, 1996:412).

Legal influences refer to relevant legislation and the agencies and processes by which these laws are upheld. The legislative environment was addressed in detail in Chapter 2. Legal influences serve to guide organisations to keep their activities within the law. Agencies such as the Advertising Standards Authority (ASA) and the Consumer Union regulate business and marketing practices in South Africa. As was mentioned in Chapter 2, the Law Commission has instituted a Project Committee which is currently investigating the privacy and data protection issue in South Africa, with the aim of improving existing legislation and adding new legislation as soon as possible. The DMA,

the ASA, the Harmful Business Practice Act, and other relevant industry law and codes were recently synthesised to provide guidelines to organisations regarding unsolicited e-mail marketing practices (Direct Marketing Association, 2001b).

Political influences refer to the pressure exerted by various consumer groups to control marketing practices. These groups use a variety of methods to influence marketing practice, such as lobbying with various government agencies to enact legislation or working directly with consumers in redress assistance and education. Several consumer protection groups have been formed to address privacy on the Internet. Two main groups have launched programmes to help consumers distinguish between legitimate e-mail pitches from marketers and other unsolicited e-mail which may be sent by scam artists or pornographers: website privacy certification organisation TRUSTe and privacy consultancy ePrivacy group launched a certification and seal programme for commercial e-mail, called Trusted Sender, in February 2002. The seal is intended to let consumers verify that the message is not spam and that the organisation sending the message is in compliance with the programme's guidelines (Schultz, 2002b).

Competitive influences refer to actions of competing organisations intended to affect each other and consumers. Consumer privacy concern is a source of competitive advantage and should be leveraged by an organisation. Organisations have a choice in how they respond to the matter of consumer privacy. They can see it as a threat and simply react defensively, or they can treat this as an opportunity and be proactive in maximising the gains through technologies and sharing such gains with the customers (Prabhaker, 2000:165). Consumers can benefit from the development and marketing of better products and services and better privacy policies and information handling practices brought about by competitive pressure. Organisations can set high standards with regard to privacy policies as a means of gaining a competitive edge.

Perhaps the most important constraints on marketing practices are ethical influences and self-regulation by marketers. Information privacy has been called one of the most important ethical issues of the information age (Campbell, 1997:47). The concern about

ethics in marketing is closely related to the issue of social responsibility, which refers to the doing of societal good unrelated or minimally related to business activities (Kavali *et al.*, 1999:573). Social pressures increasingly require marketers also to examine, from an ethical perspective, how they deal with consumers, competitors, suppliers and the government (Takala & Uusitalo, 1996:50). The Direct Marketing Association has, for example, established a number of codes and guidelines for self-regulatory actions for its members. Examples are the industry's Code of Ethics, Privacy File and Media Preference Services.

As was mentioned at the start of the chapter, discussion will focus on the dual nature of the information privacy issue in relational exchange processes. The role of organisations in relationship building as well as external influences on its marketing activities have been discussed. The remainder of the chapter addresses the consumer's decision-making processes as influenced by individual and external factors.

4.7 INFORMATION PRIVACY RELATED CONSUMER BEHAVIOUR

The field of consumer behaviour is characterised by various definitions emphasising certain dimensions of consumer' behaviour, such as affect, cognition, behaviour, decision-making processes and environmental influences. For the purposes of this discussion, the definitions of various authors (Du Plessis & Rousseau, 2003:9; Hawkins, Best & Coney, 2001:7; Peter & Olson, 2002:6) have been adapted to place consumer behaviour in perspective against the backdrop of consumers' concerns about their personal information. Consumer behaviour is defined as the behaviour patterns and activities that precede, determine and follow a consumer's decision-making, as influenced by environmental events, conducted during exchange relationships with marketers, impacting on themselves and society. Consumers' decision-making processes regarding the protection of their personal information are influenced by their beliefs, attitudes, behaviour intentions, buying behaviour and the environment. The next section discusses consumer decision-making, whereafter different factors influencing this decision-making process are addressed.

4.7.1 Consumer decision-making

Depending on the context, privacy exists when an individual can control social interaction and/or unwanted external stimuli, can make autonomous decisions without outside interference, and/or can control the release and subsequent circulation of personal information (Culnan, 1993:344). The findings of a study by Harris Interactive and Westin (2000:14) indicate that an overwhelming number of consumers in the USA, United Kingdom and Germany contend that it is 'absolutely essential' or 'very important' for organisations to show privacy notices before consumers will provide personal information for purchases. There is ample evidence to suggest that consumers world-wide view a lack of information privacy control over personal information (once divulged to organisations) as a problem. A Wall Street Journal/NBC News poll of 2 025 adults by phone found that the loss of personal privacy was the number one concern of Americans as the twenty-first century approached (EPIC, 2002:11). High majorities, ranging from 72 per cent in Germany, 78 per cent in Britain to 94 per cent in the USA, said they perceived the possible misuse of their personal information as problematic (Harris Interactive & Westin, 2000:2). The findings of a consumer behaviour survey indicate that 79 per cent of consumers agree that they have lost control over how their personal information is collected and used by organisations (Harris Interactive, 2002b:29).

The findings of the above-mentioned studies suggest that information privacy forms part of consumers' daily activities, thus impacting on their decision-making processes. The process of consumer decision-making consists of five stages, namely problem recognition, information search, alternative evaluation, the purchase and the post-purchase experience (Sheth, Mittal & Newman, 1999:520). Each of the five stages is discussed below, with specific reference to how privacy can be affected at each stage.

4.7.1.1 Problem recognition

The decision-making process begins with a consumer recognising a problem to be solved, or a need to be satisfied. Problem recognition is defined as the result of a discrepancy between a desired state and an actual state that is sufficient to arouse and activate the decision process (Hawkins *et al.*, 2001:512). Problem recognition can be a physical problem, but can also be a state of deprivation or discomfort. It is necessary to point out that the presence of need recognition does not automatically activate action. The kind of action taken by consumers in response to recognised problems relates directly to its importance to the consumer, the situation and the dissatisfaction or inconvenience created by the problem. This depends on whether there is a need of sufficient importance and whether the consumer believes there is a solution to the need that is within his or her means (Engel, Blackwell & Miniard, 1995:176).

Problem recognition can be the result of a variety of factors that influence consumer desires and perceptions, such as previous experiences, motives, emotions and culture. If a consumer has experienced a situation where there was a lack of information privacy and the consumer's information privacy has been violated by an organisation, the consumer may remember a loss of control over his or her information use. This past experience may affect the consumer in the problem recognition phase (and all other phases), leading to a situation where the consumer will consider terminating all future dealings with the specific organisation, and turn to other organisations who offer privacy protection to satisfy their needs.

4.7.1.2 Information search

Once a need or problem has been recognised, consumers search for information about various alternative ways of solving the problem. An information search is selective, since consumers choose information that is most relevant to their needs and most likely to conform to their beliefs and attitudes (Du Plessis & Rousseau, 2003:118). An information search can be internal of external. An internal search is nothing more than a

memory scan for knowledge stored in long-term memory. An external search occurs when information is collected from the environment, from family, friends, advertisements and salespeople (Engel *et al.*, 1995:183).

Information reduces uncertainty in decision-making and is the foundation for value of information. Like organisations, consumers need information to make wise decisions (Franzak *et al.*, 2001:634). Perceptions regarding the costs versus the benefits of an information search play a vital role in guiding the search process. Consumers usually invest more effort in an information search when the perceived benefits of this activity increase and the costs decline. The magnitude of information sought depends on factors such as perceived risk, involvement, familiarity and expertise, time pressure and information overload (Sheth *et al.*, 1999:529).

One of the main objectives facing marketers is to present consumers with information on which to base their decisions. Part of this process can be to inform consumers of privacy protection policies and privacy seals. The global customer quickly learns about the wide range of choices available through various kinds of modern telecommunications technologies that give virtually instant access to information world-wide (Webster, 1994:24). One of the most interesting and distinguishing dimensions of such information systems is the level of control which the consumer has over the information system (Ariely, 2000:234). As with an information search, control over the information flow seems to have both advantages and disadvantages (benefits and costs). In terms of benefits, information control allows consumers to deal with information systems that fit their individual informational needs better and are more flexible, whereas in terms of the costs, information control requires the user to invest processing resources in managing the information flow (Ariely, 2000:235). Privacy enhancing technologies are growing at a dramatic rate with the purpose of enabling Internet consumers to be informed and to make choices about the collection, use and disclosure of their private information on the Internet (Wang, Lee & Wang, 1998:68).

4.7.1.3 *Evaluation of alternatives*

The third stage in the consumer's decision-making process is an evaluation of alternatives. This occurs when the consumer decides on the value offered in the potential exchange process versus the costs (s)he has to incur. The type of evaluative criteria which a consumer uses in a decision varies from tangible costs and performance features to intangible factors such as information privacy (Hawkins *et al.*, 2001:566). Present day global consumers can choose among a much larger variety of products and services from producers located worldwide. Consumers are much more likely to judge products and services in terms of their fundamental value, defined simply as the ratio of benefit to cost (Webster, 1994:24). Placing privacy in the market environment together with such choices as colour, durability and size creates an environment in which privacy becomes another cost (Agre & Rotenberg, 1998:161). Consumers will relax their concern about information privacy if they feel that the benefits of disclosure are significant. For example, if consumers prefer custom-designed promotional offerings that fit their profile, they may decide that disclosing their information is worth it. This trade-off implies that consumer information has value (Franzak *et al.*, 2001:640). Sourcing and decision-making costs are thus reduced as consumers develop trust in a single provider.

4.7.1.4 *Purchase*

Once the consumer has evaluated the alternatives, (s)he makes the decision to purchase. It is important to note that not all purchase intentions are fulfilled, because the consumer always faces the option of aborting the purchase process. This can happen when motivations for the purchase change, circumstances change, new information provides new purchasing options, an desired alternatives are no longer available (Engel *et al.*, 1995:236).

There is a substantial proportion of consumers who maintain that the benefits of purchasing through the Internet do not outweigh their concerns (Harris Interactive,

2001b). An average of 60 per cent of online American respondents state that security and privacy concerns stop them from doing business on the Internet (GartnerG2, 2000:59; Harris Interactive, 2001b). It is estimated that as much as $24.5 billion worth of online sales will be lost by 2006 because websites are not addressing consumer's fears about privacy and security (Jupiter Media Metrix, 2002).

The Information Technology Association of America postulates that high-profile computer crime incidents sensitise people to become more concerned about the privacy and security of their personal information (Creed, 2000). It was reported that only 14 per cent of Internet users indicated that they feel safe when releasing their credit card information on the web (Udo, 2001:171). A survey of Chinese Internet users showed that 37 per cent regard a lack of information security as the biggest disadvantage of online shopping (Johnson-Page & Thatcher, 2001:266). Between 52 per cent and 60 per cent of Internet users are more willing to purchase products online when there is a secure ordering process (Greenfield Online, 2001:58) and 82 per cent believe that online companies should inform consumers exactly how their sensitive information will be secured during transmission and storage (Taylor, 2002:21). From an information privacy point it is not only important that the consumer makes the decision to purchase, but also that (s)he will be satisfied after the purchase. The final phase in the consumer decision-making process, namely post-purchase behaviour, is addressed next.

4.7.1.5 Post-purchase

The consumer's decision-making process does not end with the purchase. Instead, the experience of buying and using the product or services provides information that the consumer will use in future decision-making (Sheth *et al.*, 1999:547). If a consumer realises that the organisation discloses his or her information to others without permission after a purchase, it can lead to dissatisfaction. Dissatisfaction with delivered products and services or information practices can affect consumers' decisions to continue a relationship, and conversely increase the likelihood of exit from the

relationship, as well as negative word-of-mouth (Hirschman, 1970:55; Selnes, 1998:306).

Hirschman (1970:30) was the first to suggest a taxonomy of consumer complaining behaviour responses. This taxonomy classified options available to dissatisfied consumers into three groups: they could exit the relationship; they could voice their dissatisfaction to the seller; or they could show loyalty to the seller by neither exiting from the relationship or voicing their dissatisfaction.

Singh (1988:95) added to this taxonomy by providing more consumer complaint behaviour response categories. Besides voicing complaints to the seller, informal complaints can also be voiced to friends and relatives, and formal complaints can be lodged with agencies not directly involved in the exchange, such as consumer protection groups.

Customer service and loyalty programmes created with the best intentions by organisations are sometimes viewed as annoying junk mail and can lead to dissatisfaction after a purchase (Caisse, 2002). The Opinion Research Group Corporation contacted a random sample of 1 017 adults in the USA and reported that 60 per cent of respondents regarded junk mail as an invasion of privacy, and 47 per cent contended that receiving unsolicited e-mails from marketing made them more likely to believe that certain information practices are unethical, rather than privacy invading.

Improper activities from organisations after purchases can lead to consumer dissatisfaction. An example is activities by web-based organisations that monitor (through the use of cookies) a consumer's Internet activities without notice to or acknowledgement from the consumer, as well as a transfer of consumer's private information to other organisations without notice to or acknowledgement from the consumer (Wang *et al.*, 1998:65).

Maintaining an ongoing relationship with customers is crucial to an organisation's success. One way to secure this is by creating and publishing a customer-friendly privacy policy. Organisations have to recognise that when a consumer shares personal information with the organisation, it is an expression of trust. If an organisation protects its customers' privacy, it is protecting the proprietary nature of the relationship with its most valuable asset: its customers (Mabley, 1999:4).

In theory, all participants in an effective marketing relationship benefit. Organisations acquire the information needed to tailor product offerings and provide superior customer satisfaction in the long term. They retain customers, and through retention they obtain continuously updated information. Consumers, the recipients of improved products and services, enjoy the benefits of products designed to meet their needs, personalised attention and the stability of longer-term contracts and relationships. But both parties also sustain additional costs. For the consumer, a major cost issue relates to loss of privacy. Aspects of costs associated with loss of privacy range from the time and attention needed to eliminate or attend to unsolicited advertising, to the loss of identity.

Value requires that the benefits from information in a relationship exceed the costs associated with acquiring and using it (Franzak *et al.*, 2001:633). The above discussion on the consumer decision-making process would not be complete without some reference to the different factors that influence this decision-making process. The remainder of the chapter discusses some of the individual and external factors influencing consumers' decisions regarding information privacy.

4.7.2 Individual factors influencing consumer decision-making

The literature identifies several individual factors relating to consumer decision-making. This section focuses on the link between beliefs, attitudes, behavioural intentions and behaviour. A consumer's evaluation process begins with a combination of his or her beliefs about a product or service. Through previous experiences, knowledge and perceptions, consumers acquire many beliefs about products and services in their

environment. These beliefs form a consumer's attitude that is in turn related to behaviours toward a product or service. Consequently, consumers' intentions to perform certain actions should increase as their attitudes become more favourable.

Behavioural intentions are created through a decision process in which attitudes about two types of consequences are considered and integrated to evaluate alternative behaviours and select among them. Behaviour is expected to be highly related to behavioural intention even though certain behaviours cannot be accurately predicted from beliefs, attitudes, and intentions. The behaviour of consumers who have little knowledge and low levels of involvement are virtually impossible to predict because such consumers have very few beliefs in memory on which to base attitudes and intentions (Engel *et al.*, 1995:366; Peter & Olson, 2002:166). The different factors, namely beliefs, attitudes, behavioural intentions and behaviour are discussed individually below, with specific reference to their relevance to the empirical study.

4.7.2.1 Beliefs

Beliefs are thoughts linking an object to some feature or characteristic, and represent the information that consumers have about a situation or object (Arnould, Price & Zinkhan, 2002:460). A belief is the result of a relationship between knowledge, previous experiences and perceptions, and it eventually affects a person's attitude toward an object (Du Plessis & Rousseau, 2003:264). There appear to be different beliefs among consumers regarding unethical issues versus privacy issues (Taylor *et al.*, 1995:39). For example, consumers are more likely to believe that certain information practices are unethical, than that they are invading privacy.

Consumers' beliefs are relevant to the empirical study and some of the privacy concern questions in the measurement instrument represented belief statements pertaining to consumers' information privacy concerns. The section below focuses on the influence of knowledge, previous experiences and perceptions on consumers' beliefs regarding information privacy.

(a) Previous experience

If a consumer's knowledge is acquired from past experiences, then these experiences can be important mediating variables in understanding consumers' views on privacy. This implies that previous exposure to attempts by organisations to collect data would affect consumers' willingness to become involved in relationships (Long *et al.*, 1999:6). Personal negative experiences with any misuse of information by specific organisations are likely to increase all aspects of consumer privacy concerns, since such experiences undermine consumers' trust not only in the particular organisation involved, but in all organisations. The findings of a study by Campbell (1997:51) indicated that there was a significant positive correlation between direct negative personal experiences and consumer concerns about personal information collection.

In a study by Louis Harris and Associates (1998b:ix), 41 per cent of consumers reported that they had personally been the victim of an improper invasion of privacy by an organisation. Privacy can rapidly become an important issue, based either on bad personal experiences or on negative media coverage of offensive violations of privacy (Taylor, 2002:20). It is believed that changes in consumer perceptions about how most organisations operate and whether existing laws and practices provide reasonable privacy protection, is caused by the continued critical mass media treatment of consumer profiling, target marketing, and business information-sharing practices – especially on the Internet (Westin in Harris Interactive, 2002b:23).

(b) Knowledge

There is evidence that knowledge, or the lack thereof, is a key determinant of privacy concerns (Nowak & Phelps, 1992:37). Consumers' knowledge of actual information privacy policies and information practices may also affect their privacy concerns, although two opposing arguments have been formulated about this effect. The more knowledge consumers have about the collection and use of personal information, the more concerned they may be about information privacy practices. Milne and Boza (1999:18) have reported that consumers were less likely to trust organisations once

they become more knowledgeable about their information practices. At the same time, if consumers understood that the information collected had the potential to build a relationship in which they could participate in the creation of goods or services, privacy concerns might be diminished or superseded by their desire to participate (Campbell, 1997:46).

Privacy becomes a more meaningful concern, however, when consumers lack knowledge of the information collection and therefore its actual use. According to Nowak and Phelps (1997:100) consumers' knowledge of the method employed to gather information typically falls into one of three categories: full knowledge of information collection and information use; knowledge of information collection but not information use; and ignorance of both information collection and use.

(c) Perceptions

Both previous experience and knowledge of information practices influence consumers' perceptions of and beliefs regarding fair information practices. Perceptions concerning information privacy have a strikingly negative influence on consumers' willingness to engage in relationship exchanges (Hoffman *et al.*, 1999:81). A study by Eddy, Stone and Stone-Romero (1999:347) provided empirical evidence that the ability to authorise the disclosure has important main and interactive effects on perceptions of invasion of privacy. Consumers' perceptions affect their actions and buying habits because they make decisions and take actions based on what they perceive to be a reality (Du Plessis & Rousseau, 2003:231).

Results from research by the Web Credibility Research group at Stanford University indicate that more than 50 variables affect online users' perceptions of credibility (O'Connell, 2002). The concerns over privacy span the dimensions of environmental control and secondary use of information control. Environmental control, or the consumer's ability to control the actions of an organisation, directly affects consumer perception of the security of the exchange. In the physical world, a consumer may be concerned about giving out credit card information over the telephone to an unknown

voice within a mail-order company. On the Web, consumers may fear typing in credit card information to any commercial Web provider. Control over secondary use of information reflects consumers' perceived ability to control the use of their personal information for other purposes subsequent to the transaction during which the information is collected (Hoffman *et al.*, 1999:81).

4.7.2.2 Attitudes

Hawkins *et al.* (2001:394) refer to attitudes as the ways individuals think, feel and act toward some aspect of their environment, such as an organisation. The relationship between attitudes and beliefs is part of the cognitive and the affective processing of learning. An attitude can serve several key functions for individuals. One is a knowledge function that serves primarily as a means of organising beliefs about objects or activities such as information practices by organisations. Another is a value-expressive function where attitudes are formed based on a set of beliefs, and serve to express an individual's central values and self-concept. Hence, consumers who value privacy are likely to develop attitudes about organisations and activities that are consistent with that value. Attitudes can also serve a utilitarian function where consumers tend to form favourable attitudes toward objects and activities that are rewarding, and negative attitudes toward those that are not (Hawkins *et al.*, 2001:395).

It can be argued that the motivation for privacy often has its roots in a desire for autonomy, or at least in an avoidance of future control of one's behaviour by others (Berscheid, 1977:94). Attitudinal commitment research indicates that this is true even when the threat of control is 'self-imposed self-control, stemming from the individual's desire to act in a way consistent with his or her publicly known attitude.

Consumers' attitudes are relevant to the empirical study and some of the privacy-concerned questions in the measurement instrument represented attitude statements pertaining to consumers' information privacy concerns.

4.7.2.3 Behavioural intention

The theory of reasoned action proposes that every voluntary form of behaviour is determined by a behavioural intention. Behavioural intentions are consumers' plan to engage in specific behaviour to reach a goal. This theory assumes that consumers consciously consider the consequences of the alternative behaviours before them and choose the one that leads to the most desirable consequence. The outcome of this reasoned choice process is an intention to engage in the selected behaviour (Peter & Olson, 1996:155).

Previous research (Stone, Gueutal, Gardner & McClure, 1983:461) suggests that consumers have different beliefs about the information handling practices of organisations, based on their information-related experiences. If consumers' beliefs about information-handling practices change, their attitudes also change (attitude changes because beliefs change). If attitudes change, then behavioural intentions will also change. In the case of information privacy, a consumer may perceive that the desired level of information control was not achieved during a particular interchange with an organisation (belief), and is now experiencing a negative affect as a consequence (attitude), and, therefore, (s)he does not intend to disclose any additional information to the organisation during subsequent interactions (behavioural intention).

Consumers' behavioural intentions are relevant to the empirical study and some of the privacy-concerned statements in the measurement instrument addressed the issue of whether consumers intend to engage in specific behaviour to protect their information privacy.

4.7.2.4 Behaviour

The relationship between attitudes and behaviour, and particularly the importance of attitudes as either a precondition or a predictor of behaviour, has been widely discussed in marketing and consumer behaviour literature (Long *et al.*, 1999:6). Several

researchers have struggled with the link between privacy concern and behaviour (Sheehan & Hoy, 1999:40). Whether an individual determines that his or her privacy is being invaded or not depends on the characteristics of the situation, on an individual's own judgement of the situation, and on the perceived reputation of the organisation using the information (Sheehan & Hoy, 1999:40; Wang & Petrison, 1993:17).

Several studies have indicated that consumers are willing to change their purchasing behaviour due to privacy concerns. A study conducted by Cyber Dialogue (2001:57) has shown that 27 per cent of Internet users stated that they had abandoned an order online because of privacy concerns, while 21 per cent had switched from online purchasing to placing an order offline. Findings from a study by Harris Interactive (2002b:14,44,72) concluded that consumers are willing to change their behaviour if they feel an organisation has established strong and trustworthy privacy practices. A total of 83 per cent said they would stop doing business entirely with an organisation if they heard or read that an organisation was using its customers' information in a way they considered to be improper. In the same study, 56 per cent of consumers decided not to use or purchase something from an organisation because these consumers were not sure how the organisation would use their information. These findings demonstrate that consumers will alter their behaviour if they are confident that an organisation, whether online of offline, will follow its privacy policies. Interesting findings from a study by Sheehan (1999:26) indicated that men were likely to adopt behaviours to protect their privacy when they become concerned, whereas women rarely adopt protective behaviours. Harris Interactive (2002b:77) reported, however, that women are more likely than men to change their behaviour if they were confident an organisation would follow its privacy policies.

Harris Interactive and Westin (2000:11) identified six information privacy protective behaviours by consumers. First, they remove personal information such as a name and address from marketing lists. Second, they may refuse permission to sell or give personal information to another organisation. Third, they may demand to be informed on information practices before the purchase. Fourth, they may refuse to provide

information considered irrelevant or too personal. Fifth, they can decline a purchase opportunity when they feel unsure of how personal information will be used. Finally, they can request access to their own personal information in organisational databases.

There is also evidence to suggest that even though consumers are concerned about their privacy, they do not necessarily change anything about their behaviour to address the concern. Some individuals consider privacy an absolute right, and many people are concerned about their privacy in an abstract sense. However, there have recently been indications that individuals are increasingly changing or adopting behaviours in light of information requests which they feel invade their privacy (Sheehan & Hoy, 1999:40). Many consumers surrender their personal information willingly, knowing that they receive substantial benefits in return. For most people, the benefits gained by providing such potentially invasive information far outweigh any of their concerns.

Some organisations, however, do not intelligently organise and use the information they collect, much less deliver value to consumers in return for it (Hagel & Rayport, 1997:55). Turner and Varghese (2002:11) reviewed the results of five major consumer privacy surveys conducted in 2001. Their report concluded that these consumer surveys were consistent in finding high levels of concern about privacy. However, they caution that a closer look shows wide variations in results and a disconnection between consumer preferences and behaviour.

Consumer behaviour is relevant to the empirical study and specific items in the measurement instrument addressed the issue of whether or not consumers adopt protective behaviour when it comes to their information privacy.

In the previous sections, the link between beliefs, attitudes, behavioural intentions and behaviour as it pertains to information privacy, was addressed. This is particularly relevant to the study, since the privacy-concerned statements in the measurement instrument represent consumers' beliefs, attitudes, behavioural intentions and

behaviours. Detail on the different questions in the measurement instrument is discussed in Chapter 6.

The final section in this chapter relates to external influences and its impact on both organisations' marketing activities and consumers' decision-making processes.

4.7.3 External influences on consumers' decision-making processes

A powerful approach to understanding external influences is to analyse the situations in which the consumer experiences the environment (Peter & Olson, 2002:266). While the business environment continues to provide a relatively friendly climate for accessing personal information, consumers are increasing their demands for protection. However, although more consumers are concerned about attacks on their privacy, the courts continue to uphold the rights of commercial free speech. Most consumers are unaware of how personal information is collected, used and distributed, and they are unaware of how technology helps in collecting personal information. There is also widespread misunderstanding about existing privacy laws and regulations. Frustrated by their lack of control, more consumers demand to know how their personal information will be used by organisations.

The social environment includes all social interactions between and among people. It is especially the social interactions between consumers and organisations that affect consumers and their behaviour regarding information privacy. Indirect social environmental factors such as culture, subculture and social class can also influence the beliefs, attitudes, behavioural intentions and behaviours of consumers.

4.7.3.1 Culture and subculture

Culture is defined as the meanings that are shared by people in a social group (Peter & Olson, 2002:290). Cultural factors can have a strong impact on individual responses

and sometimes overshadow the impact of other individual background factors such as education (Milne, Beckman & Taubman, 1996:23).

Consumers from different cultures tend to view information privacy issues differently (Rawwas *et al.*, 1996:53). It was found that a country's cultural values have a significant role in explaining the level of privacy concern in a country (Smith, 2001:12). Higher levels of individualism, masculinity and power distance in a society such as the USA, were associated with higher levels of privacy concern. The relationship with uncertainty avoidance was the reverse in European countries. There also seems to be a relationship between the cultural values in a country and the regulatory approach embraced by that country.

Subcultures are distinctive groups of people in a society that share common cultural meanings. Marketers use a variety of demographic characteristics to identify subcultures based on factors such as age, gender and income level. Various studies have reported that information privacy concerns increased with age, indicating that older people were generally more concerned about privacy and less positive about data collection practices (Nowak & Phelps, 1992; Milne *et al.*, 1996; Campbell, 1997:51; Milne & Boza, 1999:18; Harris Interactive & Westin, 2000:5; Rainie, 2002:20). Studies comparing consumer attitudes of high and low income consumers found conflicting results. Some studies indicated that more affluent and established individuals viewed the concept of privacy more seriously (Wang & Petrison, 1993; Harris Interactive & Westin, 2000:8), whereas other studies indicate that consumers with a lower income are more concerned about potential misuse of their information (Milne & Boza, 1999:18; Harris Interactive, 2002b:43). Women were generally more concerned about the secondary use and potential misuse of their personal information than men (Louis Harris & Associates, 1998b, ix-xviii; Milne & Boza, 1999:18; Sheehan, 1999:24-38; Harris Interactive, 2002b:93). This led to women's being more likely to express concern about insecure transactions or situations where their personal information could be stolen (Harris Interactive, 2002b:32).

Consumer culture and subculture are relevant to the empirical study since privacy concerns were compared between language groups (reflecting different cultures) and age and gender groups (reflecting subculture).

4.7.3.2 Social class

Social class refers to a national status hierarchy by which groups and individuals are distinguished in terms of esteem and prestige. Social class is influenced by the level of education and occupation (Peter & Olson, 2002:340). Findings from a study by Harris Interactive and Westin (2000:5, 8) indicated that more highly educated consumers were more likely than less educated consumers to report personal experiences of privacy invasion and to limit the use of their personal information. This was supported by findings from studies by Phelps *et al.* (2000:34) and Rainie (2002:20). Other studies, however, showed conflicting results. One study suggested that respondents with the least and the most education were the most concerned about privacy, while the middle group was less concerned (Milne *et al.*, 1996:25). A study by Harris Interactive (2002b:43) found the opposite: consumers with less education were more concerned about privacy than those with more education.

Social class is relevant to the empirical study since comparisons between different income groups, educational groups and occupational groups in terms of privacy concerns were investigated.

4.7.3.3 Family and reference groups

Direct social environmental factors such as family and reference groups also have a strong influence on consumers' knowledge and feelings about organisations. People learn acceptable and appropriate behaviours, and acquire many of their values, beliefs and attitudes through direct social interaction with their families and reference groups. A reference group is a group whose presumed perspectives, attitudes or behaviours are used by an individual as the basis for his or her perspectives, attitudes, or behaviours

(Arnould *et al.*, 2002:553). Consumers who are concerned about their information privacy will be influenced by consumer advocacy groups and may share their common values, beliefs and behavioural norms.

Marketers are interested in how family members interact and influence each other when making decisions for themselves and/or the household. Through socialisation processes, families transmit the cultural meanings of society, subcultures and social class to their children (Peter & Olson, 2002:361).

One area of concern that has arisen as part of the international privacy issue is children's safety issues as they relate to databases (Direct Marketing Association. 2001a:3). In 1998, the USA passed the Children's Online Privacy Protection Rule (COPPA) to force operators of youth-oriented websites to obtain parental consent before collecting any personal data about children younger than 13 years (McGuire, 2002). The findings of a research survey conducted by David Binder Research (2001:22) in the USA have indicated that 82 per cent of parents said that it was necessary for households with children to be equipped with child-filtering and spam control to block unsuitable Internet material from reaching children, and 81 per cent of parents showed concern about violations to their children's privacy when using the Internet.

4.8 SUMMARY

The evolution of marketing and the advocacy to extend relationship marketing into the management of the exchange processes within consumer markets have resulted in a growing interest in treating customers on an individual basis. This chapter has provided an explanation and overview of the relational exchange processes between consumers and marketers, and of the key elements in this process. On the one hand, it focused on the role of organisations in relationship building, and on the other hand it focused on consumers and the factors influencing their decision-making process. This chapter has addressed certain consumer elements such as beliefs, attitudes, behavioural intentions,

behaviour and consumer decision-making. Together with the background on consumer information privacy set out in Chapter 3, Chapter 4 creates the basis for the empirical part of the study. The next chapter provides a discussion on the different research hypotheses and their underlying rationale.

CHAPTER 5
PROBLEM STATEMENT AND FORMULATION OF HYPOTHESES

5.1 INTRODUCTION

Chapter 2 explored the theoretical foundation of the topic under investigation, and Chapters 3 and 4 provided an overview of the specific literature upon which the research hypotheses in this study are based. In this chapter, the focus shifts toward the empirical study. Here the problem statement is discussed and specific research hypotheses are formulated. A rationale is given to place each hypothesis in perspective in relation to the set objectives.

5.2 PROBLEM STATEMENT

There is sufficient evidence to suggest that consumers world-wide recognise a problem with regard to a lack of information privacy and control over personal information once information has been divulged to organisations. Consumer attitudes about privacy have been researched in various countries and have been addressed in public opinion surveys in a number of disciplines, including law, political science, sociology and psychology. Several studies have documented high levels of concern among consumers regarding their information privacy. Consumer privacy concerns are seen as an issue of high intensity expressed by more than three quarters of American consumers in 2001 (Westin, 2002:16). Louis Harris & Associates and Dr Alan Westin conducted a Privacy Concerns and Consumer Choice Survey in 1998, analysing privacy attitudes and concerns. The conclusion from this study was that concern over threats to personal privacy remains at a very high level, and is increasing (Louis Harris & Associates & Westin, 1998:ix). A Wall Street Journal/NBC News poll of 2 025 adults has also found that the loss of personal privacy was the number one concern of Americans as the twenty-first century approached (EPIC, 2002:11).

The findings of studies in Japan, Canada, the United Kingdom and Germany have indicated that consumers in these countries were also concerned about information privacy (Maynard & Taylor, 1996:41; Campbell, 1997:51; Gallup, 2000:49; Harris Interactive & Westin, 2000:5). A 1998 survey conducted by the Georgia Institute of Technology's Graphic, Visualization & Usability Center found that 77 per cent of respondents reported that privacy was more important to them than convenience (EPIC, 2002:14). Turner and Varghese (2002:11) reviewed the results of five major consumer privacy surveys conducted in 2001. Their report shows that recent consumer surveys were consistent in finding high levels of concern about privacy. Nearly two-thirds of all consumers who were very concerned about their privacy also conveyed a great deal of concern about the potential misuse of their information by organisations (Harris Interactive, 2002b:100).

Marketing is growing and expanding into global markets. Much of this expansion is due to rapid improvements in technology, making certain marketing practices, especially direct marketing, more feasible (Milne, Beckman & Taubman, 1996:22). The Internet has grown considerably during the past decade, particularly in respect of its use as a tool for market exchange. This rapid growth has raised concern regarding the collection and dissemination of consumer information by marketers who participate in online activities (Miyazaki & Fernandez, 2001:27). Recently, several studies have been conducted to determine privacy concerns in an online environment. Sheehan and Hoy (1999:40) have demonstrated that as individuals' concerns with privacy increased, the frequency with which they registered for websites decreased, and that they were more likely to provide incomplete information to websites. A survey of 10 000 web users conducted by the Georgia Institute of Technology concluded that privacy overshadowed censorship as the most important issue facing the Internet (Machlis, 1997:2). Other studies have confirmed that privacy is online consumers' biggest concern (Tweney, 1998:66; Udo, 2001:169).

Research by Hoffman, Novak and Peralta (1999:80) has also revealed that consumers believe that their lack of control over the access that web merchants have to their personal information during online transactions reduces the trust between themselves and the organisations on the Internet. Seventy-eight per cent of e-mail users surveyed said they were concerned about the privacy of personal information that they give out on the Internet (Gallup, 2001:51), and several studies have indicated that an average of 70 per cent of American consumers are concerned about threats to their personal privacy when using the Internet (Harris Interactive, 2002a:2; Tedeschi, 2002a; Jupiter Media Metrix, 2002). A study by Harris Interactive (2002b:13) at the end of 2001 concluded that both on and off the Internet, consumers are more concerned about privacy than they had been previously (over the past two years), and they are much more assertive in taking steps to protect their privacy.

While several international studies have shown strong evidence indicating different dimensions of information privacy concerns, similar findings do not exist in South Africa. Although privacy policies and practices are of great concern in the international arena, there is no research evidence that information privacy is an issue or a matter of concern to South African consumers. The research problem can thus be formulated as a **lack of knowledge and understanding of information privacy concerns among South African consumers.** On the basis of this research problem, several research objectives can be formulated and are discussed in the following section.

5.3 RESEARCH OBJECTIVES

Consumers' concerns regarding the privacy issue are very real. For marketers, the challenge is to balance the advantages of using consumers' personal information for marketing purposes with consumers' information privacy concerns (Milne & Gordon, 1994:46). In order to do this effectively, marketers have to understand the consumer's concerns in a privacy sensitive commercial environment, since consumer privacy concerns can potentially turn long-term relationships into short-term transactional exchanges (Prabhaker, 2000:161). The primary objective (PO) of this study is **to**

identify and explore the information privacy concerns of South African consumers in a commercial environment.

In the past decade, many researchers have recognised that consumer privacy concern is a multi-faceted issue (Wang & Petrison, 1993:17; Campbell, 1997:45; Taylor, 2002:20). This has been corroborated by empirical research. Given the multi-dimensional nature of information privacy concerns, several secondary objectives were set to determine the level of concern among South African consumers about privacy.

The first secondary objective (SO1) is to determine the underlying dimensions of information privacy concern. This objective was formulated to support the primary objective by **identifying** the different information privacy concerns of consumers. Kelman (1977:169) referred to privacy as 'the freedom of the individual to pick and choose for himself the time and circumstances under which, and most importantly, the extent to which, his attitudes, beliefs, behavior and opinions are to be shared with or withheld from others'. A thorough understanding of consumers' privacy concerns requires a detailed examination of the beliefs, attitudes, behavioural intentions and expectations that underlie those concerns. The focus of the research was therefore to explore the concern of consumers about different aspects of information privacy pertaining to data collection, data storage, data use, data disclosure and solicitation.

A better understanding of the multi-dimensional structure of information privacy will enable marketers to understand information privacy and privacy invasion, as well as to predict the types of situations that can potentially create privacy or invasion experiences (Laufer & Wolfe, 1977:25). As early as 1983, Stone *et al.* (1983:459) realised that information privacy has several dimensions. They compared information privacy values, beliefs and attitudes across several types of organisations. Their results revealed significant differences among the various organisational types regarding information privacy values, beliefs and attitudes. Nowak and Phelps (1992:34) focused their investigation on consumers' information-related knowledge of and beliefs about information privacy. Their results indicated that privacy was an important concern, that

many consumers were not very knowledgeable about specific direct marketing practices, that consumer concern was affected by the type of practice and the specificity of information, and that most consumers favoured restrictions on the gathering and use of personal information.

Culnan (1993:341) measured differences in attitudes between consumers who objected to certain uses of personal information and those who did not object. She reported that consumers with positive attitudes were less concerned about privacy, perceived shopping by mail as beneficial and had coping strategies for dealing with unwanted mail. Wang and Petrison (1993:12) found that consumers were more concerned about situations where their personal and financial records were sold to other organisations without their consent, than they were about relationship marketing situations where an organisation collects and uses information to contact its own customers repeatedly. The same authors conducted a follow-up study in 1995, indicating different dimensions of consumer privacy among American and British consumers (Petrison & Wang, 1995:19). In their study, Americans expressed more concern about solicitations as privacy invasion, while the Britons were primarily concerned with the collection and exchange of consumer information. Findings from a study by Taylor, Vassar and Vaught (1995:45) demonstrated that consumers did not believe that their privacy rights were adequately protected by law and business practices. The Privacy Concerns and Consumer Choice Survey in 1998 (Louis Harris & Associates & Westin, 1998:ix) reported that most people felt that organisations asked for too much personal information, and that consumers had lost control over how this information was used. Moreover, few people expressed strong confidence that organisations were using consumers' personal information properly. A follow-up study showed that the vast majority of Internet users were very concerned about threats to their personal privacy online, despite the fact that only a very small portion reported that they had actually been victims of online privacy invasion (Louis Harris & Associates & Westin, 1998a).

Phelps, Nowak and Ferrell (2000:27) examined consumers' information concern behaviour consistency and their perceptions regarding the exchange relationships with

marketers that gathered and used personal information. Their findings indicated that public policy and self-regulatory efforts to alleviate consumer privacy concerns should provide consumers with more control over the initial gathering and subsequent dissemination of personal information. The IBM-Harris Multi-National Consumer Privacy Survey (Harris Interactive and Westin, 2000:5) showed that significant numbers of American, British and German consumers said that they were victims of privacy invasions by organisations, and that the majority of consumers voiced concern about the possible misuse of their personal information. Harris Interactive (2001a, 2001b, 2001c) conducted a series of three surveys on consumer privacy attitudes and behaviours. Their findings revealed relative consistency over the three surveys, indicating that consumers were willing to provide both online and offline companies with basic information, but that they were more protective of personal information and less comfortable sharing more sensitive information. A survey commissioned by NCR and BMRB Financial, European Union, indicated that 60 per cent of consumers were satisfied when organisations used their personal data in marketing, as long as they received personalised services and tangible rewards in return (Darby, 1999:2). Another study by Jupiter Research confirmed this attitude and reported that 82 per cent of Internet users would give personal information to new shopping sites in exchange for the chance to win something in a competition (Tedeschi, 2002a).

This study is an extension of the above-mentioned previous studies, and focuses on different aspects of consumer information privacy. Previous studies have examined some dimensions underlying information privacy concerns, but the dimensions differed from study to study, and a common framework relating to these dimensions has not yet emerged. Since the theoretical base on information privacy is very fragmented, and few empirical tests exist on the dimensions of concern regarding information privacy, several constructs have been identified from the theory discussed in Chapters 2, 3 and 4. From the literature, eight main dimensions have been identified:

- data collection (Chapter 3, Section 3.4.1);
- data storage and security (Chapter 3, Sections 3.4.2 and 3.4.5);
- data use (Chapter 3, Section 3.4.4);

- data disclosure and dissemination (Chapter 3, Section 3.4.6);
- solicitation (Chapter 3, Section 3.3.1);
- privacy protection policies (Chapter 3, Section 3.5);
- legislation and government protection (Chapter 2, Section 2.6); and
- behavioural intentions (Chapter 4, Section 4.7.2.3).

The first five dimensions were addressed from a consumer perspective and related to consumers' beliefs and attitudes (addressed in Chapter 4, Sections 4.7.2.1 and 4.7.2.2). The first secondary objective was thus set with the aim of measuring South African consumers' beliefs, attitudes, behavioural intentions and expectations regarding data collection, data storage, data use, data disclosure and solicitation. The underlying dimensions of consumers' information privacy concerns were uncovered by means of factor analysis. Thereafter, the other secondary objectives were addressed in support of the primary objective.

The remainder of the secondary objectives aimed to **explore** the different information privacy concerns in relation to specific consumer behaviour activities. Hypotheses were formulated for each secondary objective to enable empirical testing of the issues at hand. The different hypotheses are discussed in full in the next section. The remaining secondary objectives are listed below for the sake of convenience (also mentioned previously in Chapter 1, Section 1.4.2):

- SO2: To establish differences between consumers' manifest behaviours to protect their privacy and their privacy concerns;
- SO3: To establish differences between consumers in terms of their personal experiences of invasions of privacy and their privacy concerns;
- SO4: To establish the dependency between gender and personal experiences of invasions of privacy;
- SO5: To establish differences between consumers in terms of their knowledge about information protection practices and their privacy concerns;
- SO6: To establish the dependency between age and knowledge about information protection practices;

- SO7: To establish the dependency between level of education and knowledge about information protection practices;
- SO8: To establish differences between consumers in terms of their Internet usage and their privacy concerns;
- SO9: To establish differences between consumers in terms of their direct purchasing behaviour and their privacy concerns;
- SO10: To classify consumers into different privacy sensitive segments based on their general privacy concerns;
- SO11: To identify differences between consumers in terms of their demographic characteristics and their privacy concerns.

The research hypotheses will now be formulated and discussed.

5.4 RESEARCH HYPOTHESES

Based on the literature review presented in Chapter 2, the theoretical foundations of consumer information privacy discussed in Chapter 3, and the overview of consumer behaviour presented in Chapter 4, as well as the research objectives, it is now possible to formulate and state specific hypotheses to be tested in the empirical study. The empirical research addresses selected aspects regarding consumer information privacy. The identification of the underlying dimensions of consumer information privacy concerns (SO1), serves as the basis to test the hypotheses formulated to address the rest of the secondary objectives. The different hypotheses formulated for testing are discussed below.

5.4.1 Hypothesis 1

Consumers may engage in various protective behaviours, believing that they can manage their information and thus minimise the potential consequences of supplying this information. The crucial element of information management in terms of planning behaviour is that the consumer is often unable to predict the nature of that which has to

be managed (Laufer & Wolfe, 1977:36). The results of the Privacy Concerns and Consumer Choice survey (Louis Harris & Associates & Westin, 1998:x) indicated that consumers' concern about how organisations use their personal information manifested in privacy protection behaviours. The IBM-Harris Multi-National Consumer Privacy Survey (Harris Interactive & Westin, 2000:11) compared Internet users and non-users in terms of six privacy protective behaviours in three different countries. The results showed several differences in behaviour between Internet users and non-users, with Internet users being more prone to taking protective action. Both groups have, however, refused to provide information which they regard as not really needed or too personal.

Sheehan and Hoy's study (1999:40) reported several significant correlations between consumers' online privacy concerns and their behaviour. One such form of behaviour is the request to remove personal information from mailing lists. Phelps *et al.* (2000:35) have found that previous name removal behaviour had a strong correlation to people's privacy concern level. A study by Harris Interactive (2002b:13) concluded that consumers were becoming much more assertive in taking steps to protect their privacy. Nearly a third of all consumers were in the high privacy assertiveness category, suggesting that they are very active in protecting their privacy (Harris Interactive, 2002b:101). The results of five major consumer privacy surveys conducted in 2001 were reviewed by Turner and Varghese (2002:11), who reported a disconnection between consumer preferences and behaviour. Conflicting results have also been reported regarding protective behaviour in respect of privacy concerns and gender. A study by Harris Interactive (2002b:77) found that women are more likely than men to change their behaviour if they were confident that an organisation would honour its privacy policies. The findings of a study by Sheehan (1999:25) indicated the opposite, namely that men were likely to adopt behaviours to protect their privacy when they become concerned, and that women rarely adopted such behaviours.

A secondary objective was set **to investigate whether there are differences between consumers' manifest behaviours to protect their privacy and their privacy concerns (SO2).** The following null and alternative research hypotheses were

formulated in the context of the findings of the above-mentioned studies and the stated objective:

H_0: There is no significant difference between consumers in terms of their protective behaviour and their privacy concerns.
H_1: There is a significant difference between consumers in terms of their protective behaviour and their privacy concerns.

5.4.2 Hypotheses 2a and 2b

Previous empirical research has suggested that an individual's concern for privacy is likely to vary over the course of his or her lifetime, based on personal experiences. When consumers have had multiple previous negative experiences with data inaccuracies, they become more reluctant to provide subsequent information (Vidmar & Flaherty, 1985:100; Campbell, 1997:46). A significant positive correlation between direct negative personal experiences and consumer concerns about data collection and errors was reported by Campbell (1997:51). The findings of studies by Louis Harris & Associates and Westin (1998b:ix) and Harris Interactive and Westin (2000:2) indicate that between 20 and 40 per cent of respondents have been victims of an invasion of privacy by an organisation. Louis Harris & Associates and Westin (1998a) 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. Internet users in the USA, the United Kingdom and Germany reported a higher incidence of privacy invasions than Internet non-users in these countries (Harris Interactive & Westin, 2000:3). Among American and British consumers, males were more likely than females to report being a victim of a privacy invasion. The gender gap is even more pronounced in Germany, where 35 per cent of male and 22 per cent of female respondents claimed that they had been victims of a privacy invasion by an organisation (Harris Interactive & Westin, 2000:5). Another study found that 45 per cent of Americans think that shopping online threatens their personal privacy (TNS Intersearch, 2001:44).

The above-mentioned findings indicate relationships between negative personal experiences and privacy concerns, as well as gender and negative personal experiences. Secondary objectives were set **to establish differences between consumers in terms of their personal experiences of invasions of privacy and their privacy concerns (SO3), and to establish the dependency between gender and personal experiences of invasions of privacy (SO4).** From this the following null and alternative hypotheses were formulated:

H_0: There is no significant difference between consumers who have been victims of invasions of privacy and consumers who have not been victims of invasions of privacy in terms of their privacy concerns.
H_{2a}: There is a significant difference between consumers who have been victims of invasions of privacy and consumers who have not been victims of invasions of privacy in terms of their privacy concerns.

H_0: Being a victim of invasion of privacy is independent of gender.
H_{2b}: There is a dependency between being a victim of invasion of privacy and gender.

5.4.3 Hypotheses 3a, 3b and 3c

Consumers' knowledge level of actual privacy policies and practices may affect their privacy concerns, although opposing arguments have been presented about this effect. When individuals have extended knowledge about the collection and use of personal information, they tend to be more concerned about information privacy practices. At the same time, however, if consumers understand that the data collected has the potential to build a relationship in which they can participate in the creation of goods and services, their privacy concerns might be diminished or superseded by their desire to participate (Campbell, 1997:46). The characteristics of consumers who are aware of name removal procedures versus those who are unaware were investigated by Culnan (1995:12-15). She suggests that a consumer information problem exists in direct

marketing practices because the majority of her respondents believe that it is important to be able to remove their names from mailing lists if they choose. However, these repondents claim to be unaware of any name removal options. The results showed that consumers who were not aware of name removal procedures were less likely to have shopped by mail and were in the younger age category (18-29 years old). Follow-up analyses found that education was also a variable that discriminated between the two groups, with the less educated group being unaware of name removal procedures.

Based on the above findings and the secondary objectives to establish **differences between consumers in terms of their knowledge about information protection practices and their privacy concerns (SO5), the dependency between age and knowledge about information protection practices (SO6), and the dependency between level of education and knowledge about information protection practices (SO7),** the following null and alternative hypotheses were set:

H_0: There is no significant difference between consumers in terms of their level of awareness of name removal procedures and their privacy concerns.
H_{3a}: There is a significant difference between consumers in terms of their level of awareness of name removal procedures and their privacy concerns.

H_0: The level of awareness of name removal procedures is independent of age.
H_{3b}: There is a dependency between the level of awareness of name removal procedures and age.

H_0: The awareness of name removal procedures is independent of levels of education.
H_{3c}: There is a dependency between the awareness of name removal procedures and levels of education.

5.4.4 Hypothesis 4

As Internet usage increases due to the efficiencies of new technological developments and increased online commerce, the increased traffic of personal consumer information will allow marketers to gain greater expertise in the evaluation of consumer purchase behaviours. This may alter consumers' privacy and security perceptions that are likely to limit online retailing in the long-term (Miyazaki & Fernandez, 2001:38). The findings of a study by Hoffman *et al.* (1999:80) indicated that there was a lack of faith between most organisations and consumers on the Web. In essence, consumers simply do not trust most Web providers enough to engage in relationship exchanges with them involving their money and personal information. Research has also revealed that this lack of trust originated from the fact that consumers felt they lack control over the access that web merchants have to their personal information during the online navigation process, and that privacy concerns tended to influence buyer-seller relationships negatively (Prabhaker, 2000:161).

The IBM-Harris Multi-National Consumer Privacy Survey (Harris Interactive & Westin, 2000:10) examined different attitudes toward the privacy practices of Internet users and non-users. The survey explored whether familiarity with the Internet affects consumer confidence and concerns about privacy practices. The results suggested that Internet users tend to be more privacy conscious, leading to more privacy protective behaviours from them. The findings of a study by Miyazaki and Fernandez (2001:38) showed that higher levels of Internet experience may lead to lower risk perceptions regarding online shopping and fewer specific concerns regarding system security. However, more concerns were found regarding online privacy. The results suggested that increased Internet experience alone did not appear to diminish privacy concerns (Lebo, 2001:65). The UCLA Internet Reports indicated that the issue of privacy continued to be the greatest concern about the Internet among both users and non-users, and respondents expressed considerable concern that using the Internet created risks to individual privacy.

Since the above-mentioned findings indicated different associations with privacy concerns, one of the secondary objectives aimed **to establish differences between consumers in terms of their Internet usage and their privacy concerns (SO8).** From this the following null and alternative hypotheses were formulated:

H_0: There is no significant difference between Internet users and Internet non-users in terms of their privacy concerns.
H_4: There is a significant difference between Internet users and Internet non-users in terms of their privacy concerns.

5.4.5 Hypothesis 5

Consumers vary in their beliefs and perceptions regarding direct marketing. These perceptions can influence whether and to what extent consumers are concerned about privacy. Milne and Gordon (1994:52), for example, have found that although respondents had favourable attitudes toward direct mail, many desired lower mail volume and improved targeting and advertising mail. There is some evidence that direct marketing users differ from non-users in their personal information and privacy concerns. An analysis of the 1994 Harris-Equifax data (Phelps *et al.*, 2000:30), for example, indicated that people who had made a direct mail purchase in the preceding year were slightly more concerned about threats to their privacy; were more likely to have refused to provide an organisation with personal information; and were more likely to have privacy concerns when a profile of their viewing and buying patterns was developed. Some researchers have suggested that as individuals are exposed more to direct marketing efforts, their concerns about personal privacy may become better articulated and perhaps increase (Campbell, 1997:45). For example, Milne *et al.* (1996:25) found that in Argentina (a country where direct marketing is in its infancy), only a small percentage of consumers were concerned about information privacy. In markets relatively developed in direct marketing, as is the case in the USA, consumers have sufficient experience and knowledge of direct marketing practices to have specific concerns. There is evidence that attitudes toward direct marketing and consumer

privacy are shaped by the level of direct response activity of the individual (Milne *et al.*, 1996:24). One of the steps individuals can take as a result of privacy concerns is to restrict their purchases of goods through direct marketing (Campbell, 1997:47).

The South African direct marketing industry is not as developed as that in the USA. There are no published research findings on whether direct marketing experience and knowledge by consumers will increase privacy concerns among South Africans. This fact has inspired the objective **to establish the differences between consumers in terms of their direct purchasing behaviour and their privacy concerns (SO9).** The following null and alternative hypotheses were formulated to address this secondary objective:

H_0: There is no significant difference between direct shoppers and non-direct shoppers in terms of their privacy concerns.
H_5: There is a significant difference between direct shoppers and non-direct shoppers in terms of their privacy concerns.

5.4.6 Hypothesis 6

Alan Westin and Louis Harris & Associates created a Privacy Segmentation Index in 1995. This Index classified the American public to be divided into three privacy segments. The first segment was people with very high concern about privacy, labelled the 'Privacy Fundamentalists'. According to the latest results, this segment represents about 25 per cent of the American public (Harris Interactive, 2002b:20). This group regards privacy as something with an especially high value. They reject the claims of many organisations' need (or entitlement) to obtain personal information for their business or governmental programmes; they think more individuals should simply refuse to give out information they are asked for; and they favour the enactment of strong laws to secure privacy rights and control organisational discretion. The second group was labelled 'Privacy Pragmatists'. This segment currently represents about 55 per cent of the population. This group examines the relevance and social propriety of

the information sought; wants to know about the potential risks to breaches of their privacy and about the security of their information; is sensitive in observing whether fair information practices are being maintained widely enough; and then decides whether the segment will agree or disagree with specific information activities. The final group, the 'Privacy Unconcerned', represent about 20 per cent of the population. This group does not know what the 'privacy fuss' is all about. It supports the benefits of most organisational programmes over warnings about privacy abuse; has few problems with supplying personal information to government authorities or businesses; and sees no need for creating another government bureaucracy to protect someone's privacy.

The Privacy Segmentation Index was applied in this study with the objective **to classify South African consumers into different privacy sensitive segments based on their general privacy concerns (SO10).** The following null and alternative hypotheses were formulated to address this secondary objective:

H_0: The proportion of South African consumers is equally represented in the different privacy segments.
H_6: The proportion of South African consumers is not equally represented in the different privacy segments.

5.4.7 Hypotheses 7a to 7f

Given that privacy appears to have numerous dimensions and that different mechanisms are used to control privacy in different cultures, it seems reasonable to hypothesise that different types of people may vary in terms of how they view the construct of privacy (Petrison & Wang, 1995:21). Another secondary objective was therefore **to identify differences between consumers in terms of their demographic characteristics and their privacy concerns (SO11).** Six hypotheses were formulated to test for significant differences between the different demographic variables, as discussed below.

5.4.7.1 Hypothesis 7a

Numerous studies have found a strong relationship between age and privacy concerns. A study by Rainie (2002:20) indicated a strong link between age and Internet users' behaviour with regard to privacy. The findings of other studies have shown that younger adults (average ages 18-34) were less concerned about privacy than those aged above 50 years (Milne *et al.*, 1996:25; TNS Intersearch, 2001:44). This was supported by the findings of a study by Harris Interactive and Westin (2000:4), who reported that a significantly greater number of United States consumers aged below 30 held a positive view of personalised marketing than did consumers over 50 years. Similarly, younger consumers in the United Kingdom and Germany were more likely than consumers over 50 to report a positive view of personalised marketing. The findings of a study by Culnan (1995:14) illustrated that older consumers (aged above 50) were more aware of name removal procedures, leading to a reduced concern about privacy. Various studies have found that privacy concerns appear to increase with age (Nowak & Phelps, 1992:35; Campbell, 1997:51; Milne & Boza, 1999:15; Harris & Westin, 2000:8). American, British and German consumers over 50 were more likely to fall into the category of the 'very concerned' than consumers between 18 and 29 years of age (Harris Interactive & Westin, 2000:5). The findings of a recent study by Harris Interactive (2002b:33) were that older adults (aged above 50) were much more concerned about specific misuses of personal information than younger adults; they were more likely to feel that they have little control over how their personal information is used; but they were far more likely than younger adults to agree that most organisations handle their personal information properly and confidentially.

Louis Harris & Associates and Westin (1998b:43) also found that the older the respondents were, the more likely they were to characterise telemarketing calls as intrusive. Their results also showed that older consumers were more likely to opt out of receiving telemarketing calls, and were more likely to refuse to give information to an organisation because they argue that this kind of information is not really needed or is too personal (Louis Harris & Associates & Westin, 1998b:ix-xviii). Despite the fact that

Phelps *et al.* (2000:34) found no statistically significant relationship between age and privacy concerns, the majority of studies do show that privacy concerns increase with age.

Since no studies have been published on the relationship between age and privacy concerns in South Africa, the hypothesis tests the difference between age groups and their privacy concerns.

H_0: There is no significant difference between young and old people in terms of their privacy concerns.
H_{7a}: There is a significant difference between young and old people in terms of their privacy concerns.

5.4.7.2 Hypothesis 7b

Smith (2001:12) has found that a country's cultural values have a significant role in explaining the level of privacy concern in a country. In his study, higher levels of individualism, masculinity and power distance (USA) were associated with higher levels of privacy concern, but the relationship with uncertainty avoidance was the reverse (associated with the European approach). Second, he showed that there was a relationship between these cultural values and the regulatory approach embraced by a country. The findings of a study by Louis Harris & Associates and Westin (1998b:ix-xviii) illustrated that whites were more likely to consider telemarketing calls as intrusions than African-Americans or Hispanic Americans were. Also, whites were among those most likely to state that privacy policies for local telephone companies were absolutely essential. A comparative analysis between Japanese and United States consumers' attitudes toward privacy reported that privacy had different meanings depending on the culture (Maynard & Taylor, 1996:43). Since ethnic classification is a sensitive issue in South Africa, this study used home language as a variable instead of ethnic orientation.

The following null and alternative research hypotheses were formulated in the context of the findings from the studies cited above:

H_0: There is no significant difference between the main language groups in terms of their privacy concerns.
H_{7b}: There is a significant difference between the main language groups in terms of their privacy concerns.

5.4.7.3 Hypothesis 7c

The findings of a study by Nowak and Phelps (1992:35) indicated that concerns about threats to personal privacy did not vary across different levels of education. Most other empirical studies, however, reported a strong relationship between levels of education and privacy concerns. The findings of a study by Harris Interactive (2002b:43) showed that adults with lower educational levels were more concerned about the potential misuse of their personal information than adults with higher educational levels were. The study also noted that less educated adults were far less likely to be privacy assertive: instead, adults with higher educational levels were more active in protecting their privacy when interacting with organisations (Harris Interactive, 2002b:45). Milne *et al.* (1996:25) also reported that attitudes toward privacy differed significantly according to educational levels, but that the levels were not directly related to privacy concerns. Their findings showed that respondents with the lowest and the highest educational levels were the most concerned about privacy, with the middle group showing less concern. However, the majority of the studies done so far illustrate that more highly educated consumers had higher levels of privacy concern (Phelps *et al.*, 2000:34).

Several important privacy concerns were reported to be significantly different between more educated and less educated consumers. First, the results of a study by Culnan (1995:14) indicates that consumers who are aware of name removal procedures tend to be better educated than those who are not aware of name removal procedures. Second, Louis Harris & Associates and Westin (1998:xviii) reported that consumers with

higher levels of education were more likely than less educated consumers to request an organisation not to sell or give their name and address to another organisation. These consumers regarded privacy policies as absolutely essential. The findings of a study by Harris Interactive and Westin (2000:5,8) contended that more highly educated consumers were more likely than less educated consumers to report personal experiences of privacy invasion and were more inclined to limit the use of their personal information. A study among consumers in the USA, the United Kingdom and Germany indicated that as education levels increased, consumers in all three countries were more likely to refuse to give out personal information (Harris Interactive & Westin, 2000:7).

Given all the above-mentioned findings, and the fact that no relationships between educational levels and privacy concerns have been reported on in the South African situation, the following null and alternative hypotheses were formulated:

H_0: There is no significant difference between consumers in terms of their levels of education and their privacy concerns.
H_{7c}: There is a significant difference between consumers in terms of their levels of education and their privacy concerns.

5.4.7.4 Hypotheses 7d and 7e

Not many studies report on relationships between employment status and privacy concerns. One study by Phelps *et al.* (2000:34) indicated that there was no statistically significant relationship between employment status and privacy concerns. Several studies reported that income levels had no direct effect on consumer information privacy concerns (Milne *et al.*, 1996:25; Campbell, 1997:51; Phelps *et al.*, 2000:34). Another study reported that more affluent and established individuals may view the concept of privacy more seriously (Wang & Petrison, 1993:16). More specifically, the higher the household income the more likely it is that telemarketing calls will be characterised as intrusive. More affluent consumers were more likely to opt out of receiving telemarketing

calls, and were also more likely to refuse to give information to an organisation because they thought the information was not really needed or was too personal. Households with larger incomes were also more likely to have reported having asked an organisation not to sell or give their name and address to another organisation and more affluent consumers were among those who were most likely to argue that privacy policies are absolutely essential (Louis Harris & Associates & Westin, 1998b:x). More affluent consumers were also more likely than less affluent consumers to limit the use of their personal information (Harris Interactive & Westin, 2000:8). Some studies have, however, reported the opposite, where respondents with higher incomes were less concerned about privacy (Milne & Boza, 1999:18; TNS Intersearch, 2001:44). The findings of a study by Harris Interactive (2002b:43) showed that adults with a low income were more concerned about the potential misuse of their information than the affluent. Because of the conflicting results from studies in other countries, and the fact no relationships between employment status, income and privacy concerns are known in respect of South African consumers, the following null and alternative hypotheses were formulated:

H_0: There is no significant difference between consumers in terms of their employment status and their privacy concerns.
H_{7d}: There is a significant difference between consumers in terms of their employment status and their privacy concerns.

H_0: There is no significant difference between consumers in terms of their income levels and their privacy concerns.
H_{7e}: There is a significant difference between consumers in terms of their income levels and their privacy concerns.

5.4.7.5 Hypothesis 7f

Several studies maintain that gender is strongly associated with privacy concerns (Rainie, 2002:20), except for the findings of a study by Phelps *et al.* (2000:34) who

indicated no statistically significant relationship between gender and privacy concerns. Generally, females express more concern about threats to their personal privacy (Louis Harris & Associates & Westin, 1998b, xi; Sheehan, 1999:24-38). Females seem more concerned than males about unsolicited e-mail (Sheehan, 1999:24), about secondary usage of information (Sheehan, 1999:28); about the potential misuse of their personal information (Harris Interactive, 2002b:32); and about insecure transactions or situations where their personal information could be stolen (Harris Interactive, 2002b:32). Even in the online environment, females are more likely to express privacy concerns than males (TNS Intersearch, 2001:44). In general, when deciding if they want to do business with an organisation, females are more likely than males to take into consideration whether an organisation explains how it will use personal information and whether an audit report has been conducted that verifies the organisation's privacy practices (Harris Interactive, 2002b:93).

Since most studies report differences between gender groups and privacy concerns, the following null and alternative hypotheses were formulated:

H_0: There is no significant difference between males and females in terms of their privacy concerns.
H_{7f}: There is a significant difference between males and females in terms of their privacy concerns.

5.5 SUMMARY

This chapter has been intended to serve as a link between the three literature-specific chapters (Chapters 2, 3 and 4), and the empirical research chapters (Chapters 6 and 7). Chapter 5 provided a logical progression and cohesive framework between theory and research. The problem statement and objectives formulated in Chapter 1, together with the hypotheses formulated in this chapter, form the basis of the empirical study to follow. In terms of the progression of the study, the next chapter, Chapter 6 focuses on the research design and methodology.

CHAPTER 6
RESEARCH DESIGN AND METHODOLOGY

6.1 INTRODUCTION

Chapter 5 was devoted to a description of the problem statement and research hypotheses. This chapter presents the approach to the planned research process. The research methodology is discussed with special reference to the sample, data collection, questionnaire design and statistical procedures used. A detailed discussion on the construction of the questions for the measurement instrument is also presented.

6.2 DATA SOURCES

There are two types of data sources, namely primary and secondary data (Malhotra, 1996:116). Secondary data are data that have already been collected for purposes other than the problem at hand. Chapters 2 to 4 summarised the secondary data on information privacy found in a wide range of relevant scientific journals, research publications and media articles. Primary data is original data collected specifically for the purpose of the research in question (Cooper & Schindler, 2001:260). Chapters 6 to 8 focus on the collection and analysis of the primary data needed to address the lack of knowledge and understanding regarding information privacy concerns by South African consumers. The empirical investigation is of a quantitative nature. Quantitative research involves the collection of primary data from a large number of individuals, frequently with the intention of projecting the results to the larger population (Martins, Loubser & Van Wyk, 1996:125). Once the research problem has been defined and clearly specified, the research effort can turn to data collection, as is discussed in the next section.

6.3 DATA COLLECTION

There are various methods of collecting primary research data, for example, mail-based self-administered questionnaires, telephonic interviews, personal interviews (face-to-face) and focus groups. For the purposes of this study, data were gathered by means of telephonic interviews using a questionnaire as the measurement instrument. The telephone interviews involved phoning a sample of respondents and asking them a series of questions. The interviewer used a paper questionnaire and recorded the responses, in line with suggestions by Malhotra, 1996:198).

Telephonic interviews were chosen as the data collection method because the method offers the following advantages (Dillon, Madden & Firtle, 1993:173; Churchill & Iacobucci, 2002:282):

- The telephone can be used to complete large studies in a short time (two to three weeks) and is especially effective for national samples.
- A substantial amount of information can be collected within 15 to 30 minutes.
- Like face-to-face interviews, telephonic interviews offer very good sample control. Although non-listed households can be a problem, the desired respondents can be contacted with relative ease.
- Telephone interviewers can clear up any ambiguities, increasing the quality of the data.
- The telephone as a data collection medium offers a high response rate compared to mail.

It is important to note that in most studies, the realised sample can sometimes differ from the drawn sample, because certain types of errors can occur during data collection. One such source of bias is non-response error, which represents a failure to obtain information from some elements of the population that were selected and designated for the sample. The two main sources of non-response bias are 'not-at-homes' and refusals to answer (Churchill & Iacobucci, 2002:532). Replies may not be secured from some designated sampling units because the respondent is not at home

when the interviewer calls. In almost every study, some respondents refuse to participate. The rate of refusals depends, amongst other things, on the nature of the respondent, the circumstances surrounding the contact, the nature of the subject and the interviewer. Field errors can also arise after the individual has agreed to participate in the study. Instead of co-operating fully, the individual may refuse to answer particular questions or provide a response that differs somehow from what is actually true or correct.

Before the primary data can be collected, a sample needs to be drawn and a measurement instrument needs to be designed. The sampling procedure and the design of the questionnaire are discussed in the following sections.

6.4 SAMPLING

Sampling is one component of a research design. Churchill and Iacobucci (2002:449) have identified several basic steps to follow when drawing a sample from a population. Five of their steps are briefly described and discussed below as they apply to this study.

6.4.1 Define the target population

The first step is to define the target population, in other words, the totality of cases that conform to some designated specifications. The specifications define the elements that belong to the target group and those that are to be excluded. The target population selected for this study was all adults above the age of 18 years residing in South Africa who had a telephone number listed in a telephone directory. Since the size of the target population was large and the cost and time associated with obtaining information from the population is high, a sample was drawn. A sample is a selection of a subset of elements from a larger group of objects (Churchill & Iacobucci, 2002:981). The basic principle of sampling is that by selecting some of the elements in a population, a researcher may draw conclusions about the entire population (Malhotra, 1996:359).

6.4.2 Identify the sampling frame

The second step in the sample selection process is the identification of the sampling frame, which is the listing of the elements from which the actual sample will be drawn. The sampling frame for this study was all South African households with a listed telephone number, as contained in Telkom's electronic CyberTrade Telephone Directory Service. CyberTrade is an electronic telephone directory service that provides a basic electronic search facility to subscribers (Telkom, 2002). According to the latest statistics, the sampling frame represents 2.9 million households in South Africa. This is 30.4 per cent of the total number of households (9.5 million) with fixed telephone lines at home (SAARF, 2001). Even though the target population was all households with listed telephone numbers, the researcher had to take cognisance of the fact that the CyberTrade Telephone Directory Service does not provide a complete and accurate listing of all households. Reality dictates that there is seldom a perfect correspondence between the sampling frame and the target population of interest.

Certain errors can occur in the sampling frame. One such error is the possibility of a certain degree of non-coverage error, which occurs mainly because the telephone directories do not provide a complete sampling frame. Not every family has a phone, and not all people who have telephones have them listed in the directory. Furthermore, there is some variation between those who have and those who do not have telephones in terms of certain important demographic characteristics. Over-coverage error can also be a source of bias (Churchill & Iacobucci, 2002:527). It can arise because of duplication in the list of sampling units. Units with multiple entries in the sampling frame (for example, families with several phone listings) have a higher probability of being included in the sample than sampling units with one listing. For most surveys, however, non-coverage is much more common and troublesome.

6.4.3 Select a sampling procedure

The third step of selecting a sample procedure is linked to the identification of the sampling frame, because the choice of sampling method depends largely on what the researcher can develop as a sampling frame. Sampling techniques can be divided into two broad categories, namely probability and non-probability samples. Probability samples are distinguished by the fact that each population element has a known, non-zero chance of being included in the sample. Non-probability samples rely on personal judgment somewhere in the element-selection process and therefore prohibit estimating the probability that any given population element will be included in the sample (Churchill & Iacobucci, 2002:978). The sample for this study was drawn by means of systematic sampling. Systematic sampling has many desirable features because such a sample is relatively simple to draw, it is easy to check and it can be done at a moderate cost (Zikmund, 2000:363). With this method, the sample is chosen by selecting a random starting point and then selecting every *i*-th element in succession from the sampling frame (Malhotra, 1996:370). The sampling interval, *i*, is determined by dividing the population size *N* by the sample size *n* and rounding to the nearest integer. Table 6.1 sets out an outline of the procedure followed to determine the sampling interval for this study. Here the first number was chosen at random, after which the first number on every 11^{th} page in the electronic directory was chosen.

6.4.4 Determine the sample size

Sample size refers to the number of elements to be included in the study (Malhotra, 1996:363). Sample size can be determined through the use of statistical procedures or on the basis of managerial judgement. One judgemental factor involves the determination of sample size by selecting the appropriate item, question or characteristic for the sample size calculations. In most studies several characteristics are involved, and the desired degree of precision may vary for these items. The researcher must exercise judgement to determine which item will be utilised. Often the item that will produce the largest sample size is utilised to determine the ultimate

sample size (Zikmund, 2000:393). Given the fact that factor analysis and structural equation modeling were to be used in the data analyses in this study, the decision on sample size was very important. As a general rule for factor analysis, the sample size should be larger than 100, or have a minimum of at least five times as many observations as there are variables to be analysed. A more acceptable size would have a ten-to-one ratio, and some researchers even propose a minimum of 20 cases for each variable. The researcher should always try to obtain the highest cases-per-variable ratio to minimise the chances of 'over-fitting' the data (Hair, Anderson, Tatham, & Black, 1998:99).

In structural equation modeling, the researcher often requires a much larger sample size to maintain the accuracy of estimates and to ensure representativeness. The need for larger sample sizes is also part of the program requirements and the multiple observed indicator variables used to define latent variables. Many researchers use from 250 to 500 subjects, and the greater the sample size, the better (Schumacker & Lomax, 1996:20). Anderson and Gerbing (1988:416) argue that 150 subjects is sufficient to obtain a converged and proper solution for models with three or more indicators per factor, otherwise a sample size of at least 400 to 500 is needed. If the data violate the assumptions of multivariate normality, the ratio of respondents to parameters needs to increase with a generally accepted ratio of 15 respondents for each parameter (Hair *et al.*, 1998:605).

The above-mentioned guidelines suggest different sample sizes, depending on the number of variables or estimates of the study. Since a number of 45 variables were to be analysed in this study, the researcher decided to draw a random sample of 800 respondents from the sample frame for this study. This decision was based on the 1:15 ratio suggested by Hair *et al.* (1998:605), with a 'built-in' 20 per cent addition for anticipated 'missing responses' (see Section 6.6.1) that could reduce the dataset. Table 6.1 sets out how the sample of 800 was drawn from the sampling frame.

Table 6.1 Systematic sampling procedure

AREA	Total number of pages in directories (sample frame)	Number of pages selected from directory (sample drawn)
Boland and West Coast	482	43
Cape Peninsula	1223	111
Durban and surrounding area	782	71
East London and border	321	29
East Rand	684	62
Free State	478	43
Johannesburg	1008	91
KwaZulu-Natal North Coast	175	15
KwaZulu-Natal South Coast	87	8
Mpumalanga	387	35
North West Province	426	38
Northern Province	244	22
Northern Cape and Namaqualand	194	17
Port Elizabeth and Eastern Cape	496	45
Pietermaritzburg and KwaZulu-Natal	347	31
Pretoria and surrounding area	645	58
Southern Cape and Karoo	212	19
Vaal Triangle	208	18
West Rand	494	44
TOTAL	**8893**	**800**

Source: Adapted from http://cybertel.cybertrade.co.za

6.4.5 Select the sample elements

A sample element is the unit about which information is needed, usually the respondent (Martins *et al.*, 1996:251). A sampling unit is an element, or a unit containing the element, that is available for selection at some stage of the sampling process (Malhotra, 1996:361). In this study, the sampling units were the different households chosen to be

interviewed, and the sample elements were the household family members with the following characteristics (elements):

(a) individuals aged 18 years or older;

(b) individuals who can understand Afrikaans or English; and

(c) individuals who had most recently celebrated their birthdays.

From the above-mentioned guidelines, it is clear that this study selected individuals in the households using age and the standard 'last birthday' technique as qualifying criteria.

Once the sample was determined, the researcher could focus on the development of the measurement instrument. The next section focuses on the phase of the research design where the questionnaire was designed and pre-tested.

6.5 QUESTIONNAIRE DEVELOPMENT

This section reviews the procedures followed to develop the questionnaire. Attention is paid to the measurement and scaling procedures, the actual questionnaire design, the pre-testing, as well as the coding and editing of the questionnaire.

6.5.1 Level of measurement

Measurement in research consists of assigning numbers to empirical events in compliance with a set of rules. In other words, certain characteristics are measured such as perceptions, attitudes or preferences, instead of the consumer as an object. The levels of measurement reflect the correspondence of numbers assigned to the characteristics in question and the meaningfulness of performing mathematical operations on the numbers assigned. There are four primary scales of measurement, namely nominal, ordinal, interval and ratio (Malhotra, 1996:271-275).

- A **nominal scale** is a figurative labelling scheme in which the numbers serve only as labels or tags for identifying and classifying objects, such as classifying the respondent as a male or female.
- An **ordinal scale** is a ranking scale in which numbers are assigned to objects to indicate the relative extent to which the objects possess certain characteristics.
- In an **interval scale**, numerically equal distances on the scale represent equal values in the characteristic being measured.
- A **ratio scale** possesses all the properties of the nominal, ordinal and interval scales and, in addition, an absolute zero point.

This study used of nominal and interval scales. The nominal scales served to identify and classify respondents, whereas the interval scales represented the values of the attitudes being measured. Scaling is considered an extension of measurement and is discussed below.

6.5.2 Scaling techniques

Scaling involves creating a continuum upon which measured objects are located. The scaling techniques commonly employed in marketing research can be classified into comparative and non-comparative scales (Malhotra, 1996:276).

- **Comparative scales** involve the direct comparison of stimulus objects. Comparative scale data must be interpreted in relative terms and have only ordinal or rank order properties. Several comparative scaling techniques are available, such as paired comparisons scales, geared paired comparisons, rank-order scales, constant sum scales and continuous rating comparative scales.
- In **non-comparative scales**, also referred to as metric scales, each object is scaled independently of the others in the stimulus set. Here the resulting data are generally assumed to be interval- or ratio-scaled. Non-comparative scales are composed of continuous and itemised rating scales. In a continuous rating scale, respondents rate the objects by placing a mark at the appropriate position on a line that runs from one extreme of the criterion variable to the other. In itemised rating scales, respondents

are provided with a scale that has a number of brief descriptions associated with each category. The Likert scale, semantic differential scale and Stapel scales are commonly used itemised scales.

The scaling technique employed in this study was the Likert scale. As a general rule, researchers should use the scaling technique that will yield the highest level of information feasible in a given situation and permit using the greatest variety of statistical analyses. Likert scales are mainly used to measure attitudes, and since this study aimed to measure the attitudes of consumers regarding information privacy, the main part of the questionnaire consisted of Likert scales. The Likert scale is a widely used rating scale that requires the respondents to indicate a degree of agreement or disagreement with each of a series of statements about the stimulus objects (Malhotra, 1996:292). Each scale item has five response categories, ranging from 'strongly disagree' to 'strongly agree'. Each response is given a numerical score to reflect its degree of attitude favourableness, and the scores may be totalled to measure the respondent's attitude. The Likert scale was used here because it has several advantages. Likert scales help researchers to compare one respondent's scores with the distribution of scores from a well-defined group, it is easy to construct and administer, and respondents readily understand how to use the scale, making it suitable for telephone interviews (Cooper & Schindler, 2001:234). The main disadvantage of the Likert scale is that it takes long to complete because respondents have to read each statement or, in the case of telephonic interviews, the interviewer has to read each statement to the respondent.

The measurement levels and scaling techniques discussed above were considered during the process of questionnaire design and had an impact on the question structure and wording.

6.5.3 Questionnaire design

Questionnaire design consists of several stages of development. Some of the main stages are discussed below.

6.5.3.1 Objectives of the questionnaire

A questionnaire is a formalised set of questions for obtaining information from respondents. A questionnaire has several objectives (Malhotra, 1996:319; Zikmund, 2000:310). First, it must translate the information needed into a set of specific questions that the respondents can and will answer. Second, the questionnaire has to motivate the respondent to co-operate and complete the interview. Third, the questionnaire should minimise response errors such as inaccurate answers. Finally, the questionnaire should collect only relevant information needed to solve the problem. Special attention was paid to the afore-mentioned objectives when the questions for the questionnaire were developed.

6.5.3.2 Interview method and question content

After specifying the basic information that is required, the researcher needs to specify how it will be obtained. As has been mentioned earlier, data was collected by means of telephonic interviews where respondents interacted with the interviewer, but did not see the questionnaire. This limited the type of questions that could be asked to short and simple ones. Telephonic interviews were chosen as the data collection method because this method provides a high response rate, is ideal for completing large studies, and was manageable for the researcher in terms of a limited time-frame.

The researcher's objectives and the chosen interview method had an impact on the questions formulated. When deciding on the question content, a researcher should consider the following (Cooper & Schindler, 2001:337):

- Should this question be asked?

- Is the question of proper scope and coverage?
- Can the respondents answer this question adequately, as asked?
- Will the respondents willingly answer this question, as asked?

Careful attention was paid to these questions, ensuring that the objectives would be met using the telephonic interviews.

6.5.3.3 Question structure

The structure of a questionnaire is an important consideration in questionnaire design. A questionnaire can be structured into administrative questions, classification questions and target questions (Cooper & Schindler, 2001:333).

- **Administrative questions** identify the respondent, interviewer and conditions. These questions are rarely asked of the respondent but are necessary to study patterns within the data and to identify possible error sources. The questionnaire used in this study allowed for identification of the respondent using a respondent code, the name of the interviewer, the telephone area-code, as well as qualification criteria such as identifying the person in the household who had most recently celebrated a birthday.
- **Classification questions** are usually socio-demographic variables that allow respondents' answers to be grouped so that patterns are revealed and can be classified. This questionnaire contained questions relating to variables such as age, home language, education, employment, income and gender.
- **Target questions** address the investigative questions of a specific study. Target questions may be structured (known as closed questions) or unstructured (known as open-ended questions). With open-ended questions, respondents are free to reply in their own words rather than being limited to choosing from a set of alternatives (Churchill & Iacobucci, 2002:328). A closed question can be dichotomous or multiple-choice (Malhotra, 1996:330). A dichotomous question has only two response alternatives, such as yes or no. A multiple-choice question requires

respondents to choose the alternative that most closely corresponds to their position on the subject, for example, marking the age category that applies to the respondent. This study did not use any open-ended questions. Dichotomous, multiple-choice and scale questions were formulated in the questionnaire.

6.5.3.4 Question wording

Question wording is the translation of the desired question content and structure into words that respondents can clearly and easily understand. Ordinary words should be used in a questionnaire, and they should match the vocabulary level of the respondents. Many questions, particularly those measuring attitudes and lifestyles, are worded as statements to which respondents indicate their degree of agreement or disagreement. Evidence indicates that the response obtained is influenced by the directionality of the statements: whether they are stated positively or negatively. In these cases, it is usually better to use dual statements, some of which are positive and others negative (Malhotra, 1996:335). The attitude statements formulated for this study used dual statements, with 32 statements reflecting a positive attitude and sixteen statements reflecting a negative attitude. Careful attention was also given to the wording of the questions for this study. Several 'marketing-related' terms were changed into everyday terminology to match the vocabulary level of the respondents. The questions were also formulated in a 'conversational' manner, since the data was to be collected by means of telephonic interviews.

6.5.3.5 Question sequence

Once the structure and wording of questions have been addressed, a researcher can construct the questionnaire. The introduction to the research needs to convince respondents about the importance of the research and the value of their participation. A typical questionnaire contains two types of information, namely basic information and classification information (Churchill & Iacobucci, 2002:345). Basic information refers to the subject of the study, whereas classification information refers to the other data that

are collected to classify respondents in order to extract more information about the phenomenon of interest. The proper questionnaire sequence is to present questions securing basic information first and those seeking classification information last. Since the basic information is the most critical, the researcher should not risk alienating the respondent by asking a number of personal questions before getting to the heart of the study. Questions should also be asked in a logical order. All questions that deal with a particular topic should be completed before beginning a new topic (Malhotra, 1996:337).

6.5.4 Constructing the questionnaire

The survey included 66 questions, some of which inquired about general demographic information, and others about consumers' beliefs, attitudes and behaviour regarding information privacy. All the questions were formulated based on the theoretical discussion on consumer privacy. Information needed to address the problem, research objectives and hypotheses were integrated into the question bank. The questionnaire (see the example in Appendix 1) was divided into five sections:

- Section 1: Qualification and introduction
- Section 2: 45-item Likert scale measurements containing belief, attitude and behaviour intention statements relating to privacy concerns
- Section 3: Privacy Segmentation Index measurement
- Section 4: Behaviour, experience and knowledge measurement
- Section 5: Classification questions

In the next section there is a discussion of the above-mentioned sections in the questionnaire.

6.5.4.1 Section 1: Qualification and introduction

The questionnaire was compiled using the guidelines discussed above. The first page of the questionnaire indicated the procedure for the interviewer. The procedure guided the interviewer through the initial process of introduction and qualification. Thereafter, a

background on the study was provided and certain important information such as the confidentiality of the answers was emphasised. Finally, the respondent was prepared for the first set of questions, by explaining the question formats and procedure to be followed.

The next section focuses on the different questions in the questionnaire.

6.5.4.2 Section 2: 45-item Likert scale measurement

The second section of the questionnaire (Questions 1-45) contained the main constructs or dimensions designed to measure information privacy concerns. As was mentioned in Chapter 5, eight main dimensions had been identified and were measured using a 45-item instrument using 5-point Likert scales. The following questions were formulated to address the issue.

(a) Questions 1 and 2

The first two questions in the questionnaire were adapted from a study by Phelps *et al.* (2000). The purpose of the questions was to measure consumers' concerns regarding **data collection**. The items specifically addressed the issue of collecting an excessive amount of personal information, and were structured to represent a **belief** and an **attitude** of a consumer.

(b) Questions 3 and 4

Questions 3 and 4 were adapted from a field experiment by Stone *et al.* (1983). The purpose of these questions was to address consumers' concerns regarding the practice of **data collection** without prior permission from the consumers. Question 3 was worded to represent a **belief** statement, and Question 4 to represent an **attitude** statement.

(c) Questions 5 and 6

Questions 5 and 6 aimed to determine how consumers would feel if organisations **collected** their personal information in return for certain benefits. Question 5 was formulated to represent the consumer's general **belief** regarding the issue, and Question 6 to represent the consumer's own **attitude** to the situation. These questions were adapted from a Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b).

(d) Questions 7 and 8

Questions 7 and 8 were adapted from the Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b). The purpose of these questions was to measure consumers' concerns regarding **data storage**. Specifically consumers' **beliefs** and **attitudes** pertaining to the access they have to their personal information while in the possession of organisations were measured.

(e) Questions 9 and 10

Questions 9 and 10 were adapted from a similar question constructed by Campbell (1997). These questions were designed to measure consumers' concerns regarding the accuracy of their information while it is contained **(stored)** in organisations' records. The two questions were formulated to represent the issue from a **belief** as well as from an individual **attitude** perspective.

(f) Questions 11 and 12

The next two questions were formulated to address consumers' concerns regarding **data security**. The items were adapted from two previous studies by Harris Interactive (2000; 2002b) on consumer information privacy. The questions were specifically designed to determine consumers' **beliefs** and **attitudes** regarding the safety of their personal information while it is stored on organisations' databases.

(g) Questions 13 and 14

Questions 13 and 14 were constructed with the purpose of measuring consumers' **beliefs** and **attitudes** regarding the control they have over the ways organisations **use** their personal information. These questions were adapted from previous studies by Stone *et al.* (1983) and Phelps *et al.* (2000).

(h) Questions 15 and 16

The objective of the next two questions was to address consumers' concerns over organisations' **use** of information for other purposes than those provided when the information was collected. The questions were adapted from several previous studies (Culnan, 1993; Campbell, 1997; Harris Interactive, 2002b) and were formulated to represent consumers' **beliefs** and **attitudes** regarding the purpose of information use.

(i) Questions 17 and 18

Questions 17 and 18 were adapted from the IBM-Harris Multi-National Consumer Privacy survey (Harris Interactive & Westin, 2000). The questions were designed to measure consumers' concerns regarding the possible **misuse** of their information by organisations. Question 17 was formulated to measure consumers' **beliefs** regarding misuse and Question 18 to measure consumers' personal **attitudes** toward misuse.

(j) Questions 19 and 20

These two questions were formulated to address the issue of **data disclosure**. Question 19 aimed to measure consumers' **beliefs** regarding the practice of information-sharing with other organisations without the permission of the consumer to whom the information belongs. The purpose of Question 20 was to measure consumers' **attitudes** regarding the same practice. This concept has been addressed in several previous studies on consumer information privacy concerns and was adapted from previous studies by Nowak and Phelps (1992), Culnan (1993), Taylor *et al.*, (1995) and Campbell (1997).

(k) Questions 21 and 22

Questions 21 and 22 addressed a similar issue as Questions 19 and 20 did **(data disclosure)**. Questions 21 and 22 differed from Questions 19 and 20 in that consumers' **beliefs** and **attitudes** were measured when they receive benefits in return for the sharing of their information with other organisations. The questions were adapted from the Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b).

(l) Questions 23 and 24

A third set of questions addressed **data disclosure** as an issue of concern to consumers. In Questions 23 and 24, consumers were asked whether they **believed** that name removal opportunities existed and whether they were concerned when they were not offered an opportunity to remove their information from records shared with other organisations **(attitude)**. These questions were also adapted from the Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b).

(m) Questions 25 and 26

The purpose of Questions 25 and 26 was to determine consumers' concerns regarding **solicitation**. The questions were adapted from a study by Culnan (1993) and aimed to measure consumers' **beliefs** and **attitudes** about receiving unrequested advertising material that is of no interest to them.

(n) Questions 27 and 28

Questions 27 and 28 were adapted from several previous studies (Vidmar & Flaherty, 1985; Nowak & Phelps, 1992; Louis Harris & Associates & Westin, 1998b). These studies' aim was to measure consumers' **beliefs** and **attitudes** regarding telemarketing **(solicitation)**. Since this has proved to be a medium that is very intrusive to consumers, they were questioned about whether they were interested in receiving such telephone calls.

(o) Questions 29 and 30

Questions 29 and 30 contained the final **belief** and **attitude** statements of the questionnaire. These questions were formulated to measure consumers' reaction when they receive information **(solicitation)** from organisations they have not done business with before. These questions were adapted from a study by Sheehan (1999).

(p) Questions 31, 34, 37, 40 and 43

Five questions were formulated to measure consumers' **expectations regarding government or legislative protection** during stages of **data collection, data security, data use, data disclosure and solicitation**. Question 31 measured respondents' expectations regarding data disclosure, and the question was adapted from previous ones used in several studies (Nowak & Phelps, 1992; Culnan, 1993; Taylor *et al.*, 1995; Campbell, 1997). The purpose of Question 34 was to measure consumers' expectations as to whether government should restrict organisations only to collect the information needed for a specific transaction. This question was adapted from studies by Nowak and Phelps (1992) and Taylor *et al.* (1995). The objective of Question 37 was to establish whether consumers expected government to do more to protect the safety of personal information. The question was adapted from two previous studies by Harris Interactive (2000; 2002b) on consumer information privacy. Question 40 was constructed to gauge consumers' concerns regarding data use and their expectation that government should limit those uses. The question was adapted from a study by Stone *et al.* (1983). The final question measured consumers' expectations regarding government protection (Question 43). This question was adapted from a study by Culnan (1995) and questioned consumers on possible limitations on unrequested advertising material.

(q) Questions 32, 35, 38, 41 and 44

Consumers' **behavioural intentions regarding data collection, data security, data use, data disclosure and solicitation** were measured by means of five questions. The first question (Question 32) was adapted from the IBM-Harris Multi-National Consumer Privacy survey (Harris Interactive & Westin, 2000) and determined consumers'

intentions to request an organisation to remove their personal information if they suspected it was being misused. Question 35 was formulated to measure consumers' intentions to support initiatives that would enable them to stop unrequested advertising material. The question was adapted from a study by Sheehan (1999). The purpose of Question 38 was to measure consumers' intentions to remove their information from organisations' records if the organisation sold the information to others. The question was adapted from the Privacy On and Off the Internet survey by Harris Interactive (2002b). Question 41 was constructed to establish the expectations of consumers regarding their support of an organisation's efforts to ensure that their personal information is kept safely. The question was adapted from a study by Harris Interactive (2002a) measuring Americans' fear on the Internet. Question 44 measured the behavioural intentions of consumers when organisations cannot provide reasons for why they want to collect personal information, and was adapted from studies by Culnan (1993) and Campbell (1997).

(r) Questions 33, 36, 39, 42 and 45

The final set of questions to be discussed as part of the 45-item instrument is Questions 33, 36, 39, 42 and 45. All these questions related to consumers' **expectations regarding privacy protection policies** of organisations during stages of **data collection, data security, data use, data disclosure and solicitation**. Question 33 measured consumers' expectations regarding the provision that privacy policies make for unrequested advertising material. The purpose of Question 36 was to establish consumers' expectations of the extent to which privacy policies should indicate their data disclosure practices. Question 39 was formulated to determine consumers' expectations regarding the protection of privacy policies during data collection. Questions 33, 36 and 39 were all adapted from the Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b). The purpose of Question 42 was to measure whether consumers expected organisations to use independent auditing firms to verify their privacy policies. Question 45 was included to gauge consumers' expectations regarding protection of their personal information while

it was in the possession of organisations. Both Questions 42 and 45 were adapted from the Privacy On and Off the Internet by Harris Interactive (2002b).

6.5.4.3 Section 3: Privacy Segmentation Index (Questions 46, 47 and 48)

Alan Westin and Louis Harris & Associates created a Privacy Segmentation Index in 1995 (Harris Interactive, 2002b:20). The third section in the questionnaire contained the three questions from the Privacy Segmentation Index. This index was in the format of 4-point Likert scales ranging from 'strongly disagree' to 'strongly agree'. Respondents who strongly agreed or slightly agreed with the statement Question 46, and strongly disagreed or slightly disagreed with the statements in Questions 47 and 48, were grouped into one segment. Respondents who strongly disagreed or slightly disagreed with the statement in Question 46, and strongly agreed or slightly agreed with the statements in Questions 47 and 48 were grouped into the second segment. All the remaining options formed the third segment.

6.5.4.4 Section 4: Behaviour, experience and knowledge measurement (Questions 49 to 60)

Section Four of the questionnaire contained dichotomous questions asking consumers certain questions to which they had to answer 'yes' or 'no'. Questions 49 to 60 measured consumers' actual protective behaviours, experiences of privacy invasion, knowledge of specific data practices, as well as Internet and direct marketing behaviours. Questions 49 to 53 were constructed to measure consumers' behaviour to protect their personal information during the stages of data collection, data security, data use, data disclosure and solicitation. These questions were adapted from several previous studies that measured concerned consumers' behaviour (Campbell, 1997; Sheehan, 1999; Harris Interactive & Westin, 2000; Harris Interactive, 2002b). Question 54 determined how many consumers had personally been a victim of privacy invasion. This question was addressed in various previous studies (Culnan, 1995; Campbell, 1997; Harris Interactive & Westin, 2000; Louis Harris & Associates & Westin, 1998b).

The purpose of Question 55 was to establish whether consumers were aware of any options to remove their names from records of organisations. This item was adapted from studies by Culnan (1993), and Milne and Boza (1999). Questions 56 and 57 were uniquely formulated for this study and the objective was to determine how many consumers had purchased via the Internet or had made use of Internet banking services. The last three questions of Section Four (Questions 58 to 60) were formulated to measure consumers' involvement with direct marketing, and were adapted from the Privacy Concerns and Consumer Choice survey by Louis Harris & Associates and Westin (1998b) for this study.

6.5.4.5 Section 5: Classification questions (Questions 61 to 67)

Section Five was the last section of the questionnaire and contained classification questions. The following socio-demographic characteristics were measured in Questions 61 to 67: age, home language, level of education, employment status, monthly income, gender and ethnic orientation. These questions were used to identify significant differences between respondents' socio-demographic characteristics and their privacy concerns.

The above section discussed the design of the questionnaire and the construction of specific questions. To place the different questions and its purpose into perspective, Table 6.2 provides an overview of the secondary objectives and hypotheses, and how they relate to the different questions in the measurement instrument. Table 6.2 serves to link the questions in the questionnaire with the secondary research objectives and research hypotheses (as discussed in Chapter 5, Sections 5.3 and 5.4).

Table 6.2 Summary of objectives, hypotheses and questions

Questions linked to secondary objectives and hypotheses		
	Objectives	**Questions**
(SO2)	To establish differences between consumers' manifest behaviours to protect their privacy and their privacy concerns. *H_1: There is a significant difference between consumers in terms of their protective behaviour and their privacy concerns.*	1-45 & 49-53
(SO3)	To establish differences between consumers in terms of their personal experiences of invasions of privacy and their privacy concerns. *H_{2a}: There is a significant difference between consumers who have been victims of invasions of privacy and consumers who have not been victims of invasions of privacy in terms of their privacy concerns.*	1-45 & 54
(SO4)	To establish the dependency between gender and personal experiences of invasions of privacy. *H_{2b}: There is a dependency between being a victim of invasion of privacy and gender.*	54 & 66
(SO5)	To establish differences between consumers in terms of their knowledge about information protection practices and their privacy concerns. *H_{3a}: There is a significant difference between consumers in terms of their level of awareness of name removal procedures and their privacy concerns.*	1-45 & 55
(SO6)	To establish the dependency between age and knowledge about information protection practices. *H_{3b}: There is a dependency between the level of awareness of name removal procedures and age.*	55 & 61
(SO7)	To establish the dependency between level of education and knowledge about information protection practices. *H_{3c}: There is a dependency between the awareness of name removal procedures and levels of education.*	55 & 63
(SO8)	To establish differences between consumers in terms of their Internet usage and their privacy concerns. *H_4: There is a significant difference between Internet users and Internet non-users in terms of their privacy concerns.*	1-45 & 56-57

	Objectives	Questions
(SO9)	To establish differences between consumers in terms of their direct purchasing behaviour and their privacy concerns. *H_5: There is a significant difference between direct shoppers and non-direct shoppers in terms of their privacy concerns.*	1-45 & 58-60
(SO10)	To classify consumers into different privacy sensitive segments based on their general privacy concerns. *H_6: The proportion of South African consumers is not equally represented in the different privacy segments.*	46-48
(SO11)	To identify differences between consumers in terms of their demographic characteristics and their privacy concerns. *H_{7a}: There is a significant difference between young and old people in terms of their privacy concerns.* *H_{7b}: There is a significant difference between the main language groups in terms of their privacy concerns.* *H_{7c}: There is a significant difference between consumers in terms of their levels of education and their privacy concerns.* *H_{7d}: There is a significant difference between consumers in terms of their employment status and their privacy concerns.* *H_{7e}: There is a significant difference between consumers in terms of their income levels and their privacy concerns.* *H_{7f}: There is a significant difference between males and females in terms of their privacy concerns.*	1-45 & 61, 62, 63, 64, 65, 66, 67

6.5.5 Pre-testing the questionnaire

The acid test of a questionnaire is how it performs under real conditions of data collection. For this assessment, the questionnaire pre-test is vital (Churchill & Iacobucci, 2002:351). The pre-test can be used to assess both individual questions and their sequence. An important purpose of pre-testing is to discover the respondents' reactions to questions. Pre-testing should help to discover where repetitiveness or redundancy occurs and is bothersome. In telephonic interviews the sound of the question and its transition must be fluid as well. Most draft questionnaires or interview schedules suffer from lengthiness. By timing each question and section, the researcher is in a better

position to make decisions about modifying or cutting material. Given the fact that the data for this study was to be collected by means of telephonic interviews, consideration was given to the length of the questionnaire, since telephone interviews are labour intensive and an accurate estimate of elapsed time had to be made. A lengthy telephone questionnaire could also contribute to fatigue or boredom by the respondents. The purpose of the pre-testing was thus twofold: first to test the questionnaire, and second to determine the interview time.

The questionnaire was refined after conducting a pilot test across a sample of 20 respondents, drawn from the identified sampling frame. The length of the interview proved to be between 15 minutes and 25 minutes, depending on the respondent. Interviewers alerted respondents to their involvement in a preliminary test of the questionnaire, enlisting the respondents as collaborators in the refinement process. According to Cooper and Schindler (2001:361), detailed probing of the parts of the questionnaire, including phrases and words, is appropriate under pre-testing conditions.

The pre-testing resulted in the following:

- The Likert scale-typed questions were initially worded in a first-person statement format. An example is: 'I do not mind to provide a lot of personal information if I think it is necessary.' Some respondents indicated that they were uncertain to whom the 'I' referred to in these statements. Did the 'I' refer to themselves, or to the interviewer? It was decided to change all the 'I' statements, to 'you' statements. For example: 'You do not mind to provide a lot of personal information if you think it is necessary.' Given the conversational nature of telephone interviews, formulating the statement as a 'you' statement would seem to be clearer to the respondent at the other end.
- Several respondents indicated that there seemed to be repetition in the questions. When measuring attitudes, researchers often ask several similar (but not the same) questions for the purpose of reliability. As a result of these comments, a decision was made to group similar questions together. Grouping questions that dealt with similar topics together eliminated the sense of repetition and seemed to create a more logical sequence for the respondents.

- Overall, the survey questions proved to be understandable and meaningful to the target population.

An example of the questionnaire used for pre-testing is appended in Appendix 2.

6.5.6 Coding and editing

Coding means assigning a code, usually a number, to each possible response to each question. The code includes the indication of the column position and the data record it will occupy. For example, the gender of respondents can be coded as 1 for females, and 2 for males (Malhotra, 1996:475). Assigning numerical symbols permits the transfer of data from the survey to the computer (Zikmund, 2000:421). Since the questionnaire contained only structured questions, it was pre-coded. This means that codes were assigned before the fieldwork was conducted. The respondent code and the record number also appeared on each record in the data.

Editing is the review of questionnaires with the objective of increasing accuracy and precision. It consists of screening questionnaires to identify illegible, incomplete, inconsistent or ambiguous responses. Treatment of unsatisfactory responses is commonly handled by returning to the field to get better data, assigning missing values and discarding unsatisfactory respondents (Malhotra, 1996:473). Questionnaires with unsatisfactory responses may be returned to the field, where the interviewers contact the respondents again. If returning the questionnaires to the field is not feasible, the researcher may assign missing values to unsatisfactory responses. Another approach is to discard the unsatisfactory responses. The treatment of unsatisfactory responses is addressed from a statistical perspective in the next section.

6.6 STATISTICAL PROCEDURES USED

Data was captured on a database and stored in ASCII-format. The data was also subjected to a verification process in order to eliminate non-response and data

capturing mistakes. The ASCII-file was prepared for data processing using the SAS computer statistical software package.

6.6.1 Data cleaning

A researcher may be confronted with various missing responses that need to be addressed before data analysis can commence. Missing responses represent values of a variable that are unknown: either because respondents provided ambiguous answers; or because their answers were not properly recorded (Malhotra, 1996:481). There are various approaches to deal with missing responses by either preserving missing or blank spaces, or by assigning values to missing data.

- **Casewise deletion** is one method of treating missing responses. Here the respondent (case) is removed if any of the answers are identified as missing. If 75 per cent or more of a questionnaire is not completed, a researcher employs casewise deletion (Dillon *et al.*, 1993:349).
- **Pairwise deletion** is a method of handling missing values in which all cases or respondents with any missing values are not automatically discarded, but only the respondents with complete responses are considered (Malhotra, 1996:482).
- A **mean response** is an approach that involves replacing the missing response with a constant mean, median or mode response of all the other respondents to the question (Dillon *et al.*, 1993:372).
- An **imputed response** is an approach where the respondent's answer to other questions is used to impute or deduce an appropriate response to the missing question. This can be done statistically by determining the relationship of the variable in question to other variables based on the available data (Malhotra, 1996:482).

The researcher can decide to use casewise deletion, pairwise deletion or mean response, depending on the statistical technique used and the extent of the missing data.

6.6.2 Descriptive statistics

Descriptive analysis refers to the transformation of the raw data into a form that is easy to understand and interpret (Zikmund, 2000:437). Describing responses or observations is typically the first form of analysis. The calculation of averages, frequency distributions, and percentage distributions is the most common form of summarising data. The following are the main statistical procedures that were considered for use in the data analysis.

6.6.2.1 Frequency distributions

In a frequency distribution, one variable is considered at a time. The objective is to obtain a count of the number of responses associated with different values of the variable. A frequency distribution for a variable produces a table of frequency counts, percentages and cumulative percentages for all the values associated with that variable. It also indicates the shape of the empirical distribution of the variable and can be used to construct histograms (Malhotra, 1996:504). The most commonly used statistics associated with frequencies are the mean, mode, median and standard deviation.

(a) The mean

The mean is the arithmetic average of a variable (Sudman & Blair, 1998:456) and a measure of central tendency for interval- and ratio-scaled data (Dillon *et al.*, 1993:374). The researchers can make use of mean values on the Likert scaled questions in order to determine the mean scores for the total sample and to make comparisons between different demographic characteristics.

(b) The variance and standard deviation

The variance is the average squared distance between the values of individual observations and some variable and the mean of that variable (Sudman & Blair, 1998:459). The standard deviation is the positive square root of the variance (Malhotra,

1996:508). Variances and standard deviations can be used to determine whether mean differences between groups can be regarded as significantly different or not.

6.6.2.2 Cross-tabulation

Analysing results by groups, categories, or classes is known as the technique of cross-tabulation (Zikmund, 2000:439). The purpose of cross-tabulation is to allow the inspection of differences between groups and to make comparisons. Cross-tabulation was used by in this study to allow for a determination of relationships or associations between variables.

6.6.3 Multivariate statistics

Multivariate statistical methods allow the effects of more than one variable to be considered at one time (Zikmund, 2000:533). Multivariate techniques can be classified into two groups, namely dependence and interdependence techniques. Typical dependence techniques include multiple regression analysis, multiple discriminant analysis, multivariate analysis of variance and canonical correlation analysis. These are techniques where criterion or dependent variables and predictor or independent variables are present. Interdependence techniques include factor analysis, cluster analysis, and multidimensional scaling. These are techniques in which the whole set of interdependent relationships is examined (Malhotra, 1996:645).

Factor analysis as an interdependent multivariate technique was used as a data analysis procedure in this study. Factor analysis is a general term for several specific computational techniques. The objective of this technique is to reduce the variables to a manageable number that belong together and have overlapping measurement characteristics (Cooper & Schindler, 2001:591). Mathematically, factor analysis is somewhat similar to multiple regression in that each variable is expressed as a linear combination of underlying factors. The general purpose of factor analysis is to summarise the information contained in a large number of variables into a smaller

number of factors (Zikmund, 2000:544). The following steps were followed to conduct the factor analysis (Malhotra, 1996:648):

- Specify the variables to be included in the factor analysis.
- Construct the correlation matrix.
- Choose the method of factor analysis.
- Determine the number of factors.
- Rotate the factors.
- Interpret the factors.
- Calculate the factor scores.
- Determine the model fit.

One of the research objectives (as identified in Chapter 1) was to measure South African consumers' beliefs, attitudes, behavioural intentions and expectations toward data collection, data storage, data use, data disclosure and solicitation. The purpose for the factor analysis in this study was to uncover the underlying dimensions of consumers' information privacy concerns.

6.6.4 Hypotheses testing

In statistical theory, a hypothesis is an unproven proposition or supposition that tentatively explains certain facts or phenomena. A hypothesis is a statement, an assumption, about the nature of the world (Zikmund, 2000:459). A null hypothesis is a statement about a *status quo*. An alternative hypothesis states that there are differences and it is the opposite of the null hypothesis. The purpose of hypothesis testing is to determine whether the null hypothesis can be rejected, which in turn provides support for the alternative hypothesis. Whenever inferences are drawn about a population, there is a risk that an incorrect conclusion may be reached. Two types of errors can occur (Malhotra, 1996:512). A Type I error occurs when the sample results lead to the rejection of the null hypothesis when it is in fact true. A Type II error occurs when, based on the sample results, the null hypothesis is not rejected when it is in fact false.

Several hypotheses have been identified in Chapter 5 and were tested following the steps below (Malhotra, 1996:511; Cooper & Schindler, 2001:493):

- Formulate the null hypothesis and the alternative hypothesis.
- Select an appropriate statistical technique and the corresponding test statistic.
- Choose the level of significance.
- Calculate the value of the test statistic.
- Interpret the test and make the statistical decision to reject or not reject the null hypothesis.
- Express the statistical decision in terms of the marketing research problem.

There are two general classes of significance tests, namely parametric and non-parametric (Cooper & Schindler, 2001:496). Parametric tests are more powerful because their data are derived from interval and ratio measurements. Non-parametric tests are used to test hypotheses with nominal and ordinal data. Parametric tests were to be the preferred tests of choice for the test of significance for this study, provided that their assumptions are met. The following were typical tests for consideration in this study: chi-square tests, analysis of variance (ANOVA), and multiple analyses of variance (MANOVA). The researcher was responsible for reviewing the assumptions pertinent to the chosen test before conducting the analysis.

Despite specific results from hypothesis testing and factor analysis, a study has to pay attention to the validity and reliability of the measurement instrument. Some of the main validity and reliability techniques are discussed in the following section.

6.6.5 Validity and reliability

Validity and reliability are criteria for evaluating a measurement tool and are briefly discussed below.

6.6.5.1 *Reliability*

Reliability refers to the extent to which a scale produces consistent results if repeated measurements are made (Malhotra, 1996:304). Two dimensions underlie the concept of reliability, namely repeatability and internal consistency (Zikmund, 2000:280). The repeatability of a measure can be assessed using the test-retest method. This involves administering the same scale or measure to the same respondents at two separate times to test for stability. The second dimension of reliability concerns the homogeneity of the measure. An attempt to measure an attitude may require asking several similar questions or presenting a battery of scale items. To measure the internal consistency of a multiple-item measure, scores on subsets of the items within the scale are correlated. One technique measuring internal consistency is Cronbach's coefficient alpha. The final items derived from the factor analysis were tested for their reliability by submitting them to item analysis and a Cronbach alpha assessment. Cronbach's coefficient alpha is a very suitable assessment of the realiability of the construct indicators because it has the most utility for multi-item scales at the interval level of measurement (Cooper & Schindler, 2001:217).

6.6.5.2 *Validity*

The validity of a scale may be defined as the extent to which differences in observed scale scores reflect true differences among objects on the characteristic being measured, rather than the systematic or random error (Malhotra, 1996:306). Researchers may assess content validity, criterion validity, or construct validity.

- **Content validity** consists of a subjective but systematic evaluation of the representativeness of the content of a scale for the measuring task at hand. If the instrument contains a representative sample of the universe of subject matter of interest, then content validity is acceptable. Determination of content validity is judgemental and can be approached in several ways. First, the researcher may determine it through a careful definition of the topic of concern, the items to be scaled and the scales to be used. A second way to determine content validity is to

use a panel of persons to judge how well the instrument meets the standards (Cooper & Schindler, 2001:212).

- **Criterion validity** examines whether the measurement scale performs as expected in relation to other variables selected as meaningful criteria. One source suggests that any criterion measure must be judged in terms of four qualities: relevance, freedom from bias, reliability and availability (Cooper & Schindler, 20011996:213).
- **Construct validity** addresses the question of what construct or characteristic the scale is measuring. In attempting to evaluate construct validity, both the theory and the measuring instrument are considered. Construct validity is the most difficult type of validity to establish (Churchill & Iacobucci, 2002:351). As a confirmatory procedure, factor analysis is primarily a method for assessing the construct validity of measures. Construct validity is supported if the factor structure of the scale is consistent with the constructs the instrument purports to measure (Floyd & Widaman, 1995:287).

To report the validity of the results for this study, the researcher assessed the construct validity of the measurement instrument. Confirmatory factor analysis (CFA) was used, since this analysis is, in its purest form, a form of validation. CFA is the predominant method of analysis found in the literature concerning validation studies, particularly when validating the internal factor structure of a newly developed test instrument (Steenkamp & Van Trijp, 1991:283; Hair *et al.*, 1998:114, 247; Burgers, De Ruyter, Keen & Streukens, 2000:154; Ferrara, 2000:102). More specifically, the construct validity was assessed by determining the unidimensionality, reliability, convergent validity, and discriminant validity of the measurement instrument. Unidimensionality can be defined as the existence of one construct underlying a set of items, and has been recognised as one of the critical and basic assumptions of measurement theory (Hattie, 1985:139). Convergent validity is demonstrated when a measure has relatively high correlations with other measures of the same common factor (Hair *et al.*, 1998:118). Another method to assess construct validity is to estimate the reliability (Steenkamp & Van Trijp, 1991:290; Burgers *et al.*, 2000:155) and variance-extracted measures (Hair *et al.*, 1998:611; Smith, Milberg & Burke, 1996:185) for each construct to assess whether

the specified indicators are sufficient in their representation of the constructs. Discriminant validity is determined by demonstrating that a measure does not correlate very highly with another measure from which it should differ (Peter, 1981:136).

6.7 SUMMARY

This chapter has provided a description of the various data sources and data collection methods, focusing on telephonic interviews as the preferred method of data collection. Special attention was paid to the sampling procedure, with systematic sampling as the chosen probability sampling method. Most of the chapter focused on the development of the questionnaire as the measurement instrument relating to objectives and hypotheses. Finally, the statistical procedures that were used for data analyses were briefly discussed.

In the next chapter the results and hypotheses testing of the data were discussed.

CHAPTER 7
RESEARCH RESULTS AND INTERPRETATION

7.1 INTRODUCTION

The empirical data collected during the study were subjected to statistical analysis to assess the reliability and validity of the measuring instrument and its constructs. This chapter first presents a summary of the realised sample compared to the planned sample for this study. It then provides a profile of the individuals interviewed for this study by providing their demographic characteristics, followed by descriptive analyses concentrating on all the questions in the questionnaire. The next section addresses the scale purification process by focusing on the exploratory factor analysis used to identify the underlying privacy dimensions, the reliability assessment of the measurement instrument, and the confirmatory factor analysis used to validate the earlier results. Finally, the chapter sets out the results of the hypothesis tests and a summary of the main findings.

7.2 REALISATION RATE

The data collection was conducted by means of telephonic interviews between 2 September and 7 October 2002. All phone calls were made between 08:00 and 21:00 from Mondays to Saturdays and lasted between 15 and 25 minutes per interview. In each household where an interview was conducted, one adult was interviewed. These individuals were randomly selected using the standard 'last birthday' technique. Trained interviewers from the Bureau of Market Research (BMR) conducted the telephonic interviews and the BMR's central office edited all the completed questionnaires. Although the interviewers were well-trained, checkbacks by BMR's central office revealed cheating by one interviewer and poor quality work from another interviewer. It was decided to conduct another 160 interviews to replace the incorrectly recorded responses. These further interviews were conducted between 14 and 28 October 2002.

It should be noted that the study cannot be generalised to South Africa as a whole, since it only represents South African households with listed numbers in the Telkom telephone directory service. Table 7.1 provides an outline of the realised sample compared to the planned sample for this study (as discussed in Chapter 6, Sections 6.4.3 and 6.4.4).

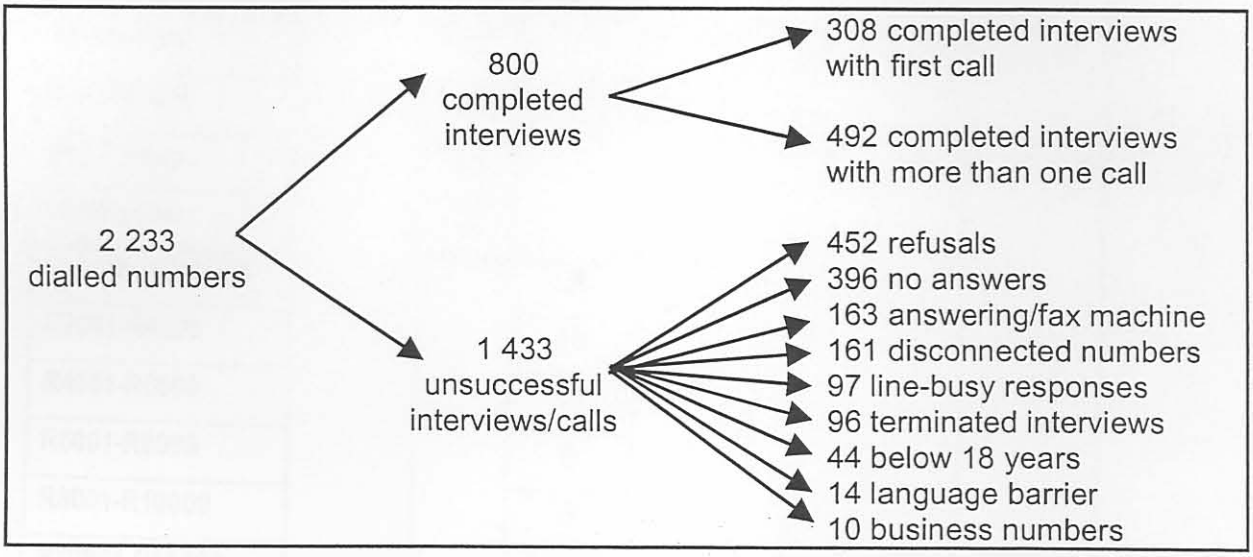
Table 7.1 Planned versus realised sample

AREA	Planned sample	Realised sample
Boland and West Coast	43	43
Cape Peninsula	111	111
Durban and surrounding area	71	71
East London and border	29	24
East Rand	62	64
Free State	43	38
Johannesburg	91	96
KwaZulu-Natal North Coast	15	16
KwaZulu-Natal South Coast	8	8
Mpumalanga	35	36
North West Province	38	41
Limpopo	22	21
Northern Cape and Namaqualand	17	17
Port Elizabeth and Eastern Cape	45	47
Pietermaritzburg and KwaZulu-Natal	31	27
Pretoria and surrounding area	58	60
Southern Cape and Karoo	19	17
Vaal Triangle	18	18
West Rand	44	45
TOTAL	800	800

The few discrepancies between the planned and the realised sample are mainly due to communication problems and inexperience among some population groups in rural areas regarding the topic under investigation. Although a random sample was drawn, a small percentage of respondents had to be replaced with respondents in areas where population groups were more familiar with English or Afrikaans, or more experienced with regard to the information privacy issue.

As has been mentioned in Chapter 6, the 800 pages of systematically selected telephone numbers for the survey were generated using Telkom's electronic telephone directory. If interviewers dialled the first telephone number on their telephone sheet and could not identify an adult or complete an interview with an appropriate person at the identified number, the second number on their telephone sheet was chosen, thereafter the third number, until a complete interview could be recorded. A total of 2 233 telephone numbers had to be dialled to reach the target of 800 completed interviews. Of all the dialled numbers, there were 800 completed interviews (452 refusals, 396 numbers with no answers, 163 automatic answering responses and/or fax machines, 161 disconnected numbers, 97 repeated line-busy responses, 96 terminated interviews, 44 individuals below the age of 18 years, 14 individuals who could not understand Afrikaans or English, and 10 unaccounted for business numbers). Figure 7.1 provides a summary of the dialled numbers. The response rate for the survey was 39 per cent, excluding the disconnected and the unreachable numbers. Based on the number of contacts with eligible households, the overall co-operation rate was 59 per cent. The total realised sample was 800 and the complete dataset was used for the descriptive analysis. However, for the exploratory factor analysis, only 627 questionnaires were useful for the scale purification process (don't know and refuse answers in the questionnaires were excluded from the dataset). Please refer to Section 7.4 for the discussion on scale purification.

Figure 7.1 Distribution of dialled numbers



After all the interviews had been completed, the questionnaires were edited, detected errors were corrected, and the data were coded. Coding entails a technical process whereby codes are assigned to the respondents' answers preparatory to the tabulation of the raw data (Martins, Loubser & Van Wyk, 1996:299). The coding process was two-dimensional:

- All completed questionnaires were transformed into symbols (codes) which could be assessed by a computer (data input).
- Mistakes which were invariably made during the coding and data input process were 'cleaned'.

The coding process was followed by computerised data capturing before the data analysis was performed. The dataset was cleared of possible coding and data-capturing errors. The next section provides an overview of the descriptive analysis of the dataset.

7.3 DESCRIPTIVE STATISTICS

The first section below provides a profile of the individuals interviewed for this study by setting out percentages of their demographic characteristics. All percentages were rounded to a full number with no decimals. The following demographic results are

presented in Table 7.2: gender, age, income, language, ethnic orientation, employment status and level of education. The percentage distribution of each demographic subgroup is presented. Although the results are mainly self-explanatory, a few remarks on the percentage distributions follow.

Table 7.2 Demographic profile of respondents

PERCENTAGES OF SUBGROUPS*	Gender (%)	Age (%)	Income (%)	Language (%)	Ethnic orientation (%)	Employ-ment status (%)	Level of education (%)
Male	36						
Female	64						
18-25 years		14					
26-35 years		20					
36-45 years		21					
46-55 years		17					
56-65 years		15					
66-75 years		10					
76-85 years		3					
Less than R2 000			35				
R2001-R4000			19				
R4001-R6000			13				
R6001-R8000			8				
R8001-R10000			5				
R10001-R15000			6				
R15000 plus			6				
Refused to answer			8				

PERCENTAGES OF SUBGROUPS*	Gender (%)	Age (%)	Income (%)	Language (%)	Ethnic orientation (%)	Employ-ment status (%)	Level of education (%)
English				41			
Afrikaans				37			
Black African				20			
Other				2			
Black African					21		
Coloured					13		
Indian/Asian					10		
Caucasian					56		
Employed full-time						39	
Employed part time						6	
Self-employed						13	
Not-employed						9	
Student						6	
Homemaker/ Housewife						9	
Pensioner/ Retired						17	
Unfit for work						1	
Lower than Grade 10							11
Grade 10							14
Grade 12							38
Degree/Diploma							29
Post graduate/ Higher diploma							8

* All percentages add up to 100 per cent

The following observations can be drawn from the above table:

- **Gender:** Nearly two-thirds of the respondents were female. Since many of the telephonic interviews were conducted during the day, more females, especially stay-at-home mothers or housewives, were likely to answer the telephone.

- **Age:** Respondents were requested to provide their year of birth at the end of the interview. To make the processed results more interpretable, the answers were grouped into seven age categories. From Table 7.2 it can be observed that 55 per cent of the respondents were below the age of 46 years. Of the respondents, 13 per cent were above 65 years of age, which corresponds with the percentage of respondents (17 per cent) who indicated that they are pensioners or retired.

- **Income:** Income always seems to be a sensitive question to respondents. In this study, eight per cent of the respondents refused to provide their total monthly income. Of those who answered the question, 59 per cent indicated that they earn below R4 000 per month, with the remaining 41 per cent earning more than R4 000 per month.

- **Language:** Respondents were given an opportunity to indicate their home language from a list containing all eleven official languages. A twelfth option, marked as 'other', was provided to respondents whose home language did not fit within one of the eleven options. Two per cent of the respondents indicated that they have another home language such as Bulgarian, Chinese, Dutch, French, German, Hindi, Koisan, Polish and Portuguese. To simplify the results, a decision was made to group all of the nine Black African languages into one group. Of the respondents, 20 per cent belonged to the Black African language group. The majority of respondents (41 per cent) reported that English was their home language, while 37 per cent were Afrikaans-speaking respondents.

- **Ethnic orientation:** Although the questionnaire did not contain specific questions regarding racial classification, this category was recorded by interviewers by means of deduction from the telephone sheets (surname and geographical area), as well as the accent of the respondent. The majority of the respondents (56 per cent) were categorised as being Caucasian, with the minority (10 per cent) being respondents from Indian or Asian origin. The fact that many African consumers do not have telephone lines, may explain why only 21 per cent of the respondents were classified as being Black African.

- **Employment status:** Fifty-eight per cent of the respondents formed part of the workforce. The remaining 42 per cent were not actively involved in the formal workplace, since they were physically unfit for work (1 per cent), or were housewives or students (15 per cent). As mentioned previously, 17 per cent of the respondents identified themselves as being retired.

- **Level of education:** Three-quarters of the respondents (75 per cent) specified that they had completed their high school education. Almost 40 per cent of the respondents have some form of tertiary education.

The next section of the descriptive analysis focuses on the remaining questions in the questionnaire. The results of Questions 1 to 45 are discussed in different sections, according to the eight dimensions identified in Chapter 5, Section 5.3. The percentage distributions are provided for each of the 45 information privacy-concerned responses. These concerns were measured on 5-point Likert scales. The cumulative percentages for the two 'top-boxes' and the two 'low-boxes' are presented in each table.

7.3.1 Respondents' concerns regarding companies' data collection practices

Six statements in the questionnaire (Questions 1 to 6) related to consumers' information privacy concerns regarding the data collection practices of companies. (Refer to

Appendix 1 for an example of the questionnaire). Table 7.3 shows the percentage distributions.

Table 7.3 Concerns regarding data collection practices

DATA COLLECTION CONCERNS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
1. Companies generally ask too much personal information from consumers.	27	7	65	99
2. You do not mind to provide a lot of personal information if you think it is necessary.	24	4	71	99
3. Companies seldom collect personal information from consumers without their permission.	36	9	51	96
4. You are confident that you can prevent companies from collecting personal information that you would like to keep secret.	40	8	51	99
5. Most companies collect personal information from consumers in order to provide them with products and services to better suit their needs.	30	8	60	98
6. You are satisfied when companies collect your personal information as a means to provide you with products and services which better suit your needs.	24	6	69	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

A few remarks on the above-mentioned percentages are appropriate:

- Nearly two-thirds of respondents (65 per cent) believe that companies ask for too much personal information, although 71 per cent say that they do not mind providing a great deal of personal information if they think it is necessary.
- Five out of ten respondents (51 per cent) agreed that companies seldom collect information from consumers without their permission, although 36 per cent felt that this was not the case.
- A slight majority of respondents (51 per cent) contended that they could prevent companies from collecting information which they would like to keep secret; as

opposed to 40 per cent of respondents who were not convinced that they could do so.

- Six out of ten respondents (60 per cent) felt that companies collected their personal information in return for better provision of products or services, and 69 per cent were satisfied that their information was used to provide them with better products and services.

From the above it can be concluded that the majority of respondents (65 per cent) indicated one major concern relating to data collection, namely that companies ask for too much personal information. Lower levels of concern were indicated for all the other areas pertaining to data collection practices.

7.3.2 Respondents' concerns regarding companies' data storage and security practices

Questions 7 to 12 in the questionnaire related to consumers' information privacy concerns with regard to the data storage and security practices of companies. Table 7.4 indicates the percentage distribution of respondents' answers.

Table 7.4 Concerns regarding data storage and security practices

DATA STORAGE AND SECURITY CONCERNS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
7. You believe that most companies allow their consumers to have access to their personal information kept by the companies.	40	10	46	96
8. You feel it is important to have access to the personal information companies keep of you.	12	3	84	99
9. You believe that companies have adequate measures in place to ensure that all personal information in their records is accurate.	34	10	54	98

	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
10. You feel concerned that companies do not devote enough time and effort to ensure that your personal information is accurate while in their possession.	23	9	66	98
11. Personal information is safe while stored in a company's records.	56	8	35	99
12. You fear that your personal information may not be safe while stored in a company's records.	27	6	67	100

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

A few remarks on the above-mentioned percentages are provided below:

- A large majority of respondents (84 per cent) believed that it is important for them to have access to their personal information, and 40 per cent of the respondents felt that companies did not allow their customers to have access to their personal information.
- More than half of the respondents (54 per cent) believed that companies had adequate measures in place to ensure that their information was accurate, although 66 per cent were concerned that companies did not devote enough time and effort to ensure that their information was accurate while in their possession.
- A total of 56 per cent of the respondents said that they did not think their personal information was safe while stored in a company's records, and 67 per cent were afraid of this situation.

From the above it can be concluded that the greatest concern of respondents regarding data storage and security, was their level of access to their personal information in an organisation's database. South Africa's Promotion of Access to Information Act of 2000 addresses this concern and was enacted to force all organisations to produce manuals of information held by the organisation (refer to Chapter 2, Section 2.5.2).

7.3.3 Respondents' concerns regarding companies' data use practices

Six statements in the questionnaire (Questions 13 to 18) related to consumers' information privacy concerns with regard to the data use practices of companies. Table 7.5 depicts the main findings.

Table 7.5 Concerns regarding data use practices

DATA USE CONCERNS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
13. Most consumers have control over the ways their personal information is used by companies.	60	6	34	100
14. You are satisfied about the control you have over the ways companies use your personal information.	53	6	40	99
15. You believe that companies regularly use consumers' information for other purposes than that for which it was collected.	23	10	64	97
16. You do not mind when companies use your personal information for other purposes than those provided when they collected your information.	85	3	12	100
17. You believe that consumers' personal information is often misused by companies.	16	9	71	96
18. You are concerned about the possible misuse of your personal information by companies.	15	5	79	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

The above results indicate that respondents were concerned about organisations' use (and misuse) of their personal information. For many respondents, the information privacy issue related to their control over their personal information.

- Many respondents (60 per cent) were concerned that they do not have control over the ways their personal information is used by companies, and 53 per cent were not satisfied about the **control** they had over the ways companies use their personal information.

- Nearly two-thirds (64 per cent) expressed a belief that companies regularly use their information for other purposes than that for which it was collected, and a large majority (85 per cent) did not find this practice acceptable.
- Some respondents' anxiety over the collection of personal information was related to **how** the information is used rather than **what** data are being collected. This was confirmed by the results indicating that a clear majority (71 per cent) agree strongly or slightly that companies often misuse their information, and 79 per cent were very concerned about the possible misuse of their personal information.

This dimension of concern points to a higher level of concern than the results from the previous data practices. It is worth nothing the very high concern of respondents regarding the **misuse** or **possible misuse** of their personal information (71 per cent and 79 per cent).

7.3.4 Respondents' concerns regarding companies' data disclosure and dissemination practices

Questions 19 to 24 in the questionnaire related to consumers' information privacy concerns with regard to the data disclosure and dissemination practices of companies. Table 7.6 illustrates the main findings.

Table 7.6 Concerns regarding data disclosure and dissemination practices

DATA DISCLOSURE AND DISSEMINATION CONCERNS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
19. Companies regularly share personal information with other companies without the permission of the individuals to whom the information belongs.	20	10	66	96
20. You are uncomfortable when companies share your personal information with other companies without asking your permission first.	8	1	90	99

	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
21. You believe that companies regularly share personal information of consumers with other companies, so that these other companies could offer products and services to consumers.	20	10	68	98
22. You feel it is unacceptable when a company shares your personal information with other companies so that those companies can offer their products and services to you.	13	4	83	100
23. Companies always provide their customers with the opportunity to request the removal of their names and addresses from records that are sold to other companies.	64	9	24	97
24. You are concerned when companies do not provide you with an opportunity to remove your name and address from any records that it provides to other companies.	8	4	87	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

The above results indicate that respondents had high level of concern about organisations' disclosure and dissemination practices.

- A large majority of the respondents (90 per cent) were uncomfortable when companies shared their personal information with other companies without first asking their permission. This is supported by 83 per cent who felt it was unacceptable when companies share their personal information with other companies so that those companies can offer their products and services to them.
- Respondents also exhibited high levels of concern (87 per cent) about companies' unwillingness to provide them with an opportunity to remove their name and address from records that they provide to other companies.
- A total of 66 per cent of respondents was of the opinion that companies regularly shared their information without their permission. This correlates with their very high level of concern (90 per cent) regarding this practice.

- A further 68 per cent of respondents believed that companies regularly share their personal information with other companies to use for marketing purposes.
- Nearly two-thirds of respondents (64 per cent) contended that companies provide their customers with an opportunity to request the removal of their names and addresses from lists that are sold to other companies.

Respondents expressed the opinion that companies' sharing personal information with other companies is by far their greatest concern (90 per cent). Respondents seemed most concerned about the risk that their personal information could be made available to other individuals or companies. This is a serious signal to businesses that they should pay careful attention to their data disclosure practices and the dissemination of data.

7.3.5 Respondents' concerns regarding companies' solicitation practices

One of the privacy concerns of individuals was media intrusiveness. Questions 25 to 30 in the questionnaire related to consumers' information privacy concerns regarding the solicitation practices of companies. Table 7.7 provides the main findings relating to respondents' solicitation concerns.

Table 7.7 Concerns regarding solicitation practices

SOLICITATION CONCERNS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
25. Companies send consumers too many unrequested advertising material that is not of interest to them.	18	5	77	100
26. It bothers you that you receive so many unrequested advertising material that is of no interest to you.	22	4	74	100
27. Too many companies call consumers at their homes to sell products and services to them.	25	10	65	100

	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
28. You do not mind when you receive telephone calls at your home from companies wanting to sell products and services to you.	62	8	30	100
29. Consumers are not interested in getting information about new products and services from companies with which they have not done business before.	33	11	56	100
30. You are pleased when you receive information about new products and services from companies with which you have not done business before.	46	10	44	100

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

A few remarks on the above table are pertinent:

- The majority of respondents (77 per cent) were of the opinion that companies send them too many unrequested advertising material, and 74 per cent reported that this bothered them.
- With regard to telemarketing practices, 65 per cent of respondents said that too many companies call consumers at home to sell their products and services to them, and 62 per cent were not satisfied when this occurs.
- More than half of the respondents (57 per cent) reported that they were not interested in getting information from companies with which they had not done business before. It is, however, interesting to note that 44 per cent indicated that they were, nevertheless, pleased when they received this information.

The solicitation practices of companies seemed to be one of the major concerns of respondents, which is in line with trends in other countries. The USA has approved a national do-not-call list in March 2003 intended to help consumers block unwanted telemarketing calls (refer to Chapter 3, Section 3.3.1.1).

7.3.6 Respondents' expectations regarding privacy policies

Questions 33, 36, 39, 42, and 45 in the questionnaire related to consumers' privacy policy expectations from companies during the various stages of data collection, storage and security, use, disclosure and dissemination, and solicitation. Table 7.8 outlines the main findings of respondents' privacy policy expectations.

Table 7.8 Privacy protection policy expectations

PRIVACY POLICY EXPECTATIONS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
33. Companies must have privacy protection policies to make provision for customers who would not like to receive unrequested advertising material.	4	2	94	100
36. Companies should have privacy protection policies indicating that no personal information will be provided to other companies without consent from their customers.	2	1	97	100
39. Companies should have privacy protection policies indicating the reasons for collecting personal information from consumers.	3	1	95	99
42. Companies should use independent auditing firms to confirm that they use the personal information of consumers, as promised in the companies' privacy policies.	8	4	87	99
45. Companies should have privacy protection policies indicating how they will protect the customer's information while it is in their possession.	1	1	97	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

The following can be deduced from Table 7.8:

- The highest expectations related to the protection that privacy policies offer when information is provided to others without one's consent (97 per cent), as well as to

how a company protects consumers' information while it is in the company's possession (97 per cent).

- Other expectations included a clear guideline from companies as to the reasons why they collect one's personal information (95 per cent); and provision for customers who would not like to receive unrequested advertising material (94 per cent).
- Retaining an independent auditing firm to verify that a company is doing what it promises in its privacy policies, would instil confidence in 87 per cent of respondents.

The above results indicate that respondents regarded it as very important for companies to establish effective privacy protection policies. The majority of these respondents have very strong expectations regarding companies' privacy protection policies.

7.3.7 Respondents' expectations regarding legislation and government protection

Questions 31, 34, 37, 40, and 43 in the questionnaire related to consumers' legislation and government protection expectations. Table 7.9 sets out the main findings regarding respondents' expectations in respect of government protection.

Table 7.9 Legislation and government protection expectations

EXPECTATIONS ABOUT GOVERNMENT'S ROLE	Disagree slightly/strongly %	Neutral %	Agree slightly/strongly %	TOTAL* %
31. Legislation should prevent a company from sharing your personal information with other companies without your permission.	9	2	89	100
34. Government should restrict companies to collect only the information needed for a specific transaction.	6	3	91	100
37. Government should do more to protect the safety of personal information.	5	2	93	100
40. Government should limit companies' use of personal information to only that purpose for which it was collected.	6	2	92	100

	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
43. Government should limit unrequested advertising material sent to consumers.	19	5	75	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

Respondents expressed extremely high expectations regarding legislation and government protection of their information privacy.

- The highest expectation (92 per cent) related to government's role in protecting the safety of consumers' information.
- It is worth noting the very high expectations of respondents regarding the notion that government should restrict companies' collection of personal information (91 per cent), as well as limit the use thereof (92 per cent).
- Almost nine out of ten (89 per cent) consumers responded that there should be legislation to prevent companies from sharing their information with others without their permission.
- Three quarters of consumers (75 per cent) also expressed the expectation that government has an obligation to limit unrequested advertising material.

The above results indicate that respondents regarded it is extremely important that government should protect their information privacy. In all the responses, a large majority of respondents displayed very strong expectations regarding government's role in handling their information privacy.

7.3.8 Respondents' behavioural intentions

Questions 32, 35, 38, 41, and 44 in the questionnaire related to consumers' behavioural intentions when it comes to protecting their privacy. Table 7.10 highlights the main findings of respondents' behavioural intentions.

Table 7.10 Behavioural intentions

BEHAVIOURAL INTENTIONS	Disagree slightly/strongly	Neutral	Agree slightly/strongly	TOTAL*
	%	%	%	%
32. You would request a company to remove your personal information from their records if you suspected that they were misusing it.	3	1	96	100
35. You would support any initiatives that will enable you to stop companies from sending you unrequested advertising material.	16	5	79	100
38. You would request to having your personal information removed from any company's records if they sell the information to others.	3	1	95	99
41. You would support a company's efforts that will ensure that your personal information is safely kept.	2	1	97	100
44. You would refuse to provide your personal information to a company who cannot provide reasons why they want to collect your personal information.	3	1	95	99

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

Consumers may engage in various protective behaviours, believing that they can manage their information, and thus minimise the potential consequences. Most notable is consumers' willingness to change their behaviour if they feel a business is not addressing the information privacy issue appropriately. The high percentages found in this study indicated that the majority of respondents intended to change their behaviour to protect their personal privacy.

- One very positive indication is respondents' willingness to support (97 per cent) a company's efforts to ensure that their information is safely kept.
- Alarming news to companies is the fact that 79 per cent of respondents are also willing to support any initiatives to stop companies from sending unrequested advertising material.
- Respondents indicated very strong intentions to behave 'negatively' if they felt their privacy was not protected. Large majorities indicated that they would requested the

removal of their information if they suspected misuse of their information (96 per cent), or if their information was sold to others (95 per cent).

- Respondents also expressed their intention to refuse to provide their personal information if companies could not provide reasons for wanting to collect their information (95 per cent).

The next section of the descriptive analysis presents the results of three questions relating to the opinions of respondents regarding information control (Question 46), businesses handling of information (Question 47), and consumer protection (Question 48).

7.3.9 Concerns relating to control, businesses' use of information and level of protection

Questions 46 to 48 in the questionnaire measured specific consumer concerns. Table 7.11 shows the percentage distribution of respondents with regard to the three information privacy related questions. These concerns were measured on 4-point Likert scales, indicating the cumulative percentages of the two 'disagree' options and the two 'agree' options. The shaded cells indicate where the 'highly concerned' percentages lie.

Table 7.11 Concerns relating to control, businesses' use of information and level of protection

PRIVACY STATEMENTS	Disagree slightly/strongly	Agree slightly/strongly	TOTAL*
	%	%	%
46. Consumers have lost all control over how personal information is collected and used by companies.	25	72	97
47. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	45	50	95
48. Existing laws and organisational practices provide a reasonable level of protection for consumer privacy.	55	40	95

* Percentage totals do not add up to 100 per cent because of 'don't know', 'refuse', and 'missing' responses.

The strongest concern expressed by respondents (72 per cent) was that they 'have lost all control over how their personal information is collected and used by companies'. As mentioned previously in Chapter 6 (Section 6.5.4.3), the three above-mentioned statements (Questions 46 to 48) formed part of the measurement instrument to classify respondents into different privacy sensitive segments. The results in this regard are discussed later in this chapter (see Section 7.4.1.4).

The final section of the descriptive analysis presents the percentages of Questions 49 to 60. Answers to these questions related to respondents' previous protective behaviour, their knowledge of protective options, their Internet transaction use, their direct shopping behaviour, and the number of victims of privacy invasions. Table 7.12 highlights the results of respondents' answers.

Table 7.12 Results of respondents' answers to Questions 49 to 60

QUESTIONS	YES (%)	NO (%)	TOTAL (%)
49. Have you ever refused to give information to a company because you thought it was not really needed or it was too personal?	51	49	100
50. Have you ever requested a company to remove your name and address from records that they use for marketing purposes?	22	78	100
51. Have you ever notified a company that you do not want to receive their unrequested advertising material?	30	70	100
52. Have you ever requested that a company not share your personal information with any other company?	24	76	100
53. Have you ever requested a company to inform you which measures they use to keep your personal information safe?	17	83	100
54. Have you ever personally been a victim of a situation you felt was an invasion of your private information?	31	69	100
55. Are you aware of any options to remove your name from records of companies?	21	79	100
56. Have you ever purchased anything via the Internet?	12	88	100
57. Do you make use of Internet banking services?	19	81	100

	YES (%)	NO (%)	TOTAL (%)
58. During the past year, have you personally bought something from a catalogue or brochure sent to you?	35	65	100
59. During the past year, have you personally bought any product or service offered to you by a telephone call?	14	86	100
60. During the past year, have you personally called a toll-free (0800) number to order something?	9	91	100

Despite the very high privacy concerns indicated previously in the areas of data collection, storage and security, use, disclosure and dissemination and solicitation, these concerns have not been manifested in privacy protective behaviours. A minority of the respondents have shown protective behaviours, as indicated by the following:

- Half of the respondents (51 per cent) said that they had refused to give personal information to a business at one time or another because they felt the information requested was just too personal or not really necessary (Question 49).
- Consumers have the option to request that their name and address be removed from lists that are used for marketing purposes or lists that are shared with other companies. It is interesting that only 22 per cent of the respondents had ever requested a company to remove their name and address from lists used for marketing purposes (Question 50), and only 24 per cent had requested that their information not be shared with other companies (Question 52).

Only two out of ten respondents (21 per cent) were aware of any options available to remove their names from the records of companies. The fact that a large majority of the respondents (79 per cent) were **not** aware of name removal procedures may be a reason for the high levels of concern in this survey, since they did not know about available options to safeguard their personal information.

In this survey, two questions investigated consumers' use of the Internet for basic transactions. Only 12 per cent of the respondents indicated that they had purchased something via the Internet (Question 56), with 19 per cent reporting that they used Internet banking services (Question 57).

During the past year, 35 per cent of respondents had purchased something from a catalogue or brochure sent to them (Question 58), and 9 per cent had called a toll-free number to place an order (Question 60). A total of 14 per cent said that they had bought something through telemarketing (Question 59).

From the above descriptive statistics it is clear that: the majority of respondents did not exert protective behaviour toward their personal information (Questions 49-53); did not feel that their personal privacy had been invaded (Question 54); and did not have knowledge about how to protect their personal information (Question 55). This corresponds with the descriptive statistics of Questions 56 to 60, which indicated that a minority of the respondents is active in terms of transactions on the Internet or through direct marketing media, where individuals are more exposed to possible privacy invasions. One exception here was that a total of 51 per cent of the respondents had, occasionally, refused to provide information to a company because they contended that the information requested was not really needed or it was too personal.

The next section focuses on the purification of the information privacy scale.

7.4 SCALE PURIFICATION

As has been mentioned in previous chapters, there is an absence of validated measurements for empirical studies addressing individual perceptions on information privacy. Therefore, a measurement instrument was developed, but it had to be validated for use in future information privacy research. The scale purification process aimed to address the primary research objective, namely, to identify and explore the information privacy concerns of South African consumers. A prerequisite step in the creation of a validated measurement instrument was the consideration of the dimensionality of the relevant construct (Smith *et al.*, 1996:168). This led to a scale purification process consisting of three distinct phases:

- first, an assessment of the underlying dimensionality of privacy concerns using exploratory factor analysis (Section 7.3.1);

During the past year, 35 per cent of respondents had purchased something from a catalogue or brochure sent to them (Question 58), and 9 per cent had called a toll-free number to place an order (Question 60). A total of 14 per cent said that they had bought something through telemarketing (Question 59).

From the above descriptive statistics it is clear that: the majority of respondents did not exert protective behaviour toward their personal information (Questions 49-53); did not feel that their personal privacy had been invaded (Question 54); and did not have knowledge about how to protect their personal information (Question 55). This corresponds with the descriptive statistics of Questions 56 to 60, which indicated that a minority of the respondents is active in terms of transactions on the Internet or through direct marketing media, where individuals are more exposed to possible privacy invasions. One exception here was that a total of 51 per cent of the respondents had, occasionally, refused to provide information to a company because they contended that the information requested was not really needed or it was too personal.

The next section focuses on the purification of the information privacy scale.

7.4 SCALE PURIFICATION

As has been mentioned in previous chapters, there is an absence of validated measurements for empirical studies addressing individual perceptions on information privacy. Therefore, a measurement instrument was developed, but it had to be validated for use in future information privacy research. The scale purification process aimed to address the primary research objective, namely, to identify and explore the information privacy concerns of South African consumers. A prerequisite step in the creation of a validated measurement instrument was the consideration of the dimensionality of the relevant construct (Smith *et al.*, 1996:168). This led to a scale purification process consisting of three distinct phases:

- first, an assessment of the underlying dimensionality of privacy concerns using exploratory factor analysis (Section 7.3.1);

- second, an assessment of the internal consistency of the measurement instrument by calculating the item-to-total correlation as well as the Cronbach alpha coefficients (Section 7.3.1.1); and
- third, testing the validity of the factor model identified by the exploratory factor analysis using confirmatory factor analysis (Section 7.3.2).

It is important to note that a different set of data is required to test the validity of a factor model identified using exploratory factor analysis. Therefore the sample was randomly split in half (Hair *et al.*, 1998:114; Lattin, Carroll & Green, 2003:199). First, the one half of the data was used to determine the actual number of dimensions underlying the construct. The other half of the sample was used to validate the measure that resulted from the analysis.

The scale purification process will is now discussed in detail.

7.4.1 Exploratory factor analysis

The data were prepared for the factor analysis by handling the missing values by means of casewise deletion. Respondents who had marked the 'don't know' or 'refuse' options were discarded, since they did not indicate their degree of agreement or disagreement on the 5-point Likert scales and could not be included in the factor analysis. Although the casewise deletions reduced the dataset from 800 to 627 respondents, this did not present a problem, since this was still an adequate sample size. Variables 1 to 45 (Questions 1 to 45) were included in the factor analysis, as they all measured privacy concerns. No mean substitution was necessary since all the remaining respondents had indicated their concerns on the 5-point scales.

Program 4M of the BMDP statistical package (SAS Institute, 2000a) was used to factor analyse the data. The first step was to examine whether the data was suitable for factor analysis. The critical assumptions underlying factor analysis are more conceptual than statistical. From a statistical standpoint, the researcher must ensure that the data matrix

has sufficient correlation to justify the application of factor analysis (Hair *et al.*, 1998:99). Visual inspection of the correlations revealed a substantial number of correlations greater than 0.30, indicating that factor analysis was appropriate. The correlations between variables were also analysed by computing the partial correlations between variables (the correlations between variables when the effects of other variables are taken into account). The small partial correlations indicated that 'true' factors existed in the data because the variables were explained by the factors (variates with loadings for each variable).

The next step in the scale purification process consisted of an exploratory factor analysis to assess whether the data contained different underlying dimensions of privacy concerns. For this purpose, a Maximum Likelihood Exploratory Factor Analysis (common factor analysis) was conducted to identify the latent dimensions or constructs represented in the original variables. When a large set of variables is factored, the method first extracts the combinations of variables explaining the greatest amount of variance and then proceeds to combinations that account for smaller amounts of variance (Hair *et al.*, 1998:103). To determine how many factors to extract, a combination of several criteria was used, namely, the latent root criterion, percentage of variance criterion and the scree test criterion (Cattell, 1966:245-276; Hair *et al.*, 1998:104).

- First, the latent root criterion was applied. The rationale for the latent root criterion is that each variable contributes a value of 1 to the total eigenvalue. Only latent roots (or eigenvalues) greater than 1 are considered significant, and all factors with latent roots less than 1 are considered insignificant and are discarded (Hair *et al.*, 1998:103). In this analysis (with all 45 of the privacy concerned items in the questionnaire), a number of 10 eigenvalues were greater than one, indicating a possibility of ten different factors for the data. Table 7.13 indicates the respective eigenvalues for the ten factors.

Table 7.13 Eigenvalues for identified factors

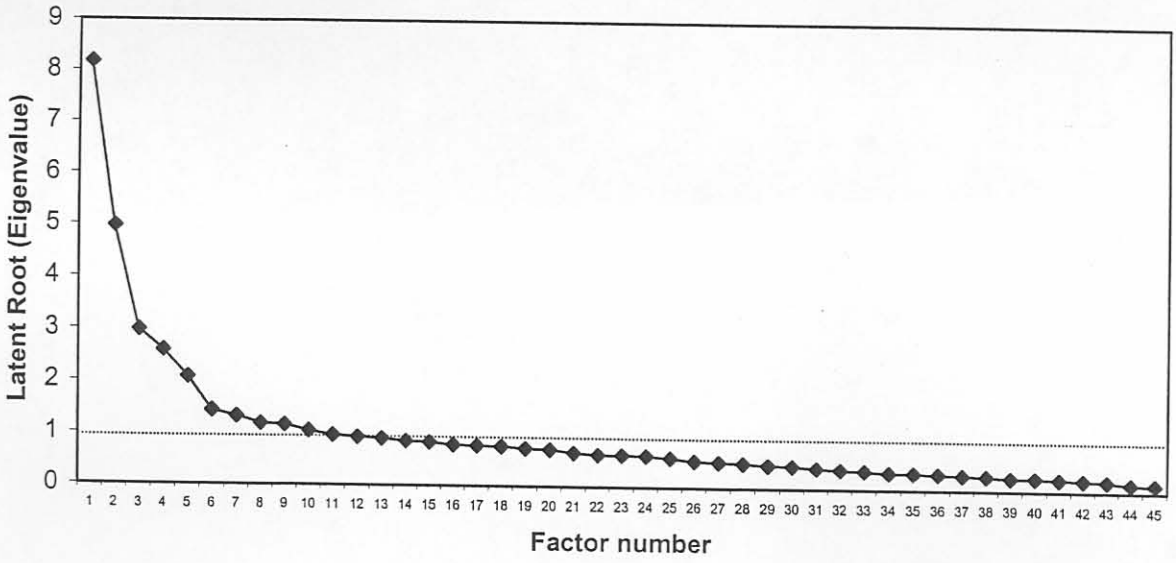
Factor	Eigenvalue	Cumulative proportion of variance explained
1	8.17	0.0776
2	4.97	0.1561
3	2.98	0.2520
4	2.59	0.3132
5	2.09	0.3640
6	1.42	0.4038
7	1.32	0.4425
8	1.19	0.4577
9	1.17	0.4758
10	1.05	0.4882

- Second, the percentage of variance criterion was considered. This is an approach based on achieving a specified cumulative percentage of total variance extracted by successive factors. Although no threshold has been adopted, a solution that accounts for 60 per cent of the total variance is regarded as satisfactory, but can even be less in instances where information is less precise (Hair *et al.*, 1998:104). As can be seen from Table 7.13 above, the first ten factors specified a cumulative percentage of 49 per cent of the total variance. It is, however, evident that the last three factors (Factors 8 to 10) each contributed less than two per cent to the cumulative percentage.

- Finally, the scree test was examined to establish the number of factors to be extracted. A scree test is used to identify the optimum number of factors that can be extracted before the degree of unique variance starts to dominate the common variance structure. A scree test is derived by plotting the latent roots against the number of factors in their order of extraction, and the shape of the resulting curve is used to evaluate the cut-off point. The point at which the curve begins to straighten

out is considered to indicate the maximum number of factors to extract (Hair *et al.*, 1998:104). According to Kline (1999:75), there is agreement among most factor analysts of any repute that Cattell's scree test is close to the best solution of selecting the correct number of factors. From the scree plot of the unaltered correlation matrix (see Figure 7.2), it is evident that the cut-off point for the number of factors to be extracted in this study, was between five and six factors, after which the curve straightened out.

Figure 7.2 Eigenvalue plot for scree test criterion



The scree test suggested that a fewer number of factors (between five or six factors) had to be considered for extraction compared to the latent root and percentage of variance criteria (suggesting ten factors). However, when considering the small contribution of Factors 8 to 10 to the cumulative percentage of total variance extracted, it supported the scree test result of considering fewer factors for extraction. Based on the indications of the different criteria discussed above, it was decided to extract six factors during the first round of analysis.

Maximum Likelihood Exploratory Factor Analysis was conducted, specifying a Direct Quartimin oblique rotation of the original factor matrix. The oblique rotation technique

was used because the theoretically underlying dimensions were assumed to be correlated with each other, and an oblique factor rotation allowed for intercorrelation between factors (Hair *et al.*, 1998:102). Items were considered for deletion depending on the item's factor loading. Factor loadings greater than 0.50 were considered to meet the minimum level and to have practical and statistical significance for all the factor solutions. The 0.50 criterion for the significance of the factor loadings was based on the sample size and the number of variables being analysed (Hair *et al.*, 1998:111-112). Items with loadings below 0.50 and items that did not load on any factor were identified for possible deletion. Items that loaded on more than one factor were considered for interpretation on the factor on which it had a significant loading, and, depending on their contribution to the research, were considered for possible deletion.

The factor loadings of the rotated six-factor matrix were examined, and that items did not meet the minimum criteria (as discussed above) were deleted. The six-factor solution did not yield satisfactory results, with only one item loading significantly on Factor 6 (refer to Appendix 3 for the rotated six-factor loading matrix for all the variables). It was decided not to pursue this solution any further, and to extract five factors during a second round of analysis. The same procedure was followed, namely factor rotation followed by a process to delete items that did not load significantly, did not load on any factors, or loaded on more than one factor. Again the factor solution did not perform very well. Only three items loaded significantly on Factor 5 (with one of the items being a double loading) (refer to Appendix 4 for the rotated five-factor loading matrix for all the variables). This was followed by a decision to consider a four-factor model for the third round of analysis.

The four-factor solution (containing all 45 items) had a total of 30 items loading greater than 0.50 on the four factors, with loadings varying between 0.50 and 0.77. The four-factor solution explained 36 per cent of the total variance. The ten items that loaded below 0.50 (Questions 1, 2, 8, 9, 10, 13, 16, 22, 23 and 42), the five items that did not load on any factors (Questions 3, 4, 5, 6 and 7), and the two items that loaded onto more than one factor (Questions 31 and 35) were discarded (refer to Appendix 5 for the

initial four-factor loading matrix containing all 45 items). The four-factor model was respecified and the analysis was repeated on the remaining 28 items. The respecified four-factor solution indicated another two items that loaded below 0.50 and one item that loaded on more than one factor. These items were again deleted, the model respecified, and the analysis repeated. The next factor solution indicated that the remaining 25 items loaded greater than 0.50 on one of the four factors. When a factor solution had been obtained in which all variables had a significant loading on a factor, labels could be assigned to the different factors. Based on the interpretation of the items that loaded on these scales, they were labelled 'privacy protection', 'information misuse', 'solicitation' and 'government protection'.

Of the eight dimensions that were built into the measurement instrument (refer to Chapter 5, Section 5.3), two dimensions were represented by two factors each, two dimensions grouped together under one factor, and the remaining four dimensions grouped together in another factor. Detail on the items of each factor is provided below:

- **Factor 1:** The first factor contained nine items, with eight items stemming from two of the anticipated dimensions, namely privacy protection policies and behavioural intentions. The factors that loaded onto factor one represented four items pertaining to privacy protection policies, and four items to behavioural intentions. Only one item did not belong to either of the two dimensions and related to data disclosure. Since all the items referred to consumers' privacy protection in general, the factor was labelled 'privacy protection'.

- **Factor 2:** The items in the second factor belonged to three of the identified dimensions, namely data storage and security, data use, and data disclosure and dissemination. Although this factor did not relate to any of the eight dimensions, all the items in the factor related to information use or misuse by organisations. This factor identified a 'new' but significant concern and was labelled 'information misuse'.

- **Factor 3:** All six the items of the solicitation dimension loaded onto factor three. This indicated a strong concern that consumers have regarding a desire to be left alone. Since the third factor related directly to one of the anticipated dimensions, namely solicitation, it was therefore labelled 'solicitation'.

- **Factor 4:** After deleting the items that did not meet the minimum criteria, only three items relating to the dimension of legislation and government protection remained. All three of these items loaded onto factor four, and the factor was labelled 'government protection'.

Since the four-factor solution emerged as the most interpretable factor structure, the internal consistency of the different factors can be assessed.

7.4.1.1 Reliability assessment

The final 25 items derived from the factor analysis were tested for their reliability by submitting them to item analysis (calculation of corrected r_{it}-values[2] of the items) using item-to-total correlations. The items for each subscale were analysed separately (Steenkamp & Van Trijp, 1991:286). Rules of thumb suggest that the item-to-total correlations should exceed 0.50 (Hair *et al.*, 1998:118). The item analysis revealed no item-to-total values below 0.50 and no items were deleted. The item-to-total correlations can be viewed in Table 7.15. The final four-factor solution had a total of 25 items with loadings varying between 0.54 and 0.84, with the four factors explaining 49 per cent of the total variance. Eigenvalues between 6.3 and 0.18 were obtained, with five eigenvalues greater than 1. The final sorted rotated factor loading matrix is set out in Table 7.14.

[2] When an item is correlated with the total score of which it is part, the value of the r_{it} tends to be inflated and there is a need for correction (Guilford, 1954:439).

Table 7.14 Sorted four-factor loading matrix

Item	Factor 1 Privacy protection	Factor 2 Misuse	Factor 3 Solicitation	Factor 4 Government protection
Q39 (PP3)	**0.755**	-0.018	-0.130	0.020
Q32 (BI1)	**0.717**	0.018	-0.014	-0.050
Q45 (PP5)	**0.674**	-0.090	0.037	0.034
Q41 (BI4)	**0.641**	-0.072	0.009	0.114
Q44 (BI5)	**0.628**	0.053	-0.023	-0.097
Q36 (PP2)	**0.619**	-0.079	0.007	0.221
Q38 (BI3)	**0.611**	0.006	0.063	0.158
Q20 (DD2)	**0.602**	0.137	-0.035	-0.012
Q33 (PP1)	**0.541**	0.032	0.181	-0.048
Q19 (DD1)	0.026	**0.843**	-0.033	-0.091
Q17 (DU5)	-0.047	**0.788**	-0.007	0.029
Q15 (DU3)	-0.025	**0.728**	-0.009	0.007
Q18 (DU6)	0.124	**0.664**	-0.016	0.034
Q21 (DD3)	0.010	**0.606**	0.021	-0.030
Q12 (DS6)	-0.005	**0.576**	0.039	0.131
Q11 (DS5)	-0.060	**0.549**	0.053	0.025
Q26 (SOL2)	-0.017	0.067	**0.762**	0.160
Q30 (SOL6)	-0.103	-0.042	**0.644**	-0.023
Q25 (SOL1)	-0.004	0.101	**0.721**	0.153
Q29 (SOL5)	-0.012	-0.066	**0.607**	0.038
Q28 (SOL4)	0.083	0.030	**0.541**	-0.121
Q27 (SOL3)	0.106	0.091	**0.540**	-0.073
Q40 (LEG4)	0.072	0.048	0.016	**0.810**
Q37 (LEG3)	0.062	0.081	-0.030	**0.804**
Q34 (LEG2)	0.018	0.009	0.040	**0.786**

Finally, Cronbach's coefficient alpha was used to assess the internal consistency or reliability of the construct indicators. Values ranged between 0 and 1, with higher values indicating higher reliability among the indicators. A lower limit of 0.70 was set for Cronbach's alpha, as suggested by Nunnally (1978:103). The reliability results of the item analysis and Cronbach's alpha are summarised in Table 7.15.

Table 7.15 Summary of item analysis and Cronbach's alpha

Scale	Items	Item-to-total correlation	Cronbach's alpha after deletion	Reliability
Privacy protection	Q20	0.571	0.861	0.87
	Q32	0.664	0.855	
	Q33	0.510	0.867	
	Q36	0.631	0.855	
	Q38	0.624	0.856	
	Q39	0.679	0.852	
	Q41	0.604	0.857	
	Q44	0.548	0.864	
	Q55	0.600	0.857	
Information misuse	Q11	0.552	0.853	0.86
	Q12	0.614	0.845	
	Q15	0.652	0.838	
	Q17	0.703	0.831	
	Q18	0.623	0.842	
	Q19	0.728	0.827	
	Q21	0.530	0.855	
Solicitation	Q25	0.643	0.774	0.81
	Q26	0.667	0.768	
	Q27	0.538	0.797	
	Q28	0.531	0.798	
	Q29	0.516	0.802	
	Q30	0.586	0.787	
Government protection	Q34	0.729	0.837	0.87
	Q37	0.754	0.815	
	Q40	0.773	0.797	

From Table 7.15 it is evident that all the Cronbach's alpha coefficients of the underlying dimensions were above the recommended cut-off value of 0.70, with values ranging between 0.81 and 0.87, and it can therefore be concluded that the four derived scales are reliable.

The four factors are discussed individually below.

7.4.1.2 Factor 1: Privacy protection

Several items loaded on the first factor. All items (except for one relating to data disclosure) pertained to either the behavioural intentions of consumers to protect their

privacy, or privacy policies of organisations regarding data collection, storage, use, disclosure and solicitation. Table 7.16 provides detail on the privacy protection factor.

Table 7.16 Items and loadings for Factor 1 (Privacy protection)

Item	Question	Factor loading
PP3	Companies should have privacy protection policies indicating the reasons for collecting personal information from consumers.	0.755
BI1	You would request a company to remove your personal information from their records if you suspected that they were misusing it.	0.717
PP5	Companies should have privacy protection policies indicating how they will protect the customer's information while it is in their possession.	0.674
BI4	You would support a company's efforts that will ensure that your personal information is safely kept.	0.641
BI5	You would refuse to provide your personal information to a company who cannot provide reasons why they want to collect your personal information.	0.628
PP2	Companies should have privacy protection policies indicating that no personal information will be provided to other companies without consent from their customers.	0.619
BI3	You would request having your personal information removed from any company's records if they sell the information to others.	0.611
DD2	You are uncomfortable when companies share your personal information with other companies without asking your permission first.	0.602
PP1	Companies must have privacy protection policies to make provision for customers who would not like to receive unrequested advertising material.	0.541

These privacy protection behaviour or policies covered general privacy issues ranging from concerns about the sharing of personal information with third parties, to the reasons for collecting information from consumers and the safekeeping of information by companies.

7.4.1.3 Factor 2: Information misuse

The second factor, labelled 'information misuse', included five items relating to how companies use or misuse personal information, as well as two safety concern items. Table 7.17 indicates the factor loadings of the seven items that constituted Factor 2.

Table 7.17 Items and loadings for Factor 2 (Information misuse)

Item	Question	Factor loading
DD1	Companies regularly share personal information with other companies without the permission of the individuals to whom the information belongs.	0.843
DU5	You believe that consumers' personal information is often misused by companies.	0.788
DU3	You believe that companies regularly use consumers' information for other purposes than that for which it was collected.	0.728
DU6	You are concerned about the possible misuse of your personal information by companies.	0.664
DD3	You believe that companies regularly share personal information of consumers with other companies, so that these other companies could offer products and services to consumers.	0.606
DS6	You fear that your personal information may not be safe while stored in a company's records.	0.576
DS5	Personal information is safe while stored in a company's records.	0.549

The two safety concern items (see DS6 and DS5 in Table 7.17) were seen as related to information misuse, because it can be argued that when a consumer's information is not safe while stored in a company's records, it opens up opportunities for misuse.

7.4.1.4 Factor 3: Solicitation

Privacy often relates to the right to be left alone, and to be free from intrusion or interruption. One of the privacy concerns of individuals seems to be media intrusiveness because consumers have little or no control over the prospecting efforts of organisations. Table 7.18 contains detail on the items that loaded on Factor 3.

Table 7.18 Items and loadings for factor 3 (Solicitation)

Item	Question	Factor loading
SOL2	It bothers you that you receive so much unrequested advertising material that is of no interest to you.	0.762
SOL1	Companies send consumers too much unrequested advertising material that is not of interest to them.	0.721
SOL6	You are pleased when you receive information about new products and services from companies with which you have not done business before.	0.644
SOL5	Consumers are not interested in getting information about new products and services from companies with which they have not done business before.	0.607
SOL4	You do not mind when you receive telephone calls at your home from companies wanting to sell products and services to you.	0.541
SOL3	Too many companies call consumers at their homes to sell products and services to them.	0.540

The sheer volume of direct mail, telemarketing and e-mails relates to the physical intrusion of marketing communications in the daily lives of consumers. The results indicate that South African consumers share solicitation concerns because the third factor contained all six items relating to solicitation.

7.4.1.5 Factor 4: Government protection

The last factor is labelled 'government protection', because only items relating to the role of government in protecting information privacy by means of legislation loaded significantly on this factor. Table 7.19 provides the factor loadings for the three items relating to government protection.

Table 7.19 Items and loadings for Factor 4 (Government protection)

Item	Question	Factor loading
LEG4	Government should limit companies' use of personal information to only that purpose for which it was collected.	0.810
LEG3	Government should do more to protect the safety of personal information.	0.804
LEG2	Government should restrict companies to collecting only the information needed for a specific transaction.	0.786

It is clear that the optimal solution, based both on interpretability and statistical measures, was formed by a four-factor model. As mentioned earlier, the exploratory factor analyses were conducted on one half of the sample. The next step is to use the remaining half of the sample to validate the four-factor model by using confirmatory factor analysis.

7.4.2 Confirmatory factor analysis

Confirmatory factor analysis (CFA) is the predominant method of analysis found in the literature concerning validation studies, particularly when validating the internal factor structure of a newly developed test instrument (Steenkamp & Van Trijp, 1991:283; Hair *et al.*, 1998:114, 247; Burgers *et al.*, 2000:154; Ferrara, 2000:102). Confirmatory factor analysis can be used to test the structure of a model that is identified using exploratory factor analysis. It is important to use a different set of data when testing the validity of the factor model identified by exploratory factor analysis (Hair *et al.*, 1998:114; Lattin *et al.*, 2003:199). Therefore, as mentioned earlier, the sample was split in half using the one half to derive a scale, and using the other half of the sample to confirm the earlier results.

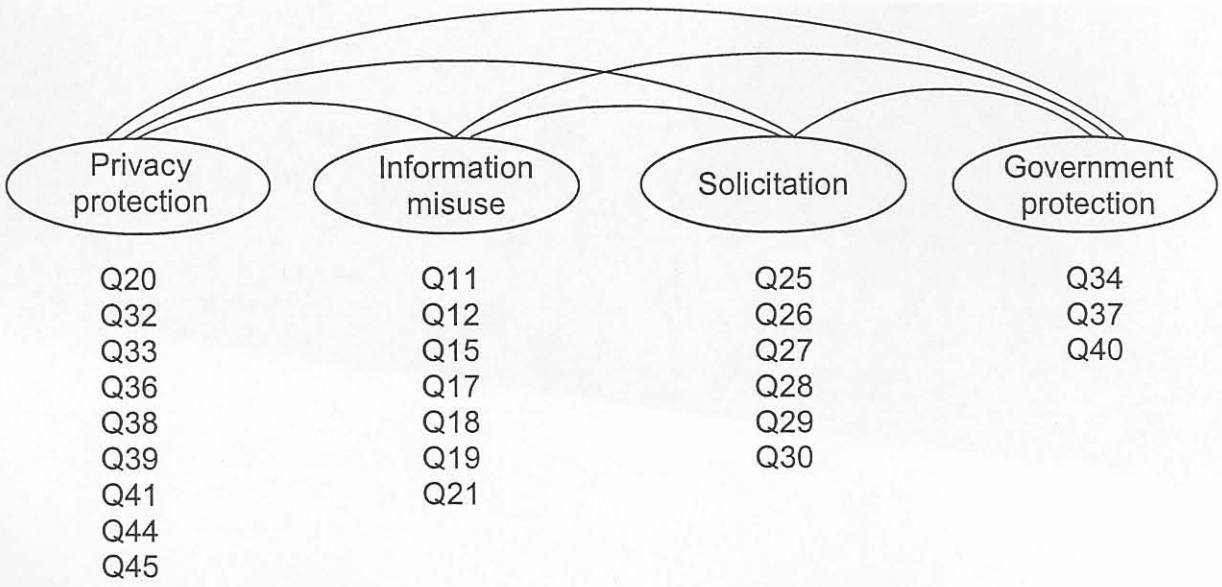
Two assumptions that underlie traditional Structural Equation Modeling programmes are (a) that the variables on which the matrix coefficients are based are intervally scaled, and (b) that the variables have a multivariate normal distribution. The first assumption, namely the scale requirement, was met since all items were measured using 5-point Likert scales. The second assumption, the normality requirement, is often difficult to comply with. The maximum likelihood estimation technique was therefore used for analysis because this technique is relatively robust with regard to violation of normality (Grimm & Yarnold, 2000:233). The data were also examined for any outliers before they were converted to matrix format, and no outliers were found in the dataset. Maximum likelihood estimation was used with the aid of the SAS Proc Calis programme (SAS Institute, 2000b) to execute the confirmatory factor analysis.

7.4.2.1 The theoretically based model converted into a path diagram for CFA

The previously discussed factor analysis indicated the existence of four factors (indicating four underlying dimensions). Therefore, the hypothesised model posited four factors (privacy protection, information misuse, solicitation and government protection), with each set of variables acting as indicators of the separate constructs (or factors).

The next stage was to portray the relationships in a path diagram. In this case, the four hypothesised factors were considered exogenous constructs. From here on forward, each 'factor' identified by the exploratory factor analysis is referred to as a 'construct'. The path diagram, including the variables measuring each construct, is shown in Figure 7.3. The correlations between the different concerns are represented by the curved lines connecting the four constructs.

Figure 7.3 Path diagram for CFA



All the constructs in the path diagram were exogenous, and therefore only the measurement model and the associated correlation matrices for exogenous constructs

and indicators needed to be considered. Without a structural model, the measurement model constitutes the entire structural equation modeling effort (referred to as confirmatory factor analysis). To specify the measurement model, a transition was made from factor analysis, where there was no control over which variables described each factor, to confirmatory analysis, where the variables that define each factor can be defined (Hair *et al.*, 1998:598).

The objective of the CFA is an exploration of the pattern of interrelationships. The correlation matrix was therefore used as the input data type. No offending estimates were found for the measurement model and no corrections were needed before the model could be interpreted and the goodness-of-fit assessed.

7.4.2.2 Determining overall model fit

The first assessment of model fit must be done for the overall model (Hair *et al.*, 1998:621). With confirmatory factor analysis, overall model fit portrays the degree to which the specified indicators represent the hypothesised constructs. By applying numerous tests of fit, the proximity of fit between the data and the model can be assessed. Model fit determines the degree to which the structural equation model fits the sample data. Model fit criteria commonly used are chi-square (χ^2), goodness-of-fit index (GFI), adjusted goodness-of-fit index (AGFI) and root-mean-square residual (RMR) (Schumacker & Lomax, 1996:124). Because some of the fit indices evaluate different aspects of fit, it is important to evaluate fit based on multiple fit statistics so that judgments will not be an artifact of analytic choice. Assessment of model adequacy must be based on multiple criteria that take into account theoretical, statistical and practical considerations (Grimm & Yarnold, 2000:271). The fit indices that were used to assess the overall model fit for the present study are discussed below.

(a) Chi-square (χ^2)

The overall model fit provided by the χ^2 value is often used as the first step in evaluating model acceptance or rejection (Baumgartner & Homburg, 1996:152). The χ^2 statistic in

isolation is not a meaningful statistic without taking into account the degrees of freedom (df) of a model (Baumgartner & Homburg, 1996:152). CFA researchers also advocate a χ^2/df ratio as an initial start to model acceptence (Schumacker & Lomax, 1996:125; Spangenberg & Theron, 2002:19). A significant χ^2 value relative to the degrees of freedom indicates that the observed and estimated matrices differ. Statistical significance indicates the probability that this difference is due to sampling variation. A non-significant χ^2 value indicates that the two matrices are not statistically different. In this study, a non-significant χ^2 value with associated degrees of freedom was sought. The χ^2 criterion is, however, sensitive to sample size. If the sample size increases (generally above 200), the χ^2 test has a tendency to indicate a significant probability level (Schumacker & Lomax, 1996:125). Because the chi-square test is sensitive to sample size (the sample size for the current study is 313) and can lead to a rejection of a model differing in a trivial way from the data for large sample sizes, it is prudent also to examine other measures of fit (Bagozzi & Heatherton, 1994:45; Baumgartner & Homburg, 1996:149; Ferrara, 2000:106). Thus, a comparison of the GFI, AGFI and RMR measures, which are independent of sample size, was performed to assess the model's fit (Smith *et al.*, 1996:177).

(b) Goodness-of-fit (GFI) and Adjusted Goodness-of-fit (AGFI)

The GFI is based on a ratio of the sum of the squared differences between the observed and reproduced matrices to the observed variances, thus allowing for scale (Schumacker & Lomax, 1996:126). The AGFI adjusts the GFI index for the degrees of freedom of a model relative to the number of variables. The advantage of GFI and AGFI is that they are scales between zero (poor fit) and 1 (perfect fit) and are not a function of sample size. One rule of thumb is that for a good fit, GFI should exceed 0.95 and for an acceptable fit, GFI should exceed 0.90. Similarly, a model with a good fit should have an AGFI value greater than 0.90, and a model with acceptable fit should have an AGFI greater than 0.80 (Lattin *et al.*, 2003:182). Most researchers expect values to be greater than 0.90 for correctly specified models (Hair *et al.*, 1998:657; Grimm & Yarnold, 2000:270).

(c) Root-mean-square residual (RMR)

The RMR index uses the square root of the mean of the squared residuals which is an average of the residuals between observed and estimated input matrices (Schumacker & Lomax, 1996:126). Ideally, RMR should be near zero for a good model fit (Ferrara, 2000:106). Values of 0.05 or less are regarded as indicative of a model that fits the data well (Grimm & Yarnold, 2000:270; Spangenberg & Theron, 2002:19).

(d) Root mean square error of approximation (RMSEA)

RMSEA is another measure that attempts to correct for the tendency of the chi-square statistic to reject any specified model with a sufficiently large sample (Hair *et al.*, 1998:656). RMSEA expresses the difference between the observed and estimated covariance matrices in terms of the degrees of freedom of the model, and is a fit index that focuses on estimated population fit. An empirical examination of several measures has found that the RMSEA was best suited to use in a confirmatory strategy with larger samples (Hair *et al.*, 1998:656). Although rarely encountered, RMSEA values below 0.01 would indicate a model that fits the data exceptionally well, since values approaching zero are desired. Different RMSEA cut-off values have been suggested: some consider values below 0.05 to indicate a very good fit (Spangenberg & Theron, 2002:19); others indicate that values between 0.05 and 0.08 are indicative of acceptable fit (Baumgartner & Homburg, 1996:152; Hair *et al.*, 1998:656; Grimm & Yarnold, 2000:271). Hu and Bentler (1999:1) suggest a cut-off value close to 0.06 for RMSEA before one can conclude that there is a relatively good fit.

(e) Bentler & Bonnet's normed fit index (NFI) and the comparative fit index (CFI)

NFI compares model fit to that of a model for the same data presuming independence of the measured or observed variables. It is one of the more popular measures ranging from 0 (no fit at all) to 1 (perfect fit). There is no absolute value indicating an acceptable level of fit, but a commonly recommended value is 0.90 or greater (Hair *et al.*, 1998:657; Maruyama, 1998:244; Grimm & Yarnold, 2000:270). NFI tends to underestimate when small samples are used and an adjustment was proposed to the NFI, namely the comparative fit index (CFI), which takes sample size into account. Some researchers

have suggested that the CFI should be a fit statistic of choice in structural equation modeling research (Grimm & Yarnold, 2000:270). The proposed cut-off value for CFI is close to 0.95 (Hu & Bentler, 1999:1).

The different fit indices for this study's overall model fit are reported in Table 7.20.

Table 7.20 Fit indices for the overall model fit

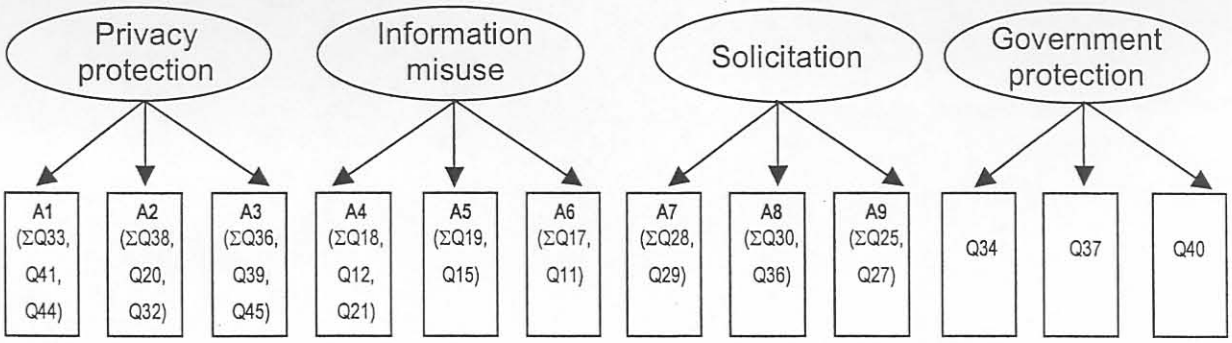
Chi-square/df	(789.9013/269) p<0.0001
Goodness of fit index (GFI)	0.83
Adjusted goodness of fit index (AGFI)	0.79
RMR	0.07
RMSEA	0.08
CFI	0.84
NFI	0.78

From Table 7.20 it is evident that several of the fit indices (χ^2, GFI, AGFI, RMR, CFI and NFI) were below the suggested cut-off values as suggested by various researchers (as discussed above). Bagozzi and Heatherton (1994:47) indicate that when more than five items per factor are treated as individual measures of factors in a multifactor CFA, it is difficult to achieve a satisfactorily fitting model and the indices obtained from confirmatory factor analysis could be an underestimate of the model fit values. Their view has been supported by several other researchers, such as Baumgarter and Homburg (1996:144), who believe that it is practically unavoidable that one has to combine items into composites if the number of indicators is even moderately larger, for example, ten items. Hair *et al.* (1998: 598) have confirmed that researchers are not likely to obtain good results from structural equation modeling (SEM) with models that have more than 20 measures.

As a solution to this problem, Bagozzi and Heatherton (1994:47) have proposed the calculation of item aggregates to obtain more accurate estimates of model fit indices. When the number of items per construct is relatively small (five to seven items), it seems prudent to form two composites for each construct in which each composite is a sum of items. When nine or more items exist per construct in a scale, it is feasible to

form three or more composites as indicators for each construct. In the present study, the four-factor solution contained 25 items. It was decided to use item pairing to form composite variables for three of the four constructs to minimise the instability of the parameter estimates (Ferrara, 2000:105). Composites were achieved in this dataset by randomly selecting items within a specific factor to be paired with another item of the same factor, resulting in a total of nine composite variables or item pairs. Figure 7.4 illustrates the composites formed from the individual items for each of the constructs.

Figure 7.4 Item pairing to form composites



A minimum of three composites was formed for each construct. Several researchers recommend that each construct be assessed using a minimum of three indicators (or items) each (Baumgarter & Homburg, 1996:144; Hair *et al.*, 1998:598). Three of the four constructs were each represented by three item pairs (consisting of two or three items each). From Figure 7.4 it can be observed that A1 to A3 represented the three item pairs of general privacy; A4 to A6 item pairs represented misuse; and A7 to A9 represented solicitation. Because government protection consisted of only three indicators, there was no need to form item pairs for this construct as well.

The item pairing resulted in a reduction of the number of items from 25 to 12. After the composites had been formed, the overall model was assessed again and the fit indices are shown in Table 7.21 below.

Table 7.21 Fit indices for overall model fit (containing composites)

Chi-square/df	(104.2686/49) p=0.0000
Goodness of fit index (GFI)	0.95
Adjusted goodness of fit index (AGFI)	0.92
RMR	0.04
RMSEA	0.06
CFI	0.97
NFI	0.94

From Table 7.21 it is clear that these fit values differ from the values presented in Table 7.20 before composites were formed. The fit indices depicted in Table 7.21 indicate that all the values are within the accepted cut-off levels, demonstrating a very good fit for the overall four-factor model. The only value that did not show an acceptable fit was the chi-square value. The chi-square measure was highly significant [χ^2 (49) = 104.2686; p=0.0000] indicating a poor model fit. However, given the large sample size, the significant chi-square was probably an artifact of sample size (refer to Section 7.3.2.2) and should be interpreted as such.

7.4.2.3 Determining the measurement model fit

The different constructs can now be evaluated by assessing each construct's validity. Construct validity is the one type of validity that has received great attention over the years and is consequently the one with the best developed technology for assessment (Steenkamp & Van Trijp, 1991:287; Smith *et al.*, 1996:178; Hair *et al.*, 1998:118; Burgers *et al.*, 2000:155). The following criteria were used to assess construct validity for this study: unidimensionality, reliability, convergent validity and discriminant validity.

(a) Unidimensionality

Unidimensionality can be defined as the existence of one construct underlying a set of items, and has been recognised as one of the critical and basic assumptions of measurement theory (Hattie, 1985:139). In this study, unidimensionality refers to each of the factors separately where each item is related to one factor. The overall fit of the model provides the necessary and sufficient information to determine whether a set of

items is unidimensional (Kumar & Dillon, 1987:100). The good model fit (GFI=0.95, AGFI=0.92, CFI=0.97, and RMSEA=0.06) indicates that the scale is unidimensional. Other researchers believe that unidimensionality is obtained when an item loads on only one construct and when only high loading items are selected (Steenkamp & Van Trijp, 1991:286). In this survey, items that did not load on only one factor were deleted, and only items loading higher than 0.50 were selected, demonstrating unidimensionality of the construct.

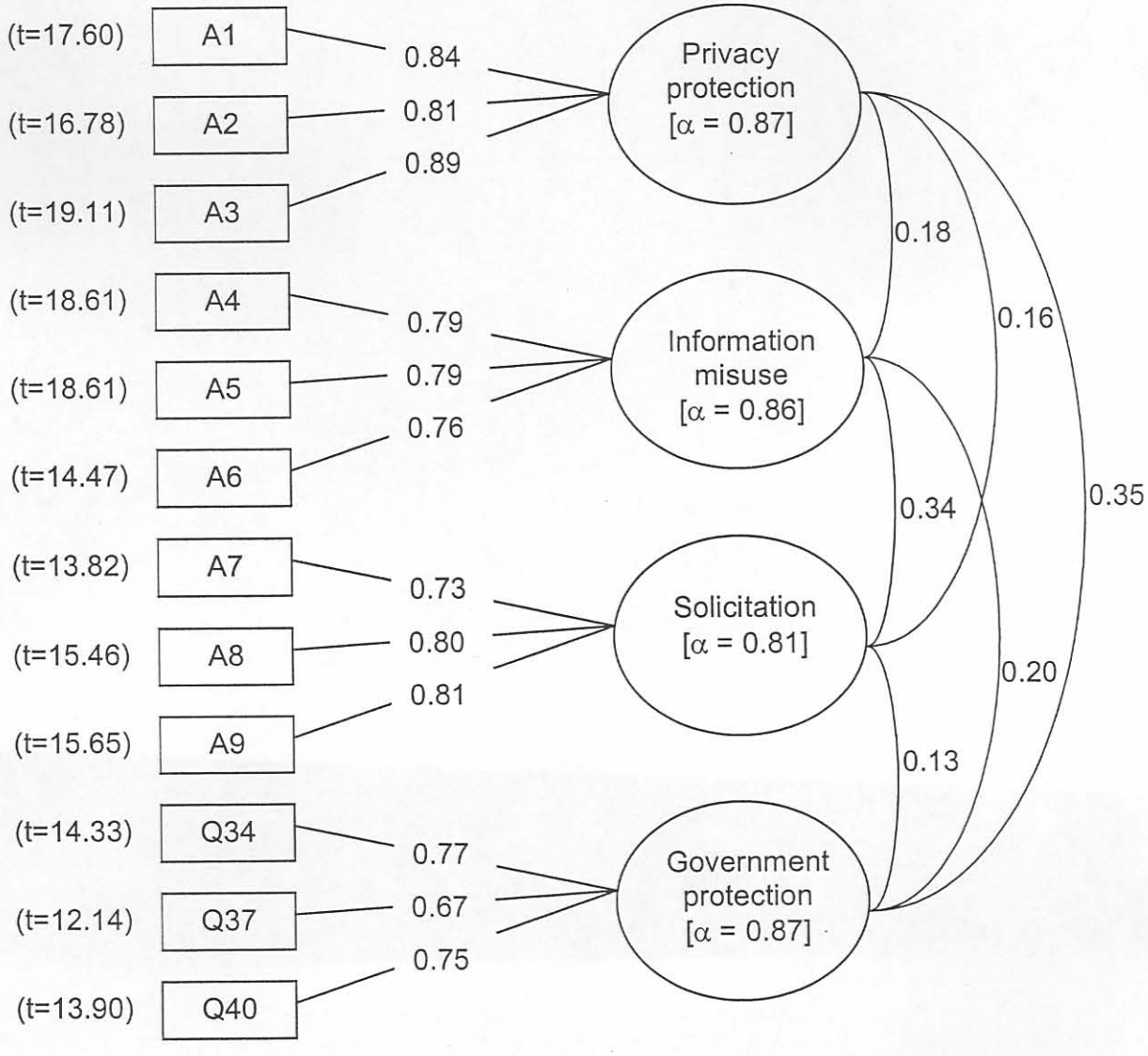
(b) Convergent validity

Convergent validity is demonstrated when a measure has relatively high correlations with other measures of the same common factor. Thus, convergent validity assesses the degree to which two measures of the same concept are correlated. High correlations indicate that the scale is measuring its intended concept (Hair *et al.*, 1998:118). Convergence implies that all within-construct correlations are both high and of approximately the same magnitude (Steenkamp & Van Trijp, 1991:290). According to Anderson and Gerbing (1988:414), within-method convergent validity should be achieved before reliability is estimated.

There are several approaches to the assessment of convergent validity through CFA. The statistical significance of the regression coefficient, the correlation of the item with the construct, as well as the overall fit of the model are all indicators of within-method convergent validity (Hildebrandt, 1987:35; Steenkamp & Van Trijp, 1991:289; Smith *et al.*, 1996:181; Burgers *et al.*, 2000:155). Within-method convergent validity was first assessed by testing the significance and magnitude of each indicator's coefficient. Each variable's *t* value was investigated in terms of how its loading exceeded the critical values at the 0.05 significance level (critical value 1.96) as well as the 0.01 significance level (critical value 2.576). All the *t* values were well above 1.96 and 2.57 (see Figure 7.5). The magnitude of the items was then assessed. Hildebrandt (1987:35) suggests in respect of the latter criterion that the correlation between the item and the construct (or factor) should exceed 0.50. All items loaded significantly higher than 0.70 on their respective constructs, except for one item that loaded 0.67. Thus, all variables are

significantly related to their specified constructs, verifying the posited relationships between indicators and constructs. The significance and magnitude of the items can be seen in Figure 7.5.

Figure 7.5 Significance and magnitude of items in the CFA model



The afore-mentioned conditions (statistical significance of the regression coefficient and the correlation of the item with the construct) should be evaluated, provided that a third requirement of convergent validity is met, namely that the overall fit of the model is acceptable (Steenkamp & Van Trijp, 1991:289). As reported earlier, a good overall

model fit was obtained. All these findings support the convergent validity of the information privacy scale.

(c) Reliability

Another method to assess construct validity is to estimate the reliability (Steenkamp & Van Trijp, 1991:290; Burgers *et al.*, 2000:155) and variance-extracted measures (Hair *et al.*, 1998:611; Smith *et al.*, 1996:185) for each construct to assess whether the specified indicators are sufficient in their representation of the constructs. As mentioned previously, all four constructs exceeded the recommended reliability level of 0.70 (0.88, 0.82, 0.83 and 0.77), indicating an adequate reliability for the four scales (Hair *et al.*, 1998:623).

Another measure of reliability is the variance-extracted measure. The average variance extracted is the sum of the squared standardised loading divided by the sum of the squared standardised loadings plus the sum of the indicator measurement error. This measure reflects the overall amount of variance in the indicators accounted for by the latent construct. Higher variance extracted values occur when the indicators are truly representative of the latent construct. Guidelines suggest that the variance-extracted values should exceed 0.50 for a construct (Hair *et al.*, 1998:612). For the variance-extracted measures, all four constructs exceeded the recommended 50 per cent with values of 0.72, 0.61, 0.61 and 0.53. Thus, the explained variance by each factor is significantly higher than the variance due to measurement error, indicating adequate convergent validity for each factor (Fornell & Larcker, 1981:42). Table 7.22 depicts the values for Cronbach's alpha as well as the average variance extracted (AVE).

Table 7.22 Summary of reliability values

FACTORS	Cronbach's alpha	AVE*
General privacy	0.87	0.72
Misuse	0.87	0.61
Solicitation	0.86	0.61
Government protection	0.82	0.53

* Appendix 6 contains details on the calculation of the average variance extracted.

(d) Discriminant validity

Discriminant validity is determined by demonstrating that a measure does not correlate very highly with another measure from which it should differ (Peter, 1981:136), or must have lower correlations with measures of different factors (Zikmund, 2003:304; Hair *et al.*, 1998:118). If the correlations are too high, this suggests that the measure does not capture a distinct or isolated trait (Peter, 1981:137; Churchill & Iacobucci, 2002:413). Discriminant validity is evident in several ways (Cole, Cho & Martin, 2001:94). The first involves cross-loadings in the factor analysis. In none of these analyses was a measure allowed to load on any factor other than the one it was designed to represent. The model also provided a good fit to the data without allowing such cross-loadings. More rigorous evidence of discriminant validity is also evident by observing the average variance extracted by each factor relative to that factor's shared variance with other factors in the model (Fornell & Larcker, 1981:41). Table 7.23 provides the factor intercorrelations of the four-factor model.

Table 7.23 Factor intercorrelations of the four-factor model

FACTORS	General privacy	Misuse	Solicitation	Government protection	AVE
General privacy	1.00				0.88
Misuse [squared correlation]	0.188 [0.035]	1.00			0.82
Solicitation [squared correlation]	0.160 [.025]	0.338 [0.114]	1.00		0.83
Government protection [squared correlation]	0.351 [0.123]	0.201 [0.040]	0.131 [0.017]	1.00	0.77

In every case, the average variance extracted (AVE) associated with a factor is greater than the shared variance (squared correlation) between that factor and every other factor. It is clear from Table 7.23 that the AVE's are all greater than the squared correlations between a factor and every other factor. This is also indicative of the existence of discriminant validity.

The results from all the relevant analyses provided support for the validation of the proposed model. Confirmatory factor analysis were used to assess the unidimensionality, reliability, and validity of the scale (Steenkamp & Van Trijp, 1991:283). The overall model goodness-of-fit results and the measurement model assessments lent substantial support for confirmation of the proposed four-factor model.

7.5 HYPOTHESES TESTING

The process of hypotheses testing was conducted as follows: first, statistical hypotheses were determined by formulating null and alternative hypotheses (as set out in Chapter 5). The next step was to specify the circumstances under which H_0 would or could not be rejected, by choosing a level of significance. A significance level is a critical probability in choosing between the null hypothesis and the alternative hypothesis. A five per cent significance level (α=0.05) was set for all hypotheses. Thereafter an appropriate statistical technique with a corresponding test statistic was chosen. Finally, the values of the test statistics were calculated, the test results interpreted and a decision was made to reject or not reject the null hypotheses. All the significant results are indicated in bold print.

All the hypotheses that were tested with the same statistical technique are discussed in the same section. This means that the hypotheses do not necessarily follow a chronological order. The following section provides detailed results for the hypotheses testing based on the above-mentioned principles.

7.5.1 Testing hypotheses using chi-square tests

Hypotheses 2b, 3b, 3c and 6 were tested by means of chi-square (χ^2) tests. In H_{2b} and H_{3b}, two groups were compared on a variable measured on a nominal scale and were therefore tested with the two-sample chi-square test for independency (Sections 7.4.1.1 and 7.4.1.2). H_{3c} was tested with the k-sample chi-square test for independency (an extension of the two-sample chi-square test) because comparisons were made between

The results from all the relevant analyses provided support for the validation of the proposed model. Confirmatory factor analysis were used to assess the unidimensionality, reliability, and validity of the scale (Steenkamp & Van Trijp, 1991:283). The overall model goodness-of-fit results and the measurement model assessments lent substantial support for confirmation of the proposed four-factor model.

7.5 HYPOTHESES TESTING

The process of hypotheses testing was conducted as follows: first, statistical hypotheses were determined by formulating null and alternative hypotheses (as set out in Chapter 5). The next step was to specify the circumstances under which H_0 would or could not be rejected, by choosing a level of significance. A significance level is a critical probability in choosing between the null hypothesis and the alternative hypothesis. A five per cent significance level (α=0.05) was set for all hypotheses. Thereafter an appropriate statistical technique with a corresponding test statistic was chosen. Finally, the values of the test statistics were calculated, the test results interpreted and a decision was made to reject or not reject the null hypotheses. All the significant results are indicated in bold print.

All the hypotheses that were tested with the same statistical technique are discussed in the same section. This means that the hypotheses do not necessarily follow a chronological order. The following section provides detailed results for the hypotheses testing based on the above-mentioned principles.

7.5.1 Testing hypotheses using chi-square tests

Hypotheses 2b, 3b, 3c and 6 were tested by means of chi-square (χ^2) tests. In H_{2b} and H_{3b}, two groups were compared on a variable measured on a nominal scale and were therefore tested with the two-sample chi-square test for independency (Sections 7.4.1.1 and 7.4.1.2). H_{3c} was tested with the k-sample chi-square test for independency (an extension of the two-sample chi-square test) because comparisons were made between

more than two groups (Section 7.4.1.3). The null hypotheses tested by the chi-square tests for independence was that there is no difference between the groups in respect of the relative frequency with which group members belonged to the various categories of the variables of interest. The reason for focusing on relative rather than absolute frequencies was that the groups had unequal sample sizes and, therefore, the calculation of expected frequencies needed to take this into account, as suggested by Diamantopoulos and Schlegelmilch (1997:175). With a 2x2 table (as is the case with H_{2b} and H_{3b}), it is often recommended that Yates's correction for continuity be applied to obtain a modified chi-square statistic (Diamantopoulos & Schlegelmilch, 1997:177). This is designed to correct or compensate for what some researchers regard as an overestimate of the chi-square value when used with a 2x2 table. Yates' correction for continuity is reported in both H_{2b} and H_{3b} (see Sections 7.4.1.1 and 7.4.1.2). H_6 was tested by means of the chi-square goodness-of-fit test. Here the 'goodness of fit' of the observed distribution with the expected distribution was tested. The null hypothesis under the chi-square goodness-of-fit test was that the observed frequencies were equal to the theoretical frequencies. With the testing of H_6, the expected frequencies were all specified to be the same (see discussion in Section 7.4.1.4).

Two assumptions underlie chi-square tests (Diamantopoulos & Schlegelmilch, 1997:180; Keller & Warrack, 2000:557). First, the observations must originate from a random sample and the scores associated with the observation must be independent from each other. The second assumption is that the sample size must be relatively large so that a minimum expected cell frequency can be obtained. There is no simple answer to the question of what sample size is large enough, but many researchers suggest that at least 80 per cent of the cells should have an expected frequency greater than or equal to 5, and that no cell should have an expected frequency smaller than 1 (Diamantopoulos & Schlegelmilch, 1997:180; Green, Salkind & Akey, 1999:346; Pallant, 2001:257). The data did not violate any of the stated assumptions. The results for the first four hypotheses are presented below.

7.5.1.1 *H_{2b}: There is a dependency between being a victim of invasion of privacy and gender*

Hypothesis 2b attempted to find support that there are differences between gender groups in terms of their privacy invasion experiences. Results from previous international studies had indicated that men seemed to be more likely than women to report being a victim of privacy invasion (refer to Chapter 5, Section 5.4.2). The result of the two-sample chi-square for the data in this study is illustrated in Table 7.24.

Table 7.24 Difference between gender and victims of privacy invasion

VICTIMS OF INVASION GENDER		Victim of privacy invasion	Not a victim of privacy invasion	ROW TOTAL	
Male	Frequency Row %	89 38	148 62	237	
Female	Frequency Row %	107 27	283 73	390	
COLUMN TOTAL		196	431	627	
p-value					**0.0104**

The specified significance level of 5 per cent resulted in a corrected p-value of 0.0104 (Yates's correction for continuity), **leading to a rejection of the null hypothesis**. There was support for H_{2b}, indicating that there is a difference between the number of privacy invasions reported between men and women. To establish what percentage of males versus females reported being a victim of privacy invasion, the row percentages needed to be interpreted. From Table 7.24, it can be deduced that 38 per cent of males were victims of privacy invasion, while 62 per cent were not victims. For females, 27 per cent reported being a victim, versus 73 per cent that were not victims. This indicates that males are more likely to perceive themselves as victims of privacy invasion (38% versus 27%). This result corresponds with findings from previous studies which indicated that **males seem to be more likely than females to perceive themselves as victims of privacy invasion**.

7.5.1.2 *H_{3b}: There is a dependency between the level of awareness of name removal procedures and age*

There is sufficient evidence in previous literature to suggest that there are differences between lower and higher age groups in terms of their awareness of name removal procedures (refer to Chapter 5, Section 5.4.3). Hypothesis 3b was formulated to seek support for age differences of consumers in terms of their knowledge of name removal procedures. Question 61 in the questionnaire (see Appendix 1) requested respondents to provide their year of birth as a 4-digit number, for example 1969. Answers to this question, based on the frequencies, were categorised into two distinct age groups, namely a younger age group (18-39 years) and an older age group (40+ years). The result of the chi-square test comparing younger and older consumers in terms of their awareness of name removal procedures is presented in Table 7.25.

Table 7.25 Difference between age groups and awareness of name removal procedures

AWARENESS OF NAME REMOVAL / AGE GROUPS		Aware of name removal procedures	Not aware of name removal procedures	ROW TOTAL	
18-39 years	Frequency	64	215	279	
	Row %	23	77		
40+ years	Frequency	80	266	346	
	Row %	23	77		
COLUMN TOTAL		144	481	625	
p-value					1.0000

Since the corrected p-value (Yates's correction for continuity) was larger than the specified significance level of 5 per cent, the null hypothesis could not be rejected. There was thus **not enough empirical support for H_{3b} to suggest that the level of awareness of name removal procedures is dependent on age.** For both groups, a total of 77 per cent of the consumers were unaware that they can remove their names from some of the major contact lists in the country as a means to protect their privacy.

7.5.1.3 *H_{3c}: There is a dependency between the awareness of name removal procedures and levels of education*

Hypothesis 3c was formulated on the basis of evidence from previous studies which had found that consumers who are aware of name removal procedures are often better educated than those who are not aware of name removal procedures (refer to Chapter 5, Section 5.4.3). Answers to question 63 in the questionnaire (see Appendix 1) were regrouped to form three different educational groups, namely low, medium and high levels of education. Table 7.26 presents the result of the chi-square test indicating the differences between the groups with low, medium and high educational levels in terms of their awareness of name removal procedures.

Table 7.26 Difference between education levels and awareness of name removal procedures

AWARENESS OF NAME REMOVAL PRODECURES / EDUCATION LEVELS		Aware of name removal procedures	Not aware of name removal procedures	ROW TOTAL	
Low educational level (Up to Grade 10)	Frequency	35	119	154	
	Row %	23	77		
Medium educational level (Up to Grade 12)	Frequency	54	179	233	
	Row %	23	77		
High educational level (Post Grade 12 qualification)	Frequency	56	182	238	
	Row %	24	76		
COLUMN TOTAL		145	480	625	
p-value					0.9832

The p-value indicates that the null hypothesis cannot be rejected as the results provide no support for H_{3c}. From this non-significant p-value, one can conclude that **there is no relationship between educational levels and awareness of name removal procedures**. This result differs from that of previous studies where more highly educated consumers were more aware of name removal procedures than less educated consumers.

7.5.1.4 H_6: The proportion of South African consumers is not equally represented in the different privacy segments

Based on the Privacy Segmentation Index designed by Westin and Louis Harris & Associates (Harris Interactive, 2002b:20), respondents were categorised into one of three segments, depending on their degree of agreement of disagreement with three questions (refer to Chapter 5, Section 5.4.6). Appendix 1 includes Questions 46 to 48 used in this analysis. Respondents who 'strongly agreed' or 'slightly agreed' with Question 46, and 'strongly disagreed' or 'slightly disagreed' with Questions 47 and 48, were labelled 'Privacy Fundamentalists'. Respondents who 'strongly disagreed' or 'slightly disagreed' with Question 46, and 'strongly agreed' or 'slightly agreed' with Questions 47 and 48 were labelled 'Privacy Unconcerned'. The remaining options were grouped to form the third segment and were labelled 'Privacy Pragmatists'. The frequencies and percentages for the different privacy segmentation groups are shown in Table 7.27.

Table 7.27 Frequencies and percentages for the different privacy segments

PRIVACY SEGMENTS	n	%
Privacy Fundamentalists	191	30.46
Privacy Unconcerned	69	11.00
Privacy Pragmatists	367	58.53
Total	627	100.00

From Table 7.27 it is clear that more than 50 per cent of the respondents belong to the Privacy Pragmatist segment. In order to empirically test H_6 for the proportions of the three segments, a chi-square goodness-of-fit test was conducted. The results are shown in Table7.28.

Table 7.28 Chi-square test results of privacy segments

PRIVACY SEGMENTS	Privacy Fundamentalists	Privacy Unconcerned	Privacy Pragmatists	Total	
Observed frequencies	191	69	367	627	
Expected frequencies	209	209	209	627	
p-value					0.0000

The chi-square test resulted in a p-value of 0.0000, indicating that there are significant differences between the segments. The null hypothesis under the chi-square goodness-of-fit test is that the observed frequencies are equal to the theoretical frequencies, therefore the expected frequencies were all specified to be equal (refer to Table 7.28). When the null hypothesis is true, the observed and expected frequencies should be similar, in which case the test statistic would be small. The chi-square result provides sufficient evidence to infer that the proportions are not the same. **This chi-square result, together with the fact that 59 per cent of South African consumers fall within the Privacy Pragmatists segment, 30 per cent within the Privacy Fundamentalists segment, and 11 per cent within the Privacy Unconcerned segment, provide enough evidence that the null hypothesis can be rejected, leading to support for H_6.**

The remainder of the hypotheses formulated in Chapter 5 were all tested by means of the same statistical test (MANOVA) and are discussed in the next section.

7.5.2 Testing hypotheses using MANOVA

The final phase in the data analysis was to test Hypotheses 1, 2a, 3a, 4, 5 and 7a to 7f. Multiple analyses of variance (MANOVA) were performed to address the remainder of the research hypotheses. All these hypotheses related to overall privacy concerns, and instead of using simple ANOVAs on each identified factor (dependent variable), MANOVA was used to take into account the pattern of covariation among all four of the factors, identified with the exploratory factor analysis, at the same time. The objective of

MANOVA is to test for differences in the mean values of several dependent variables across groups. This enables researchers to make inferences about whether the observed differences in the sample means across two or more groups are significant (Lattin *et al.*, 2003:389, 409).

For each of the hypotheses, a MANOVA was conducted to assess the differences between the groups in terms of their overall privacy concerns (Factors 1 to 4 simultaneously). Because the multivariate test of MANOVA shows only an overall significant difference, univariate analyses and *post hoc* comparisons were performed to reveal more specific differences between groups on each of the identified factors (Factors 1 to 4 individually). To test for differences between groups for each identified hypothesis (Hypotheses 1, 2a, 3a, 4, 5 and 7a to 7f), several groups had to be formed. These include:

- protective behaviour (three subgroups);
- privacy victims (two subgroups);
- awareness of name removal procedures (two subgroups);
- Internet usage (two subgroups);
- direct shopping (two subgroups);
- age (two subgroups);
- language (three subgroups);
- education (three subgroups);
- employment (two subgroups);
- income (three subgroups); and
- gender (two subgroups).

Detail on the formation of each subgroup are addressed later in the chapter, when the testing each individual hypothesis is discussed.

Before MANOVA could be conducted, certain critical assumptions about the nature of the data needed to be addressed.

7.5.2.1 *Assumptions of MANOVA*

For the multivariate test procedures of MANOVA to be valid, three assumptions must be met: the observations must be independent, the set of dependent variables must follow a multivariate normal distribution, and the variance-covariance matrices must be equal for all treatment groups (Hair *et al.*, 1998:347).

(a) Assumption 1

The most basic violation of the MANOVA assumption occurs when there is a lack of independence among observations. The independence of the respondents was relatively ensured by the random sampling plan (refer to Section 6.5 in Chapter 6).

(b) Assumption 2

The second assumption for MANOVA to be valid concerns the normality of the dependent measures. Significance tests for MANOVA are based on the multivariate normal distribution. Multivariate normality implies that the sampling distributions of the means of the various dependent variables in each cell are normally distributed (Hair *et al.*, 1998:73). The Kolmogorov-Smirnov test was conducted to assess the normality of the dependent variables. This test calculates the level of significance for the differences from a normal distribution and, if the test statistic is significant, it indicates that there is not a normal distribution. The different Kolgomorov-Smirnov tests for the sampling distributions of the means for the various dependent variables are set out in Appendix 7. Despite the fact that all the test results (except for one) were significant (indicating non-normality), a decision was made to accommodate the normality violation for several reasons. First, violations of this assumption have little impact with larger sample sizes, as is the case in the current study. Second, the normality violation can be accommodated as long as the differences are not due to outliers (Hair *et al.*, 1998:349; Tabachnick & Fidell, 2001:329). The data were examined for outliers, and a visual examination of the data did not indicate any outliers in the data. Third, Tabachnick and Fidell (2001:329) suggested that when the smallest cell has 20 or more observations, even if there are unequal cell sizes, tests are robust to the violation of the normality

assumption. All cell sizes had more than 20 observations, with the smallest cell size containing 139 observations. All the afore-mentioned aspects provided support for the decision to continue with the MANOVA despite the violations of the normality assumption.

(c) Assumption 3

The last critical assumption concerns the homogeneity of the variance-covariance matrices across the groups. In MANOVA, the focus is the variance-covariance matrices of the dependent measures for each group. The first analysis assessed the univariate homogeneity of variance across the groups for the different hypotheses. The most commonly used test to assess homogeneity, the Levene test, was used to assess whether the variance of a single metric variable is equal across the applicable number of groups (Hair *et al.*, 1998:75). The Levene test performs an analysis of variance on the absolute deviations of values from the respective group means for each dependent variable. If the Levene test is statistically significant, then there are no homogeneous variances. The results for the different Levene tests are shown in Table 7.29.

Table 7.29 Tests for equal variances of different groups

GROUP CONCERNS	Levene's test				Box *M*
	Privacy protection (factor 1)	Information misuse (factor 2)	Solicitation (factor 3)	Government protection (factor 4)	
Protective behaviour groups	0.0000	0.0001	0.0083	**0.9748**	0.0000
Privacy victim groups	0.0066	0.0000	0.0006	**0.1791**	0.0000
Awareness of name removal	**0.5739**	0.0001	0.0000	0.0000	0.0000
Internet usage groups	**0.9711**	0.0099	0.0086	**0.9856**	0.0010
Direct shopping groups	0.0011	0.0281	0.0000	**0.1096**	0.0000
Age groups	0.0000	**0.1221**	**0.8046**	**0.9101**	0.0000
Language groups	0.0000	**0.2416**	0.0251	0.0124	0.0000
Educational groups	0.0000	0.0005	0.0013	**0.8716**	0.0000
Employment groups	**0.3319**	**0.9525**	**0.1855**	0.0197	0.0000
Income groups	0.0075	0.0075	0.0065	0.0451	0.0000
Gender groups	0.0009	**0.2828**	**0.4975**	0.0000	0.0000

As can be seen from Table 7.29, many of the Levene tests indicated unequal variances (equal variances are indicated in bold print). However, it must be noted that the Levene test is itself not necessarily very robust against violations of the homogeneity of variances assumption (StatSoft, 1995:1709).

The next step was to assess the dependent variables collectively by testing the equality all the variance-covariance matrices between the groups. The test for overall equivalence of the variance-covariance matrices is the Box *M* test. If this test is statistically significant, then the variance-covariance matrices in the different between-group cells in the design are significantly different from each other. Results of the Box *M* test for the different MANOVAs are also reported in Table 7.29 above. It is important to note that the Box *M* test is very sensitive to deviations from the normal distribution and therefore the results of this test in this study should be viewed with some scepticism, according to Tabachnick and Fidell (2001:80), who report that the Box *M* is too strict with large sample sizes. They also believe that if sample sizes are equal, significance tests can be expected to be robust and the outcome of the Box *M* can be discarded (Tabachnick & Fidell, 2001:330). Several researchers have concluded that the homogeneity of variances-covariances assumption usually does not seriously threaten the validity of the multivariate results (StatSoft, 1995:1711).

A great deal of research has assessed the robustness (or lack thereof) of ANOVA and MANOVA analyses to the violation of homogeneity of variance (Tabachnick & Fidell, 2001:80). Many believe that the formal tests of homogeneity of variance are too strict because they also assess normality. Tabachnick and Fidell (2001:80) recommend that the homogeneity of variance be assessed with F_{max} in conjunction with sample-size ratios. F_{max} is the ratio of the largest cell variance to the smallest. If sample sizes are relatively equal (within a ratio of 4 to 1 from largest cell variance to the smallest), an F_{max} as large as 10 is acceptable. In view of the fact that the F_{max} in conjunction with sample-size ratios for the data was all acceptable (refer to Appendix 8), indicating a degree of homogeneity of variance compared to the stricter Levene and Box *M* tests, a

decision was made not to transform the data. Although data transformations are recommended as a remedy for failures of normality and homogeneity, it is not universally recommended, since it limits interpretation due to the transformed scores (Tabachnick & Fidell, 2001:80). However, despite the fact that the homogeneity of variances-covariances assumption usually does not seriously threaten the validity of the multivariate results, it was decided to follow another option, namely to use the untransformed variables but to set a more stringent alpha level – using 0.025 instead of 0.05 (Tabachnick & Fidell, 2001:80).

7.5.2.2 The MANOVA process

The main purpose of using the MANOVA to test each of the hypotheses, was to assess the differences between the groups collectively rather than individually using univariate tests. Wilks' lambda was the test statistic used to assess the overall significance of the MANOVA. There is ample evidence that Wilks' lambda is the measure that is, of all the available tests, the one that is most immune to violations of the assumptions underlying MANOVA without compromising on power (Hair *et al.*, 1998:351). The larger the between-groups dispersion, the smaller the value of Wilks' lambda and the greater the implied significance. Although the multivariate tests of MANOVA do allow the rejection of the null hypotheses that the groups' means are all equal, they do not pinpoint where the significant differences lie if there are more than two groups. Therefore, where a significant Wilks' lambda result was found, it was followed by univariate analyses and *post hoc* comparisons to reveal more specific differences between groups. Where this result displayed significance, it was subjected to a one-way analysis of variance (ANOVA). In the case of more than two groups, a Scheffé *post hoc* test was applied to identify which groups displayed significant differences. An alpha level of 0.025 was specified for all the hypotheses (for the reasons set out in Section 7.4.2.1) and all significant results are indicated in bold print in the different tables.

The results of the different MANOVAs for Hypotheses 1, 2a, 3a, 4, 5 and 7a to 7f are discussed in detail below.

7.5.2.3 *H_1: There is a significant difference between consumers in terms of their protective behaviour and their privacy concerns*

Questions 49 to 53 in the questionnaire (see Appendix 1) addressed respondents' protective behaviour in terms of their information privacy. In order to make respondents' answers to these five questions more digestible, respondents were divided into one of three groups according to their 'yes' or 'no' answers to each of the five statements. If respondents answered 'no' to all five behaviour questions, they were classified as displaying 'no protective behaviour'. If respondents answered 'yes' to only one or two of the five behaviour questions, they were classified as displaying 'limited protective behaviour'. The remainder of the respondents, those who answered 'yes' to three, four or all five of the behaviour questions, were classified as a 'protective behaviour' group. Hypothesis 1 was formulated to test for significant differences between different protective behaviour groups in terms of their overall privacy concerns. Results of the MANOVA, univariate analysis and *post hoc* comparisons are set out in Table 7.30.

Table 7.30 Mean values and MANOVA results for different behaviour groups

PRIVACY CONCERNS / BEHAVIOUR GROUP	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
No protective behaviour	4.6[a]	3.5[a]	3.4[a]	4.5		
Limited protective behaviour	4.8[a]	3.7[b]	3.6[b]	4.6		
Protective behaviour	4.7[b]	4.0[ab]	3.8[a]	4.6		
Univariate analyses	**0.0000**	**0.0000**	**0.0037**	0.8412		
Wilks' lambda					6.30	**0.0000**

[a] and/or [b]: The results of the Scheffé *post hoc* tests are indicated with [a] and/or [b]. All mean values containing the same letters (for example, [a]) indicate that the groups differ significantly from one another. All mean values containing different letters (for example, an [a] or [b]) indicate that these groups do not differ significantly from one another.

The Wilks' lambda value indicates a significant difference (p=0.0000) between behaviour groups and their overall privacy concerns, providing support for H_1. The follow-up univariate analyses revealed that these differences were significant for the first three factors, namely privacy protection, information misuse and solicitation. The Scheffé *post hoc* tests revealed that the 'no protection group' differed significantly from the 'limited protection group' on Factor 1 (privacy protection). There were significant differences between both the 'no protection and limited protection groups', and the 'protective behaviour group' on Factor 2 (information misuse). Finally there were also significant differences between the 'no protective behaviour group' and the 'protective behaviour group' in terms of Factor 3 (solicitation). The high mean values for Factor 4 (government protection) indicate that **all three the behaviour groups had very strong feelings about government protection resulting in no significant differences between the groups.**

7.5.2.4 *H_{2a}: There is a significant difference between consumers who have been victims of invasions of privacy and consumers who have not been victims of invasions of privacy in terms of their privacy concerns*

Previous empirical research suggests that consumers who have been victims of privacy invasion have higher privacy concerns than consumers who have not been victims of privacy invasion (refer to Chapter 5, Section 5.4.2). H_{2a} was formulated to determine whether there would be significant differences between the victims and non-victims in terms of their privacy concerns. Results of the MANOVA as well as the subsequent univariate analyses are reported in Table 7.31.

Table 7.31 Mean values and MANOVA results for different privacy victim groups

PRIVACY CONCERNS VICTIM GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Victim of privacy invasion	4.8	4.2	3.8	4.6		
Not a victim of privacy invasion	4.7	3.5	3.5	4.5		
Univariate analyses	0.1012	**0.0000**	**0.0000**	0.1829		
Wilks' lambda					17.06	**0.0000**

A total of 31 per cent of respondents indicated that they had been victims of privacy invasion (refer to Table 7.12). The MANOVA result shows significant differences between the different victim groups in terms of their overall privacy concerns. **The p-value (p=0.0000) indicated that the null hypothesis could be rejected, providing support for H_{2a}.** The follow-up univariate analyses revealed that these differences were significant for Factor 2 (information misuse) and Factor 3 (solicitation). In both cases, the victims of privacy invasion had higher mean values than the non-victims, which corresponds with the results from previous studies which indicated higher concerns among victims of privacy invasion. It is interesting to note that both groups regarded it as important to receive privacy and government protection (Factor 1 and 4) and no significant differences were identified for these two subdimensions.

7.5.2.5 *H_{3a}: There is a significant difference between consumers in terms of their level of awareness of name removal procedures and their privacy concerns*

Various studies have measured whether consumers' knowledge levels of privacy policies and practices affect their privacy concerns. Some studies have found that knowledgeable consumers are less concerned about their personal information, whereas other studies suggested that consumers are more concerned about the

collection and use of their personal information (Culnan, 1995:14; Campbell, 1997:46). In this study, consumers' knowledge was assessed by the following question: 'are you aware of any options to remove your name from records of companies?' The findings are set out in Table 7.32.

Table 7.32 Mean values and MANOVA results for the different awareness groups

PRIVACY CONCERNS AWARENESS GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Aware of name removal procedures	4.8	3.5	3.3	4.3		
Not aware of name removal procedures	4.7	3.8	3.7	4.6		
Univariate analyses	0.2580	**0.0009**	**0.0027**	**0.0000**		
Wilks' lambda					12.56	**0.0000**

The Wilks' lambda value indicated a significant difference (p=0.0000) between the different awareness groups in terms of their overall privacy concerns, providing support for H_{3a}. The follow-up univariate analyses revealed that these differences were significant for all the factors, except for Factor 1 (privacy protection) where both groups had high concerns in terms of privacy protection. The significant dimensions indicated that the respondents who were **not** aware of name removal procedures were more concerned about their privacy (see higher mean values in Table 7.32).

7.5.2.6 *H_4: There is a significant difference between Internet users and Internet non-users in terms of their privacy concerns*

Questions 56 and 57 measured respondents' involvement in Internet transactions (refer to Appendix 1). If respondents answered 'no' to both questions, indicating that they were not involved in Internet transactions, they were classified as 'Internet non-users'. If

respondents answered 'yes' to one or both of the questions, indicating Internet involvement, they were classified as 'Internet users'. The mean values of the different groups and the MANOVA results are shown in Table 7.33.

Table 7.33 Mean values and MANOVA results for Internet user groups

PRIVACY CONCERNS / INTERNET USER GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Internet users	4.7	4.0	3.8	4.5		
Internet non-users	4.7	3.6	3.5	4.5		
Univariate analyses	0.9837	**0.0010**	0.0344	0.9548		
Wilks' lambda					3.29	**0.0111**

The significant Wilks' lambda (p=0.0111) provided enough support for H_4, namely that Internet users and Internet non-users differ in terms of their overall privacy concerns. The subsequent univariate analyses revealed that these differences were mainly due to the information misuse dimension of privacy (Factor 2). Here the Internet users had a higher mean value than the Internet non-users, indicating that they were more concerned about the misuse of their personal information. Both Internet and Internet non-users felt that it was very important to receive privacy protection and government protection (Factor 1 and 4) as can be seen from the high alpha values and the similar mean values reported for these two subdimensions in the univariate analyses.

7.5.2.7 H_5: There is a significant difference between direct shoppers and non-direct shoppers in terms of their privacy concerns

Questions 58 to 60 in the questionnaire (see Appendix 1) related to direct purchasing – be it shopping by means of a catalogue, or placing an order telephonically. Respondents who answered 'no' to all the direct purchasing questions indicated that they had not bought anything directly during the past year, and were classified as 'non-

direct shoppers'. All the respondents who answered 'yes' to one, two or all three of the questions were classified as 'direct shoppers' because they had purchased directly before. There are no published research findings about whether direct purchasing experience and knowledge of consumers increases privacy concerns among South Africans. Results from studies in other countries have indicated that consumers who have been involved in direct purchasing tended to be more concerned about threats to their privacy (refer to Chapter 5, Section 5.4.5). The MANOVA results for H_5 are illustrated in Table 7.34.

Table 7.34 Mean values and MANOVA results for different direct shopping groups

PRIVACY CONCERNS DIRECT SHOPPING GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Direct shoppers	4.8	3.6	3.3	4.5		
Non-direct shoppers	4.7	3.8	3.8	4.6		
Univariate analyses	0.0456	0.0487	**0.0000**	0.0754		
Wilks' lambda					11.52	**0.0000**

The specified significance level of 2.5 per cent resulted in a p-value of 0.0000, indicating support for H_5. This demonstrates that there is a difference between direct shoppers and non-direct shoppers in terms of their privacy concerns. To establish where the differences lie, univariate analyses were conducted on the different dependent variables (factors). This revealed that the differences between direct and non-direct purchasers were related to solicitation (Factor 3). The mean values in Table 7.34 further indicate that the non-direct shoppers were more concerned about solicitation than the direct shoppers (3.8 versus 3.3). This suggests why these respondents were classified as non-direct shoppers – they specifically do not purchase by means of catalogues, direct mail or telemarketing because they view these

purchasing forms as intrusive and do not want unsolicited communication from companies.

7.5.2.8 *H_{7a}: There is a significant difference between young and old people in terms of their privacy concerns*

Several studies on information privacy have found a relationship between age and privacy concerns (refer to Chapter 5, Section 5.4.7.1). The majority of these studies show that the level of privacy concerns increases with age. As has been mentioned in Section 7.4.1.2, respondents were divided into two age groups. The one group represented young consumers (18-39 years) and the other group represented the older consumers (40+ years). The mean values of the two age groups and the MANOVA results of the hypothesis test are shown in Table 7.35.

Table 7.35 Mean values and MANOVA results for different age groups

PRIVACY CONCERNS AGE GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
18-39 years	4.7	3.6	3.5	4.5		
40+ years	4.8	3.8	3.7	4.6		
Univariate analyses	**0.0050**	**0.0157**	**0.0066**	0.3774		
Wilks' lambda					3.69	**0.0056**

The MANOVA result showed significant differences between the younger and older age groups in terms of their overall concerns. The null hypothesis was thus rejected, as there is support for H_{7a}. The follow-up univariate analyses revealed that these differences were significant for all the privacy dimensions, except for Factor 4 (government protection) where both age groups had high concerns. The higher mean values among the older age group corresponded with some of the findings of the international studies, namely that older consumers are more concerned about information privacy than younger consumers.

7.5.2.9 *H_{7b}: There is a significant difference between the main language groups in terms of their privacy concerns*

Question 62 in the questionnaire (see Appendix 1) requested respondents to indicate their home language. The question made provision for all eleven official South African languages. After an examination of the frequencies of all eleven different language groups (see Table 7.5), it was decided to reduce the eleven language groups to three main language groups to simplify the results. The first group included all English-speaking respondents, the second group all Afrikaans-speaking respondents, and the third group all the Black African language groups (refer to Table 7.5). Since the nine Black African languages accounted for 20 per cent of the sample, these languages were grouped together and labelled the Black African language group. Respondents who indicated that their home language did not belong to any one of the eleven official languages were excluded from further analysis since they only accounted for two per cent of the sample. The three main language groups where then compared in terms of their privacy concerns. The results of the MANOVA, univariate analysis and *post hoc* comparisons are shown in Table 7.36.

Table 7.36 Mean values and MANOVA results for different language groups

PRIVACY CONCERNS LANGUAGE GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
English	4.8^{a}	3.9^{ab}	3.8^{a}	4.5		
Afrikaans	4.8^{b}	3.6^{a}	3.6^{b}	4.6		
Black African	4.6^{ab}	3.6^{b}	3.2^{ab}	4.5		
Univariate analyses	**0.0002**	**0.0014**	**0.0000**	0.0611		
Wilks' lambda					6.34	**0.0000**

[a] and/or [b]: The results of the Scheffé *post hoc* tests are indicated with [a] and/or [b]. All mean values containing the same letters (for example, [a]) indicate that the groups differ significantly from one another. All mean values containing different letters (for example, an [a] or [b]) indicate that these groups do not differ significantly from one another.

The Wilks' lambda value indicates a significant difference (p=0.0000) between the main language groups and their overall privacy concerns, providing support for H_{7b}. The subsequent univariate analyses revealed that these differences were significant for the first three factors, namely, privacy protection, information misuse and solicitation. The Scheffé *post hoc* tests showed that both the English- and Afrikaans-speaking groups differed significantly from the Black African language group on the privacy protection as well as the solicitation dimensions. Both the English-speaking and the Afrikaans-speaking groups were more concerned, as indicated by the higher mean values for these two groups. There were also significant differences between the Afrikaans-speaking and the Black African language group compared to the English-speaking group in terms of the information misuse dimension. Here the English-speaking group was more concerned than the other two groups, which had lower mean values. The high mean values of all three groups on Factor 4 (government protection) indicated that all the groups had strong concerns about government protection resulting in no significant differences between the groups.

7.5.2.10 H_{7c}: There is a significant difference between consumers in terms of their levels of education and their privacy concerns

Question 63 in the questionnaire (see Appendix 1) gave respondents five options to classify their highest level of education. To simplify the analysis and the hypothesis testing, these five groups were converted into three subgroups representing low, medium and high level of education. Respondents who indicated that their highest qualification was 'lower than Grade 8' or 'up to Grade 10' were classified as the low educational group. Respondents with a Grade 12 qualification were classified as the medium educational group. Respondents who indicated that they have a degree/diploma or a post-graduate degree/higher diploma were labelled as the high educational group. Most empirical studies reported strong positive relationships between educational levels and privacy concerns (refer to Chapter 5, Section 5.4.7.3). However, the studies indicated different relationships between more and less educated

levels and their privacy concerns. Hypothesis 7c was put to the test by means of MANOVA, follow-up analyses and *post hoc* tests, as reported in Table 7.37.

Table 7.37 Mean values and MANOVA results for different educational groups

PRIVACY CONCERNS / EDUCATIONAL GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Low education level	4.6[a]	3.4[a]	3.3[ab]	4.5		
Medium education level	4.7[b]	3.6[a]	3.6[a]	4.5		
High education level	4.8[a]	4.0[a]	3.7[b]	4.6		
Univariate analyses	0.0600	**0.0000**	**0.0000**	0.8008		
Wilks' lambda					7.01	**0.0000**

[a] and/or [b]: The results of the Scheffé *post hoc* tests are indicated with [a] and/or [b]. All mean values containing the same letters (for example, [a]) indicate that the groups differ significantly from one another. All mean values containing different letters (for example, an [a] or [b]) indicate that these groups do not differ significantly from one another.

The specified significance level of 2.5 per cent resulted in a p-value of 0.0000, indicating support for H_{7c}. This means that there is a difference between groups with different levels of education and their privacy concerns. To determine where the differences between the three groups lie, univariate analyses were conducted on the different dependent variables (factors). This revealed that the differences between the different educational groups were related to information misuse (Factor 2) and solicitation (Factor 3). The Scheffé *post hoc* tests showed that all three educational groups differed from one another in terms of information misuse, with the highly educated group being the most concerned and the less educated group being the least concerned. Solicitation concerns (Factor 3) differed for the least educated group on the one hand and the medium and high level of education groups on the other. Here both the medium and high level of education groups were more concerned than the low level of education group. The high mean values for all three groups on Factor 1 (privacy protection) and Factor 4 (government protection) indicated that all the groups felt very

strongly about these two dimensions, resulting in no significant differences between the groups.

7.5.2.11 *H_{7d}: There is a significant difference between consumers in terms of their employment status and their privacy concerns*

Answers to Question 64 in the questionnaire (see Appendix 1) were divided into two meaningful groups. All the respondents who indicated that they were employed full time, part time or self-employed were labelled as the 'employed group'. Respondents who were students, homemakers, pensioners, not employed or physically unfit for work were classified as the 'not-employed group'. Only a few international studies have investigated the relationship between employment status and privacy concerns, and most of them have not found any significant relationships (refer to Chapter 5, Section 5.4.7.5). Table 7.38 shows the results of the MANOVA results for Hypothesis 7d, testing for significant differences between consumers' employment status and their privacy concerns.

Table 7.38 Mean values and MANOVA results for different employment status groups

PRIVACY CONCERNS EMPLOYED GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Employed	4.7	3.8	3.6	4.5		
Not employed	4.7	3.6	3.5	4.6		
Univariate analyses	0.4255	**0.0044**	0.0514	0.2471		
Wilks' lambda					3.61	**0.0065**

The MANOVA result showed significant differences between the employed and the not employed group in terms of their overall concerns. **The null hypothesis was thus rejected, as there was support for H_{7d}.** The follow-up univariate analyses revealed that the significant overall result was due to a significant difference on only one privacy

dimension, namely information misuse (Factor 2). Here the employed group was more concerned than the unemployed group regarding the misuse of their personal information. No significant differences were found on any of the other three privacy dimensions (or factors).

7.5.2.12 *H_{7e}: There is a significant difference between consumers in terms of their income levels and their privacy concerns*

Nine percent of the respondents refused to answer Question 65, relating to their personal total monthly income. The remaining 91 per cent of the respondents were classified into one of three different income level groups. Respondents earning less than R2 000 per month were classified as the 'low-income group'. Respondents earning between R2 001 and R6 000 per month were classified as the 'middle-income group', and respondents earning more then R6 001 were labelled the 'high-income group'. International studies have reported conflicting results regarding the relationship between consumers' income levels and their privacy concerns, with some studies finding no relationship between income and privacy concerns (refer to Chapter 5, Section 5.4.7.5). Results of the MANOVA, univariate analysis and post hoc comparisons are set out in Table 7.39.

Table 7.39 Mean values and MANOVA results for different income groups

PRIVACY CONCERNS INCOME GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Low income level	4.6^{ab}	3.5^{a}	3.3^{a}	4.5		
Middle income level	4.8^{a}	3.7^{b}	3.5^{b}	4.6		
High income level	4.8^{b}	4.1^{ab}	3.8^{ab}	4.5		
Univariate analyses	**0.0121**	**0.0000**	**0.0000**	0.2916		
Wilks' lambda					6.53	**0.0000**

[a] and/or [b]: The results of the Scheffé *post hoc* tests are indicated with [a] and/or [b]. All mean values containing the same letters (for example, [a]) indicate that the groups differ

significantly from one another. All mean values containing different letters (for example, an [a] or [b]) indicate that these groups do not differ significantly from one another.

The Wilks' lambda value indicates a significant difference (p=0.0000) between the three income groups in terms of their overall privacy concerns, providing support for H_{7e}. The follow-up univariate analyses showed that these differences were significant for the first three factors namely privacy protection, information misuse and solicitation. The Scheffé *post hoc* tests revealed that both the middle and high-income groups differed significantly from the low-income group in terms of the privacy protection dimension (or factor). Here both the middle and higher income groups have higher privacy concern levels. The *post hoc* tests also indicated that both the low and middle income groups differed significantly from the high income group on the information misuse as well as the solicitation dimensions (or factors), with the high income group being the more concerned group in both cases. **From results in Table 7.39 it can be concluded that higher income groups tend to have higher privacy concerns.**

7.5.2.13 *H_{7f}: There is a significant difference between males and females in terms of their privacy concerns*

Several international studies maintained that gender was strongly associated with privacy concerns (refer to Chapter 5, Section 5.4.7.6). It seems that generally, females express more concern about threats to their personal privacy than males do. The mean values of the two gender groups and the MANOVA results of Hypothesis 7f are shown in Table 7.40.

Table 7.40 Mean values and MANOVA results for different gender groups

PRIVACY CONCERNS GENDER GROUPS	Privacy protection	Information misuse	Solicitation	Government protection	F value	p-value
Male	4.7	3.7	3.5	4.4		
Female	4.8	3.7	3.7	4.6		
Univariate analyses	**0.0138**	0.5683	0.0481	**0.0005**		
Wilks' lambda					3.81	**0.0046**

The Wilks' lambda value indicates a significant difference (p=0.0046) between males and females in terms of their overall privacy concerns, providing support for H_{7f}. The subsequent univariate analyses revealed that these differences were significant for the first and the fourth privacy dimensions (or factors), namely privacy protection and government protection. In both cases females had higher privacy concerns, expressing their need for protection.

A summary of all of the above-discussed hypotheses is presented in Table 7.41, indicating whether support was found for the hypotheses.

Table 7.41 Summary of hypotheses tested

Alternative hypotheses		Supported or not supported
H_1	There is a significant difference between consumers in terms of their protective behaviour and their privacy concerns	Supported
H_{2a}	There is a significant difference between consumers who have been victims of invasions of privacy and consumers who have not been victims of invasions of privacy in terms of their privacy concerns	Supported
H_{2b}	There is a dependency between being a victim of invasion of privacy and gender	Supported

H_{3a}	There is a significant difference between consumers in terms of their level of awareness of name removal procedures and their privacy concerns	Supported
H_{3b}	There is a dependency between the level of awareness of name removal procedures and age	Not supported
H_{3c}	There is a dependency between the awareness of name removal procedures and levels of education	Not supported
H_4	There is a significant difference between Internet users and Internet non-users in terms of their privacy concerns	Supported
H_5	There is a significant difference between direct shoppers and non-direct shoppers in terms of their privacy concerns	Supported
H_6	The proportion of South African consumers is not equally represented in the different privacy segments.	Supported
H_{7a}	There is a significant difference between young and old people in terms of their privacy concerns	Supported
H_{7b}	There is a significant difference between the main language groups in terms of their privacy concerns	Supported
H_{7c}	There is a significant difference between consumers in terms of their levels of education and their privacy concerns	Supported
H_{7d}	There is a significant difference between consumers in terms of their employment status and their privacy concerns	Supported
H_{7e}	There is a significant difference between consumers in terms of their income levels and their privacy concerns	Supported
H_{7f}	There is a significant difference between males and females in terms of their privacy concerns	Supported

The above table provides a summary of the main findings in support of the secondary objectives specified in Chapter 5. Several other conclusions can be drawn from the data analyses conducted and discussed in this chapter. Some of the findings, in support of the primary objective, namely, to identify and explore the information privacy concerns of South African consumers, are summarised below:

- The exploratory factor analysis identified four underlying information privacy dimensions, namely privacy protection, information misuse, solicitation and government protection.
- Men seemed to be more likely than women to perceive themselves as victims of privacy invasion.
- Consumers who exercised full protective behaviour or limited protective behaviour were more concerned about privacy protection, information misuse and solicitation than consumers who did not exercise any protective behaviour.
- Consumers who had been victims of privacy invasions had higher information misuse and solicitation concerns than consumers who had not been victims of privacy invasions.
- Consumers who were not aware of any name removal options were more concerned about the misuse of their information, solicitation practices and government's protection than consumers who were aware of name removal options.
- Consumers' awareness of name removal options was not related to their levels of education or their age.
- Consumers who had undertaken Internet transactions were more concerned about the misuse of their information than consumers who had not used the Internet for transactions.
- Consumers who had not purchased directly in the past year showed higher concerns regarding the solicitation practices of companies than consumers who had purchased directly during the past year.
- Older consumers (40+ years) were more concerned than younger consumers (below 40 years) about the protection of their privacy, the misuse of their information and the solicitation practices of companies.
- English- and Afrikaans-speaking consumers were more concerned about privacy protection and solicitation practices than Black African language consumers.
- English-speaking consumers were more concerned about the misuse of their information than Afrikaans-speaking and Black African language consumers.

- Consumers with a high level of education (tertiary education) had higher privacy concerns regarding the misuse of their information compared to consumers with a medium or low level of education.
- Consumers with a medium or high level (Grade 12 and higher) of education were more concerned about companies' solicitation practices than consumers with a low level of education.
- Consumers who were employed showed higher concerns relating to information misuse than consumers who were not employed.
- Higher income consumers were more concerned regarding their privacy protection, information misuse and feelings toward solicitation than middle and low income consumers.
- Females were more concerned than males about the protection of their privacy by companies and government.
- Almost one-third of the respondents belonged to the Privacy Fundamentalist segment, which suggested that there are very high information privacy concerns among South Africans. The majority of South African consumers (58 per cent) belong to the Privacy Pragmatist segment, indicating balanced information privacy concerns, with only 11 per cent belonging to the Privacy Unconcerned segment, where there are very low levels of concern or no concern at all.

7.6 SUMMARY

In this chapter, the empirical results of the study were presented. First, there was a focus on the descriptive statistics, after which attention was given to the results of the exploratory factor analysis and the confirmatory factor analysis. The empirical analyses indicated that the information privacy scale used in this study was both reliable and valid. Finally, the empirical results were assessed against the formulated hypotheses, concluding with a summary of the outcomes of each hypothesis test. One conclusion that can be drawn from this chapter is that South African consumers show definite information privacy concern, and that their level of concern is very high in certain areas. In the final chapter, the above findings are interpreted, with particular reference to their

implications for marketers. Chapter 8 sets out conclusions and recommendations based on the main findings represented in this chapter.

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.

BIBLIOGRAPHY

African National Congress (ANC). 1990. **A working document by the ANC Constitutional Committee**. Centre for Development Studies.

Agre, P.E. & Rotenberg, M. 1998. **Technology and Privacy: the new landscape**. First Edition. Cambridge: MIT Press.

Alberta, P.M. 2002a. Groups challenge Indiana's DNC list law on free speech grounds. **Direct Newsline**, 15 April, http://www.industryclick.com.

Alberta, P.M. 2002b. Illinois to ban unsolicited telemarketing to cell phones. **Direct Newsline**, 16 May, http://www.industryclick.com.

Allen, C., Kania, D. & Yeackel, B. 1998. **Internet World Guide to one-to-one Web Marketing**. USA: John Wiley & Sons.

Anderson, J.C. & Gerbing, D.W. 1988. Structural equation modeling in practice: a review and recommended two-step approach. **Psychological Bulletin**, 103(3):411-423.

Anon. 1999. Privacy promise made to American consumers. **Direct Marketing**, 62(5):6.

Anon. 2000. In praise of privacy. **Canadian Banker**, 107(1):14-19.

Anon. 2001. Net fraud protection. **Marketing Mix**, June:20.

Anon. 2002a. The IBM Tivoli Privacy Wizard: define your privacy policies today. **Resource Center**, http://www.tivoli.com/resource_center.

Anon. 2002b. How will the cookie crumble? Opposition grows to new EP privacy proposals. **InternetWorks**, 4 February, http://www.iwks.com/news.

Anon. 2002c. Internet-related bill becomes law. **City Press**, 4 August:2.

Arganoff, M.A. 1991. Protecting personal privacy exposed in corporate databases. **Information Strategy: The Executive's Journal**, 7(4):27-32.

Ariely, D. 2000. Controlling the information flow: effects on consumers' decision-making and preference. **Journal of Consumer Research**, 27(2):233-248.

Arnould, E., Price, L. & Zinkhan, G. 2002. **Consumers**. Boston: McGraw-Hill.

Association for Competitive Technology. 2001. Consumer privacy poll. **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.

Bagozzi, R.P. & Heatherton, T.F. 1994. A general approach to representing multifaceted personality constructs: application to state self-esteem. **Structural Equation Modeling**, 1(1):35-67.

Banham, R. 2000. Share data at your own risk. **World Trade**, 13(11):60.

Baumgartner, H. & Homburg, C. 1996. Applications of structural equation modelling in marketing and consumer research: a review. **International Journal of Research in Marketing**, 13:139-161.

Berscheid, E. 1977. Privacy: a hidden variable in experimental social psychology. **Journal of Social Issues**, 33(3):85-101.

Bhatia, D. 2001. Beyong the one-to-one future. **Target Marketing**, 24(2):109-113.

Blattberg, R.C. & Deighton, J. 1991. Interactive marketing: exploiting the age of addressability. **Sloan Management Review**, 33(1):5-15.

Blotzer, M.J. 2000. Privacy in the digital age. **Occupational Hazards**, 62(7):29-31.

Brand, R. 2000a. Fate of Info Bill today. **The Daily News**, 20 January:3.

Brand, R. 2000b. ANC's information act will erode privacy, opposition parties say. **The Sunday Independent**, 23 January:3.

Brand, R. 2000c. Information Bill approved. **The Daily News**, 26 January:3.

Brand, R. 2000d. New era dawns in right to information. **The Star**, 21 March:6.

Bremner, K. 2002a. CMA criticises draft privacy legislation in Ontario. **DM News**, 3 April, http://wwww.dmnews.com.

Bremner, K. 2002b. EU Parliament passes opt-in Internet privacy bill. **DM News**, 31 May, http://wwww.dmnews.com.

Bureau of National Affairs (BNA). 2002a. Ontario privacy proposal based on principle of opt-in consent, official says. **Privacy Law Watch,** 28 March, http://pubs.bna.com.

Bureau of National Affairs (BNA). 2002b. New initiatives aim to help consumer distinguish between good and bad spam. **Privacy & Security Law,** 1(5):107.

Bureau of National Affairs (BNA). 2002c. Japan's METI issues revised ordinance requiring clear labelling of junk e-mail. **Privacy Law Watch,** 8 February, http://pubs.bna.com.

Bureau of National Affairs (BNA). 2002d. Business group and cybersecurity alliance launch public campaign for online safety. **Privacy Law Watch,** 13 February, http://pubs.bna.com.

Bureau of National Affairs (BNA). 2002e. Privacy chief criticises UK government for failing to provide enhancement tools. **Privacy & Security Law,** 1(3):61.

Bureau of National Affairs (BNA). 2002f. Legal, security, marketing sectors urged to cooperate on privacy and security. **Privacy Law Watch,** 11 March, http://pubs.bna.com.

Bureau of National Affairs (BNA). 2002g. New web site aims to help consumers locate retailers that meet BBB standards. **Privacy & Security Law,** 1(6):148.

Bureau of National Affairs (BNA). 2002h. EU says transparency, enforcement problems need attention in US Safe Harbor program. **Privacy & Security Law,** 1(8):191.

Bureau of National Affairs (BNA). 2002i. Canadian official criticises Air Canada's use of frequent flyer personal information. **Privacy & Security Law,** 1(12):317.

Burgers, A., De Ruyter, K., Keen, C. & Streukens, S. 2000. Customer expectation dimensions of voice-to-voice service encounters: a scale-development study. **International Journal of Service Industry Management**, 11(2):142-161.

Buys, R. 2002. **Privacy and the right to information**. Sonnenberg Hoffman & Galombik Attorneys, Cape Town, http://www.legalnet.co.za/cyberlaw.

Caisse, K.B. 2002. When customer service becomes spam. **CRMDaily.com**, 11 June, http://www.ecommercetimes.com.

Cameron, J. 1997. How big firms sell all your secrets. **The Cape Times**, 7 February:1.

Campanelli, M. 2002. DNC list, spam on congress' agenda. **DM News**, 23 January, http://www.dmnews.com.

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.

Cate, F.H. & Staten, M.E. 2001. Protecting privacy in the new millennium: the fallacy of opt-in. **Direct Marketing Association**, http://www.the-dma.org/isec/optin.htm.

Cattell, R.B. 1966. The scree test for the number of factors. **Multivariate Behaviour Research**, 1:245-276.

Churchill, G.A. & Iacobucci, D. 2002. **Marketing research: methodological foundations**. Eighth Edition. Fort Worth: Harcourt College Publishers.

Cohen, R. 1991. The rebellion of private Cohen. **Washington Post Magazine**, 21 April:5.

Cole, D.A., Cho. S. & Martin, J.M. 2001. Effects of validity and bias on gender differences in the appraisal of children's competence: results of MTMM analyses in a longitudinal investigation. **Structural Equation Modeling**, 8(1):84-107.

Colker, D. 2002. State spam laws rarely enforced. **Los Angeles Times**, 1 April, http://www.latimes.com.

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

Constitutional Assembly. 1996. **Constitution of the Republic of South Africa 1996**. Constitutional Assembly, http://www.polity.org.za/govdocs/constitution.

Cooper, D.R. & Schindler, P.S. 2001. **Business Research Methods**. Seventh Edition. Boston: Irwin McGraw-Hill.

Costello, S. 2002. FBI warns cybercrime is on the rise. **IDG News Service**, 8 April, http://pcworld.com.

Coviello, N.E., Brodie, R.J. & Munro, H.J. 1997. Understanding contemporary marketing: development of a classification scheme. **Journal of Marketing Management**, 13:501-522.

Credeur, M.J. 2002. EarthLink wins $25 million lawsuit against junk e-mailer. **Atlanta Business Chronicle**, 22 July, http://atlanta.bizjournals.com/atlanta/stories.

Creed, A. 2000. Computer security, data privacy doubts are rife. **Newsbytes**, 18 October, http://www.newsbytes.com.

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.

Cyber Dialogue. 2001. Internet survey commissioned by UCO Software. **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.

D'Aversa-Williams, T. 1999. Security vital to information access. **Security**, 36(8):6.

Darby, I. 1999. EU is out of step with public on data privacy, finds study. **Marketing**, 29 April:2.

David Binder Research. 2001. Telocity national poll of family use of the Internet, May: 22, **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.

Davis, J.F. 1997. Property rights to consumer information. **Journal of Direct Marketing**, 11(3):32-43.

Daya, J.C. 1996. **Privacy policies and practices: an investigation of secondary use of information within South African retail banking institutions**. Unpublished MCom research report. University of the Witwatersrand, Johannesburg.

De Waal, J., Currie, I. & Erasmus, G. 2000. **The Bill of Rights Handbook**. Kenwyn: Juta.

DeMarrais, K. 2002. Deal set for net privacy. **The Hackensack Record**, 3 January, http://www.bergen.com.

Department of Communications. 2000a. The Green Paper on Electronic Commerce for South Africa. **Direct Marketing Association**, http://www.dma.org.za.

Department of Communications. 2000b. **Green Paper on e-Commerce: making it your business**. Republic of South Africa: Department of Communications.

Devenish, G.E. 1999. **A commentary on the South African Bill of Rights**. Durban, South Africa: Butterworth.

Diamantopoulos, A. & Schlegelmilch, B.B. 1997. **Taking the fear out of data analysis**. London: Dryden Press.

Dillon, W.R., Madden, T.J. & Firtle, N.H. 1993. **The essentials of marketing research**. Homewood, Illinois: Richard and Irwin.

Direct Marketing Association (DMA). 2001a. **The privacy file**. Direct Marketing Association of Southern Africa, April, http://www.dma.org.za.

Direct Marketing Association (DMA). 2001b. **Best practice guidelines for the marketing of goods and services through the Internet**. Direct Marketing Association of Southern Africa, August, http://www.dma.org.za.

Direct Marketing Association (DMA). 2002a. DMA's FTC Comments. **3D Daily Digest**, 16 April, http://www.the-dma.org/news.

Direct Marketing Association (DMA). 2002b. FTC proposes national DNC registry. **3D Daily Digest**, 22 January, http://www.the-dma.org/news.

Direct Marketing Association (DMA). 2002c. States mull opt-in, opt-out rules. **3D Daily Digest**, 13 March, http://www.the-dma.org/news.

Donaldson, T. & Dunfee, T.W. 1994. Toward a unified conception of business ethics: integrative social contracts theory. **Academy of Management Review**, 19(20):252-284.

Du Plessis, P.J. & Rousseau, G.G. 2003. **Buyer behaviour: a multi-cultural approach**. Third Edition. Cape Town: Oxford University Press.

Eddy, E.R., Stone, D.L. & Stone-Romero, E.F. 1999. The effects of information management policies on reactions to human resource information systems: an integration of privacy and procedural justice perspectives. **Personnel Psychology**, 52(2):335-358.

Eisner, R.S. 2002. Ignorance isn't bliss. **Legal Research Center**, http://www.cio.com.

Electronic Privacy Information Center (EPIC). 2001. Cybercrime treaty signed and other international developments. **EPIC Alert**, 8(23):1-8, http://www.epic.org/alert/EPIC Alert 8.23.html.

Electronic Privacy Information Center (EPIC). 2002. Public opinion on privacy. **EPIC public opinion and privacy page**, 1 May:1-16, http://www.epic.org/privacy/survey.

Engel, J.F., Blackwell, R.D. & Miniard, P.W. 1995. **Consumer behaviour**. Eighth Edition. Fort Worth, USA: Dryden Press.

Ettinger, J.E. 1993. **Information security: an integrated approach**. London: Chapman & Hall.

European Society for Opinion and Marketing Research (ESOMAR). 2001. Maintaining the distinctions between marketing research and direct marketing. **ESOMAR Guideline**, June:1-5.

European Union (EU). 1997. Working documents on privacy enhancing technologies. **Data Protection Studies**, October: 1, http://europa.eu.int/comm/internal_market/en/dataprot/studies/petintro.htm.

Ferrara, F.F. 2000. Validation of the child sex abuse attitude scale through confirmatory factor analysis. **Structural Equation Modeling**, 6(11):99-112.

Fletcher, K. & Peters, L. 1996. Issues in customer information management. **Journal of the Market Research Society**, 38(2):145-160.

Floor, J. 2001. Moenie met kliënte se inligting mors nie. **Finansies & Tegniek**, 21 September:41.

Floyd, F.J. & Widaman, K.F. 1995. Factor analysis in the development and refinement of clinical assessment instruments. **Psychological Assessment**, 7(3):286-299.

Forcht, K.A. & Pierson, J. 1994. New technologies and future trends in computer security. **Industrial Management and Data Systems**, 94(8):30-36.

Forcht, K.A. & Thomas, D.S. 1994. Information compilation and disbursement: moral, legal and ethical considerations. **Information Management & Computer Security**, 2(2):23-28.

Fornell, C. & Larcker, D.F. 1981. Evaluating structural equation models with unobservable variables and measurement error. **Journal of Marketing Research**, 18(February):39-50.

Fowler, G.W. 1995. **Invasion of privacy: an investigation into the attitudes of consumers and the contributory role of information technology**. Unpublished MBA research report. University of Cape Town, Cape Town.

France, M. 2002. Needed now: laws to can spam. **BusinessWeek Online**, 26 September, http://www.businessweek.com.

Franzak, F., Pitta, D. & Fritsche, S. 2001. Online relationships and the consumer's right to privacy. **Journal of Consumer Marketing**, 18(7):631-641.

Furber, R. 2001. The big switch-off. **Precision Marketing**, 13(31):23.

Gallup. 2000. Derivion-commissioned research. **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.

Gallup. 2001. The Gallup poll on Internet users and privacy. **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.

Garretson, C. 2001. IBM creates institute, council on privacy. **InfoWorld**, 12 November, http://staging.infoworld.com/articles.

GartnerG2. 2000. Privacy and security: the hidden growth challenge. **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.

Gauthronet, S. & Drouard, E. 2001. Unsolicited commercial communications and data protection. **Commission of the European Communities**, January:1, http://europa.eu.int/comm/internal_market/en/dataprot/studies/spam.htm.

Gay, L. 2002. Plan in Congress may do little to slow flood of spam e-mail. **Scripps Howard News Service**, 13 May, http://www.gomemphis.com.

George, J.F. 2002. Influences on the intent to make Internet purchases. **Internet Research: Electronic Networking Applications and Policy**, 12(2):165-180.

Glazer, R. 1991. Marketing in an information-intensive environment: strategic implications of knowledge as an asset. **Journal of Marketing**, 55(October):1-19.

Gleick, J. 2003. Tangled up in spam. **The New York Times**, 9 February, http://www.nytimes.com.

Godin, S. 1999. **Permission marketing: turning strangers into friends, and friends into customers**. New York: Simon & Schuster.

Goodwin, C. 1991. Privacy: recognition of a consumer right. **Journal of Public Policy & Marketing**, 19(Spring):149-166.

Gordon, I.H. 1998. **Relationship marketing**. Canada: John Wiley & Sons.

Grant, L. 2002. Personal privacy: why cashiers want your phone number. **USA Today**, 23 April, http://www.usatoday.com

Grant, R. 2000. The social contract and human rights. **The Humanist**, Jan/Feb:18-23.

Grealy, P. 2002. Move to a paperless society. **Business Day**, 24 April:21.

Green, H. 1999. Privacy online: the FTC must act now. **Business Week**, 29 November:48.

Green, P. 2001. A wired world exposes companies to new risk. **Global Finance**, 15(3):57-58.

Green, S.B., Salkind, N.J. & Akey, T.M. 1999. **Using SPSS for windows: analysing and understanding data**. Upper Saddle River, New Jersey: Prentice Hall.

Greenfield Online. 2001. BBBOnline survey. **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.

Grimm, L.G. & Yarnold, P.R. 2000. **Reading and understanding more multivariate statistics**. Washington DC, USA: American Psychological Association.

Groenewald, M & Lehlokoe, D. 1999. **Towards and electronic commerce policy for South Africa**, http://www.isoc.org/isoc/conferences/inet/99/proceedings.

Grönroos, C. 1990. Marketing redefined. **Management Decision**, 28(8):5-9.

Grönroos, C. 1994. Quo Vadis, marketing? Towards a relationship marketing paradigm. **Journal of Marketing Management**, 10:347-360.

Grönroos, C. 1997. Keynote paper: From marketing mix to relationship marketing – towards a paradigm shift in marketing. **Management Decision**, 35(4):322-339.

Gruenwald, J. 2002. Bank of America Chief Executive endorses national do-not-call lists for telemarketing. **Privacy Law Watch,** 25 March, http://pubs.bna.com.

Guilford, J.P. 1954. **Psychometric methods**. Second Edition. New York, USA: McGraw-Hill.

Gunst, C. 1999. Give security measures top priority when implementing Internet applications. **Plant Engineering**, 53(2):62-66.

Hagel, J. & Rayport, J.F. 1997. The coming battle for customer information. **Harvard Business Review**, Jan/Feb:53-65.

Hagel, J. & Singer, M. 1999. Private lives. **The McKinsey Quarterly**, Winter(1):7-13.

Hair, J.F., Anderson, R.E., Tatham, R.L. & Black, W.C. 1998. **Multivariate Data Analysis.** Fifth Edition. Upper Saddle River, New Jersey: Prentice-Hall.

Hanks, T. 2002. HIPAA Security and Privacy rules: working together. **PricewaterhouseCoopers**, January:1-5.

Harker, M.J. 1999. Relationship marketing defined? An examination of current relationship marketing definitions. **Marketing Intelligence & Planning**, 17(1):13-20.

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

Harris Interactive. 2000. Poll on Americans' fears on the Internet. **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.

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.

Harris Interactive. 2002a. Online consumer behaviour and concerns after September 11: a 2-wave survey. **Privacy & American Business**, Study no 15938, as discussed at the 8th Annual National Conference 'Managing the new privacy revolution', 20-22 March, Washington, DC.

Harris Interactive. 2002b. Privacy on and off the Internet: what consumers want. **Privacy & American Business**. Study no 15229:1-127.

Hattie, J.R. 1985. Methodology review: assessing unidimensionality of tests and items. **Applied Psychological Measurement**, 9:139-164.

Hawkins, D.I., Best, R.J. & Coney, K.A. 2001. **Consumer behaviour: building marketing strategy**. Eighth Edition. Boston, USA: McGraw-Hill.

Heide, J.B. & George, J. 1992. Do norms matter in marketing relationship? **Journal of Marketing**, 56(2):32-46.

Hildebrandt, L. 1987. Consumer retail satisfaction in rural areas: a reanalysis of survey data. **Journal of Economic Psychology**, 8:19-42.

Hirschman, A.O. 1970. **Exit, voice and loyalty responses to declines in firms, organisations and states**. Cambridge, MA: Harvard University Press.

Hirsh, L. 2002a. Digging out of the customer data landfill. **E-Commerce Times**, 4 March, http://www.ecommercetimes.com.

Hirsh, L. 2002b. The problem of fighting spam. **E-Commerce Times**, 26 March, http://www.ecommercetimes.com.

Hirsh, L. 2002c. Cutting spam at a cost. **E-Commerce Times**, 9 May, http://www.ecommercetimes.com.

Hoexter, C., Lyster, R. & Currie, I. 2002. **The New Constitutional and Administrative Law**. Volume II: Administrative Law. Lansdowne: Juta Law.

Hoffman, D.L., Novak, T.P. & Peralta, M. 1999. Building consumer trust online. **Communications of the Association for Computing Machinery**, 42(4):80-85.

Holvast, J., Madsen, W. & Roth, P. 2001. **The Global Encyclopedia of Data Protection Regulation**. Supplement No. 3. Netherlands, The Hague: Kluwer Law International.

Hovanyetz, S. 2002a. FTC: national DNC list coming by early 2003. **DM News**, 23 January, http://dmnews.com.

Hovanyetz, S. 2002b. Privacy corps site offers devices to deter telephone solicitors. **DM News**, 22 March, http://www.dmnews.com.

Hovanyetz, S. 2002c. CEO's stance on national DNC list puzzles some. **DM News**, 25 March, http://www.dmnews.com.

Hovanyetz, S. 2002d. FTC extends DNC comment period due to large response. **DM News**, 1 April, http://www.dmnews.com.

Hovanyetz, S. 2002e. States: don't pre-empt DNC lists. **DM News**, 19 April, http://www.dmnews.com.

Hovanyetz, S. 2002f. Court victory for unsolicited fax advertising. **DM News**, 1 April, http://www.dmnews.com.

http://cybertel.cybertrade.co.za

Hu, L. & Bentler, P.M. 1999. Cutoff criteria for fit indexes in covariance structure analysis' conventional criteria versus new alternatives. **Structural Equation Modeling**, 6(1):1-55.

Hussain, D.S. & Hussain, K.M. 1992. **Information Management: organisation, management and control of computer processing**. Great Britain: Prentice Hall.

Ivans, D. & Duval, C. 2002. **DMA legalBRIEF**, 20 August, http://www.dma.org.za

Jayson, S. 2002. Privacy: a matter of trust. **Privacy Daily**, 14 May:1-9, http://privacydaily.privacycouncil.com.

Jeffery, A. 1996/7. **Bill of Rights Report**. Johannesburg: South African Institute of Race Relations.

Johnson-Page, G.F. & Thatcher, R.S. 2001. B2C data privacy policies: current trends. **Management Decision**, 39(4):262-271.

Joshi, J.B.D., Aref, W.G., Ghafoor, A. & Spafford, E.H. 2001. Security models for web-based applications. **Communications of the ACM**, 44(2):38-44.

Judin, M. & Kisch, D.M. 2001. **Protection of information per se: a general overview**. Direct Marketing Association, February, http://www.dma.org.za.

Judin, M. 2000. The great spam of the century. **IMM Journal of Marketing**, 6(4):35-37.

Jupiter Media Metrix. 2002. Consumers worried about online privacy. **NUA Internet Surveys**, 4 June, http://www.nua.com/surveys.

Kandampully, J. & Duddy, R. 1999. Competitive advantage through anticipation, innovation and relationships. **Management Decision**, 37(1):51-56.

Kane, M. 2002. Standards – P3P is the official standard for online privacy. **CNET News.com**, 16 April, http://news.com.com/2100-1023-883756.html.

Katzenstein, H. & Sachs, W.S. 1992. **Direct Marketing**. Second Edition. New York, USA: MacMillan Publishing Company.

Kavali, S.G., Tzokas, N.X. & Saren, M.J. 1999. Relationship marketing as an ethical approach: philosophical and managerial considerations. **Management Decision**, 37(7):573-581.

Keller, G. & Warrack, B. 2000. **Statistics for management and economics**. California, USA: Duxbury Thomson Learning.

Kelly, S. 2001. Risk managers need web education. **Treasury & Risk Management**, 11(3):18-20.

Kelman, H.C. 1977. Privacy and research with human beings. **Journal of Social Issues**, 33(3):169-195.

Kieckhefer, B. 2003. Committee approves statewide do-not-call list. **Las Vegas Review-Journal**, 15 March, http://www.reviewjournal.com.

Kirwin, J. 2002. EC endorses Canadian data privacy as adequate to handle Europeans' data. **Privacy Law Watch**, 15 January, http://pubs.bna.com.

Kline, P. 1999. **An easy guide to factor analysis**. New York, USA: Routledge.

Kotler, P & Levy, S.J. 1969. Broadening the concept of marketing. **Journal of Marketing**, 33:10-15.

Kotler, P. 2000. **Marketing Management.** Millennium Edition. Upper Saddle River, New Jersey: Prentice Hall.

Kovacs, B. 2002. US Chamber of Commerce and PLI form privacy partnership: privacy tools made available to 30 000 small businesses. **Business Wire**, 22 February, http://www.privacyexchange.org/news/index.html.

Kumar, A. & Dillon, W.R. 1987. The interaction of measurement and structure in simultaneous equation models with unobservable variables. **Journal of Marketing**, 24:98-105.

Lambrechts, D. 2000. Regsrubriek 161. **Pollex**, 31 May:86-93.

Lattin, J.M., Carroll, J.D. & Green, P.E. 2003. **Analyzing Multivariate Data**. California, USA: Thomson Learning.

Laufer, R.S. & Wolfe, M. 1977. Privacy as a concept and a social issue: a multidimensional development theory. **Journal of Social Issues**, 33(3):22-42.

Lebo, H. 2001. The UCLA Internet Report 2001: Surveying the digital future. **UCLA Center for Communication Policy**, http://www.ccp.ucla.edu.

Long, G., Hogg, M.K., Hartley, M. & Angold, S.J. 1999. Relationship marketing and privacy: exploring the thresholds. **Journal of Marketing Practice: Applied Marketing Science**, 5(1):4-20.

Longley, D. & Shain, M. 1988. **Data and Computer security: dictionary of standard concepts and terms**. New York, USA: Macmillan, Stockton Press.

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

Louis Harris & Associates & Westin, A.F. 1998a. E-commerce and privacy: what net users want. **Privacy & American Business,** June, http://www.pandab.org/ecommercesurvey.htm.

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

Lovelock, P. 2002. China Internet firms form coalition to counter spammer, hacker haven image. **Privacy Law Watch,** 2 April, http://pubs.bna.com.

Loyle, D. 2002. Privacy under scrutiny. **Target Marketing**, 25(3):50-51.

Ludski, H. 2000. Bid to blind Big Brother. **Sunday Times**, 3 December:1.

Mabley, K. 1999. Privacy vs personalisation: a delicate balance. **Cyber Dialogue**, at http://www.cyberdialogue.com.

Machlis, S. 1997. Web sites rush to self-regulates. **Computerworld**, 32(19):2.

Magill, K. 2002. DMA guidelines mark major shift. **iMarketing** News, 5 February, http://www.privacyexchange.org/news/index.html.

Main, F. 2002. New research says 'opt-in' legislation would cost California billions. **PRNewswire**, 25 January, http://www.privacyexchange.org/news/index.html.

Malhotra, N.K. 1996. **Marketing research: an applied orientation**. Second Edition. New Jersey: Prentice Hall International.

Mann, L. 1997. **The development of a privacy scale**. Unpublished MBA research report. University of Cape Town, Cape Town.

Mariano, G. 2002. DoubleClick able to settle privacy suits. **CNET News.com**, 21 May, http://msnbc-cnet.com.com.

Marketing Federation of South Africa (MFSA). 2003. **SMS Code**, http://www.smscode.co.za.

Martins, J.H., Loubser, M. & Van Wyk, H. de J. 1996. **Marketing research: a South African approach**. First Edition. Pretoria: UNISA Press.

Marud, M. 2002. Online directory under fire. **Cape Argus**, 8 February:1.

Maruyama, G.M. 1998. **Basics of structural equation modeling**. California, USA: SAGE Publications.

Mason, M. 2002. EU publishes Directive on Data Protection in Electronic Communications. **PX NewsFlash**, 9 August, http://www.privacyexchange.org/news/index.html.

Massey, A. 2000. Privacy: data-mining leads to the rise of Little Brother. **Houston Business Journal**, 31(12):19.

Massey, A.P., Montoya-Weiss, M.M. & Holcom, K. 2001. Re-enigineering the customer relationship: leveraging knowledge assets at IBM. **Decision Support Systems**, 32:155-170.

Mayer, C.E. 2002. FTC Anti-telemarketer list would face heavy demand. **Washington Post**, 19 March:A07, http://www.washingtonpost.com.

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.

Mazumdar, A. 2002. European Commission gives final approval to model clauses to protect personal data. **Privacy Law Watch**, 29 January, http://pubs.bna.com.

Mazur, L. 2001. Consumers hold sway in laws on data protection. **Marketing**, 22 March:20.

McDonald, W.J. 1998. **Direct Marketing: an integrated approach**. Boston, USA: Irwin McGraw-Hill.

McGuire, D. 2002. FTC extends kids' privacy sliding scale. **Newsbytes**, 22 April, http://www.newsbytes.com.

McMahon, T. 2002. Standardized clauses can protect European online data transfers overseas. **Europemedia**, 23 January, http://www.europemedia.net.

McQuoid-Mason, D.J. 1978. **The Law of Privacy in South Africa**. Cape Town: Juta.

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.

Milne, G.R. 1997. Consumer participation in mailing lists: a field experiment. **Journal of Public Policy and Marketing**, 16(2):298-310.

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.

Minister of Communications. 2002. Republic of South Africa, Electronic Communications and Transactions Bill. **National Assembly**, http://www.erat.co.za/Profile.php.

Miyazaki, A.D. & Fernandez, A. 2001. Consumer perceptions of privacy and security risks for online shopping. **Journal of Consumer Affairs**, 35(1):27-44.

Mokgoro, Y. 2000. **2000 Annual Report.** South African Law Commission, http://wwwserver.law.wits.ac.za/salc/annrep.

Moorman, C. & Rust, R.T. 1999. The role of marketing. **Journal of Marketing**, 63:180-197.

Morgan, R.M. & Hunt, S.D. 1994. The commitment-trust theory of relationship marketing. **Journal of Marketing**, 58(3):20-38.

Morphy, E. 2002. IBM data mining research tackles privacy dilemma. **CRMDaily.com**, 31 May, http://www.crmdaily.com.

Morris-Lee, J. 1996. Privacy: it's everyone's business now! **Direct Marketing**, 58(12):40.

Naraine, R. 2002. Mcafee accepts increased buyout bid. **Internetnews**, 10 April, http://www.internetnews.com.

Nash, E.L. 1992. **The Direct Marketing Handbook**. Second Edition. New York, USA: McGraw-Hill.

Nash, K.S. 2000. Chief privacy officers: forces or figureheads? **Computerworld**, 34(46):62.

Neethling, J., Potgieter, J.M. & Visser, P.J. 1996. **Neethling's Law of Personality**. Durban: Butterworth.

Neethling, R. 2000. Fighting back the online Big Brothers. **Mail & Guardian**, 8-14 September:35.

Nethaway, R. 2002. Spammers making life miserable for Internet Users. **E-Commerce Times**, 17 May, http://www.ecommercetimes.com.

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. New York: McGraw-Hill.

O'Connell, P.L. 2002. The useless files and winning web trust. **The New York Times**, 20 June, http://www.nytimes.com.

O'Malley, L., Patterson, M. & Evans, M. 1999. **Exploring direct marketing**. London: International Thomson Business Press.

O'Shea, S. 2000. Data protection in the e-commerce era. **Accountancy Ireland**, 32(4):26-27.

Odell, P. 2002a. FTC takes heat over do-not-call list proposal. **Direct Newsline**, 1 May, http://www.industryclick.com.

Odell, P. 2002b. Minnesota governor to sign do-not-call bill into law. **Direct Newsline**, 13 May, http://www.industryclick.com.

Oldenburg, D. 2002. Anti-telemarketers send out a very busy signal. **Washington Post**, 20 February:C01, http://www.washingtonpost.com.

Opinion Research Corporation International and Westin, A.F. 2001. American Privacy Officers: a benchmark survey. **Privacy & American Business**, as discussed at the 8th Annual National Conference 'Managing the new privacy revolution', 20-22 March, Washington, DC.

Pallant, J. 2001. **SPSS survival manual: a step by step guide to data analysis using SPSS for windows (version 10)**. Philadelphia, USA: Open University Press.

Pels, J. 1999. Exchange relationships in consumer markets? **European Journal of Marketing**, 33(1/2):19-37.

Perreault, W.D & McCarthy, E.J. 2002. **Basic Marketing: a global-managerial approach**. Fourteenth Edition. Boston: Irwin McGraw-Hill.

Peter, J.P. & Olson, J.C. 1996. **Consumer behaviour and marketing strategy**. Fourth Edition. Chicago: Irwin.

Peter, J.P. & Olson, J.C. 2002. **Consumer behaviour and marketing strategy**. Sixth Edition. Chicago: Irwin.

Peter, J.P. 1981. Construct validity: a review of basic issues and marketing practices. **Journal of Marketing Research**, XVIII(May):133-145.

Peters, L.D. 1997. IT enabled marketing: a framework for value creation in customer relationships. **Journal of Marketing Practice: Applied Marketing Science**, 3(4):213-229.

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. 1998. Interactive marketing and the law: the future rise of unfairness. **Journal of Interactive Marketing**, 12(3):21-31.

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.

Pitcher, N. & Oorloff, J. 2002. Understanding and complying with Canada's Personal Information Protection and Electronic Documents Act. **PricewaterhouseCoopers: Global risk management solutions privacy practice**, March:1-5.

Pounder, C. & Kosten, F. 1992. **Managing data protection**. Second Edition. London: Butterworth-Heinemann.

Prabhaker, P.R. 2000. Who owns the online consumer? **Journal of Consumer Marketing**, 17(2):158-171.

Prescott, C.A. 1999. The new international marketing challenge: privacy. **Target Marketing**, 22(4):28.

Privacy Council. 2002. Data protection and security news. **Privacy Weekly**, 27 November, http://www.privacyweekly.com.

Pruitt, S. 2002. CFP: should privacy technologies be built in? **ITworld.com**, 22 April, http://www/itworld.com.

Rainie, H. 2002. Congressional hearing on opinion surveys: what consumers have to say about information privacy. **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.

Raney, R.F. 2002. Questions about online data. **The New York Times**, 3 June, http://www.nytimes.com.

Raul, A.C. & Tyler, A.L. 2001. The USA Patriot Act of 2001: Electronic Surveillance and Privacy. **Analysis & Perspectives: Privacy & Security Law Report**, Washington, DC: The Bureau of National Affairs:21-26.

Ravald, A. & Grönroos, C. 1996. The value concept and relationship marketing. **European Journal of Marketing**, 30(2):19-30.

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

Rawwas, M.Y.A., Strutton, D. & Johnson, L.W. 1996. An exploratory investigation of the ethical values of American and Australian consumers: direct marketing implications. **Journal of Direct Marketing**, 19(4):52-63.

Reichheld, F.F. & Schefter, P. 2000. Your secret weapon on the Web. **Harvard Business Review**, July-August:105-113.

Roberts, M.L. & Berger, P.D. 1989. **Direct Marketing Management**. Englewood Cliffs, New Jersey: Prentice-Hall.

Roberts, M.L. 1997. Expanding the role of the direct marketing database. **Journal of Direct Marketing**, 11(4):27-35.

Roberts, S., Feit, M. & Bly, R.W. 2001. **Internet direct mail: the complete guide to successful e-mail marketing campaigns**. Chicago: NTC Business Books.

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

Rudraswamy, V. & Vance, D.A. 2001. Transborder data flows: adoption and diffusion of protective legislation in the global electronic commerce environment. **Logistics Information Management**, 14(1/2):127-136.

SAARF. 2001. **AMPS2001B**, available from the South African Advertising Research Foundation, Johannesburg.

Sahd, B.G. 1998. **Understanding and measuring privacy in the information age: the refinement and application of a privacy scale**. Unpublished MBA research report. University of Cape Town, Cape Town.

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

SAS Institute Inc. 2000a. **BMDP 4M**. Version 8.2, Cary NC, USA.

SAS Institute Inc. 2000b. **Proc Calis**. Version 8.2, Cary NC, USA.

Saunders, C. 2002. MMA pushes privacy. **InternetNews**, 19 March, http://www.internetnews.com/IAR/article/0,,12994451,00.html.

Schultz, R. 2002a. FTC releases proposals to national do-not-call list. **Direct Newsline**, 23 January, http://www.industryclick.com.

Schultz, R. 2002b. Online group creates and e-mail seal. **Direct Newsline**, 31 January, http://www.industryclick.com.

Schumacker, R.E. & Lomax, R.G. 1996. **A beginner's guide to structural equation modelling**. New Jersey, USA: Lawrence Erlbaum Associates Publishers.

Schwartz, D.O. 1998. Sharing responsibility for e-commerce and the privacy issue. **Direct Marketing**, 61(2):48-52.

Selnes, F. 1998. Antecedents and consequences of trust and satisfaction in buyer-seller relationships. **European Journal of Marketing**, 32(3/4):305-322.

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

Sheth, J.N., Mittal, B. & Newman, B.I. 1999. **Customer behavior: consumer behavior and beyond**. Orlando, USA: The Dryden Press.

Silver, B. 2000. DoubleClick doing a double take. **Marketing Mix**, 18(3):17.

Singh, J. 1988. Consumer complaint intentions and behaviour: definitional and taxonomical issues. **Journal of Marketing**, 52(January):93-107.

Smith, H.J. 2001. Information privacy and marketing: what the US should learn from Europe. **California Management Review**, 43(2):8-33.

Smith, H.J., Milberg, S.J. & Burke, S.J. 1996. Information privacy: measuring individuals' concerns about organizational practices. **MIS Quarterly**, 20(2):167-197.

Smith, J. 2002. States are concerned about FTC's national do-not-call registry. **Privacy Daily**, 16 April:3, http://www.privacydaily.privacycouncil.com.

Smith, T.B. 1999. Comment: programs needed to comply with privacy law. **American Banker**, 164(155):8.

Spangenberg, H.H. & Theron, C.C. 2002. Development of uniquely South African leadership questionnaire. **South African Journal of Psychology**, 32(2):9-25.

StatSoft. 1995. **Statistica Volume 1: General conventions and statistics**. Tulsa OK, USA.

Steenkamp, J.E.M. & Van Trijp, H.C.M. 1991. The use of LISREL in validating marketing constructs. **International Journal of Research in Marketing**, 8:283-299.

Stein, R.W. 2000. Overcoming privacy rules. **Best Review**, 101(3):121.

Stern, S. 2002. Will feds tackle telemarketers? **The Christian Science Monitor**, 15 April, http://www.csmonitor.com.

Stone, E.F., Gueutal, H.G., Gardner, D.G. & McClure, S. 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organisations. **Journal of Applied Psychology**, 68(3):459-468.

Stones, L. 2002. Business urged to use delay to its advantage. **Business Day**, 15 April:3.

Sudman, S. & Blair, E. 1998. **Marketing research: a problem solving approach**. USA: McGraw Hill.

Sue-Len, H. 2001. Risks of e-business. **New Straights Times-Management Times**, 2 April.

Sullivan, B. 2002. Net thieves are caught. **Privacy Daily**, 16 April:6, http://www.privacydaily.privacycouncil.com.

Tabachnick, B.G. & Fidell, L.S. 2001. Using multivariate statistics. Fourth Edition. Needham Heights, MA: Allyn and Bacon.

Takala, T. & Uusitalo, O. 1996. An alternative view of relationship marketing: a framework for ethical analysis. **European Journal of Marketing**, 30(2):45-60.

Tandberg, A. 2002. Memo from FEDMA: European Parliament considers Electronic Communication and Data Privacy Directive. **Federation of European Direct Marketing Associations**, http://www.the-dma.org.

Taylor, H. 2002. Congressional hearing on opinion surveys: what consumers have to say about information privacy. **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.

Taylor, R.E., Vassar, J.A. & Vaught, B.C. 1995. The beliefs of marketing professionals regarding consumer privacy. **Journal of Direct Marketing**, 9(4):38-46.

Tedeschi, B. 2002a. Privacy is a common issue online. **The New York Times**, 3 June, http://www.nytimes.com.

Tedeschi, B. 2002b. Technology briefing. **The New York Times**, 19 June, http://www.nytimes.com.

Telkom. 2002. **CyberTrade**, http://www.cybertrade.co.za

Temkin, S. 2002. Experts say bill offers exciting opportunities. **Business Day**, 5 March:2.

Thibodeau, P. 2002. International group eyes IT security principles, standards. **InfoWorld**, 21 May, http://staging.inforworld.com.

TNS Intersearch. 2001. ABC News expose on identity theft. **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.

Tomasula, D. 2002a. California law firm sues online marketer, says lawyers got spam. **DM News**, 25 March, http://www.dmnews.com.

Tomasula, D. 2002b. Plaintiffs accomplish goals in DoubleClick privacy suit. **iMarketing News**, 2 April, http://wwww.imarketingnews.com.

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.

Turner, M.A. 2002. Activities and supporters guide. **The Information Policy Institute**, as discussed at the 8th Annual National Conference 'Managing the new privacy revolution', 20-22 March, Washington, DC.

Tweney, D. 1998. The consumer battle over online information privacy has just begun. **InfoWorld**, 20(25):66.

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.

Van Wyk, D., Dugard, J., De Villiers, B. & Davis, D. 1996. **Rights and Constitutionalism: The new South African Legal Order**. Great Britian: Oxford University Press.

Venter, Z. 2002. Telkom customer privacy case settled. **Pretoria News**, 20 February:3.

Veysey, S. 2001. Industry not ready for e-risks: study. **Business Insurance**, 35(6):1-2.

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

Walczuch, R.M. & Steeghs, L. 2001. Implications of the new EU Directive on data protection for multinational corporations. **Information Technology & People**, 14(2):142-162.

Wang, H., Lee, M.K.O. & Wang, C. 1998. Consumer privacy concerns about Internet marketing. **Communications of the ACM**, 41(3):63-70.

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

Warren, S.D. & Brandeis, L.D. 1890. The right to privacy. **Harvard Law Review**, IV(5):193-220.

Wazeka, R. 2000. Internet privacy. **Success**, 47(4):64.

Wearden, G. 2002. EU shifts stance3 on cookies. **CNET News.com**, 18 April, http://news.com.com.

Webster, F.E. 1988. The rediscovery of the marketing concept. **Business Horizons**, May/June:29-39.

Webster, F.E. 1992. The changing role of marketing in the corporation. **Journal of Marketing**, 56:1-17.

Webster. F.E. 1994. Defining the new marketing concept (Part 1). **Marketing Management**, 2(4):23-31.

Westin, A.F. 2002. Congressional hearing on opinion surveys: what consumers have to say about information privacy. **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.

Wientzen, H. R. & Weinstein, L. 1997. Private lives: public records. **Computerworld**, 31(36):88-89.

Wientzen, H.R. 2000. What is the Internet's impact on direct marketing today and tomorrow? **Journal of Interactive Marketing**, 14(3):74-78.

Williams, C.J. 1999. Germans speak up to defend European privacy laws. **Los Angeles Times**, 2 April, http://www.latimes.com.

Williams, J. 1991. Professional standards in information handling and employee training. **Journal of Direct Marketing**, 5(1):57-61.

Winston, J. 1999. Calling for a do-not-call list with teeth. **Target Marketing**, 22(7):65.

Woodward, D. 2000. Smart security. **The British Journal of Administrative Management**, 18:22-23.

Yudelson, J. 1999. Adapting to McCarthy's four P's for the Twenty-First Century. **Journal of Marketing Education**, 21(1):60-67.

Zikmund, W.G. 2000. **Business Research Methods**. Sixth Edition. Fort Worth: The Dryden Press, Harcourt College Publishers.

Zikmund, W.G. 2003. **Business Research Methods**. Seventh Edition. Fort Worth: The Dryden Press, Harcourt College Publishers.

Zineldin, M. 2000. Beyond relationship marketing: technologicalship marketing. **Marketing Intelligence & Planning**, 18(1):9-23.

Zinkewicz, P. 2001. Survey shows cyber-risk little understood. **Rough Notes**, 144(4):50-51.

APPENDIX 1

INFORMATION PRIVACY QUESTIONNAIRE

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

HOUSEHOLD QUESTIONNAIRE – INFORMATION PRIVACY

Respondent number							1			3
Telephone code	4									11

Hello, I'm _____ from the Bureau of Market Research and we are conducting research about important national issues. I would like to speak to the person in the household who most recently celebrated his or her birthday, provided he or she is 18 years or older.

Birthday-respondent identified	1	Other respondent identified	2	12

I'm _____ from the Bureau of Market Research and we are conducting research about important national issues. I would like to ask you a few questions. There are no right or wrong answers, and all your answers are treated as confidential. Your name will not be connected to the answers you provide.

The study addresses people's opinions on the confidentiality of their personal information. When you buy from companies, they sometimes require some of your personal information (such as your name, address, telephone number) before the sale can take place. And when they have your information, they sometimes use this to send you communication (like advertising material). I am going to ask you questions on how you feel about companies who collect and use your information. Remember, there are no right or wrong answers.

Each time I am going to read you a statement. Please tell me whether you disagree strongly, disagree slightly, are neutral (do not agree or disagree), agree slightly or agree strongly with each statement.

(READ EACH ITEM) – do you disagree strongly, disagree slightly, are neutral, agree slightly, or agree strongly?

STATEMENT	Disagree strongly	Disagree slightly	Neutral	Agree slightly	Agree strongly	Don't know	Refuse	
1. Companies generally ask too much personal information from consumers.	1	2	3	4	5	6	7	13
2. You do not mind to provide a lot of personal information if you think it is necessary.	1	2	3	4	5	6	7	14
3. Companies seldom collect personal information from consumers without their permission.	1	2	3	4	5	6	7	15

STATEMENT	Disagree strongly	Disagree slightly	Neutral	Agree slightly	Agree strongly	Don't know	Refuse	
4. You are confident that you can prevent companies from collecting personal information that you would like to keep secret.	1	2	3	4	5	6	7	16
5. Most companies collect personal information from consumers in order to provide them with products and services to better suit their needs.	1	2	3	4	5	6	7	17
6. You are satisfied when companies collect your personal information as a means to provide you with products and services which better suit your needs.	1	2	3	4	5	6	7	18
7. You believe that most companies allow their consumers to have access to their personal information kept by the companies.	1	2	3	4	5	6	7	19
8. You feel it is important to have access to the personal information companies keep of you.	1	2	3	4	5	6	7	20
9. You believe that companies have adequate measures in place to ensure that all personal information in their records is accurate.	1	2	3	4	5	6	7	21
10. You feel concerned that companies do not devote enough time and effort to ensure that your personal information is accurate while in their possession.	1	2	3	4	5	6	7	22
11. Personal information is safe while stored in a company's records.	1	2	3	4	5	6	7	23
12. You fear that your personal information may not be safe while stored in a company's records.	1	2	3	4	5	6	7	24
13. Most consumers have control over the ways their personal information is used by companies.	1	2	3	4	5	6	7	25
14. You are satisfied about the control you have over the ways companies use your personal information.	1	2	3	4	5	6	7	26
15. You believe that companies regularly use consumers' information for other purposes than that for which it was collected.	1	2	3	4	5	6	7	27

STATEMENT	Disagree strongly	Disagree slightly	Neutral	Agree slightly	Agree strongly	Don't know	Refuse	
16. You do not mind when companies use your personal information for other purposes than those provided when they collected your information.	1	2	3	4	5	6	7	28
17. You believe that consumers' personal information is often misused by companies.	1	2	3	4	5	6	7	29
18. You are concerned about the possible misuse of your personal information by companies.	1	2	3	4	5	6	7	30
19. Companies regularly share personal information with other companies without the permission of the individuals to whom the information belongs.	1	2	3	4	5	6	7	31
20. You are uncomfortable when companies share your personal information with other companies without asking your permission first.	1	2	3	4	5	6	7	32
21. You believe that companies regularly share personal information of consumers with other companies, so that these other companies could offer products and services to consumers.	1	2	3	4	5	6	7	33
22. You feel it is unacceptable when a company shares your personal information with other companies so that those companies can offer their products and services to you.	1	2	3	4	5	6	7	34
23. Companies always provide their customers with the opportunity to request the removal of their names and addresses from records that are sold to other companies.	1	2	3	4	5	6	7	35
24. You are concerned when companies do not provide you with an opportunity to remove your name and address from any records that it provides to other companies.	1	2	3	4	5	6	7	36
25. Companies send consumers too much unrequested advertising material that is not of interest to them.	1	2	3	4	5	6	7	37

STATEMENT	Disagree strongly	Disagree slightly	Neutral	Agree slightly	Agree strongly	Don't know	Refuse	
26. It bothers you that you receive so much unrequested advertising material that is of no interest to you.	1	2	3	4	5	6	7	38
27. Too many companies call consumers at their homes to sell products and services to them.	1	2	3	4	5	6	7	39
28. You do not mind when you receive telephone calls at your home from companies wanting to sell products and services to you.	1	2	3	4	5	6	7	40
29. Consumers are not interested in getting information about new products and services from companies with which they have not done business before.	1	2	3	4	5	6	7	41
30. You are pleased when you receive information about new products and services from companies with which you have not done business before.	1	2	3	4	5	6	7	42
31. Legislation should prevent a company from sharing your personal information with other companies without your permission.	1	2	3	4	5	6	7	43
32. You would request a company to remove your personal information from their records if you suspected that they were misusing it.	1	2	3	4	5	6	7	44
33. Companies must have privacy protection policies to make provision for customers who would not like to receive unrequested advertising material.	1	2	3	4	5	6	7	45
34. Government should restrict companies to collecting only the information needed for a specific transaction.	1	2	3	4	5	6	7	46
35. You would support any initiatives that will enable you to stop companies from sending you unrequested advertising material.	1	2	3	4	5	6	7	47
36. Companies should have privacy protection policies indicating that no personal information will be provided to other companies without consent from their customers.	1	2	3	4	5	6	7	48

STATEMENT	Disagree strongly	Disagree slightly	Neutral	Agree slightly	Agree strongly	Don't know	Refuse	
37. Government should do more to protect the safety of personal information.	1	2	3	4	5	6	7	49
38. You would request having your personal information removed from any company's records if they sell the information to others.	1	2	3	4	5	6	7	50
39. Companies should have privacy protection policies indicating the reasons for collecting personal information from consumers.	1	2	3	4	5	6	7	51
40. Government should limit companies' use of personal information to only that purpose for which it was collected.	1	2	3	4	5	6	7	52
41. You would support a company's efforts that will ensure that your personal information is safely kept.	1	2	3	4	5	6	7	53
42. Companies should use independent auditing firms to confirm that they use the personal information of consumers, as promised in the companies' privacy policies.	1	2	3	4	5	6	7	54
43. Government should limit unrequested advertising material sent to consumers.	1	2	3	4	5	6	7	55
44. You would refuse to provide your personal information to a company who cannot provide reasons why they want to collect your personal information.	1	2	3	4	5	6	7	56
45. Companies should have privacy protection policies indicating how they will protect the customer's information while it is in their possession.	1	2	3	4	5	6	7	57

STATEMENTS (without a neutral opinion option)	Disagree strongly	Disagree slightly	Agree slightly	Agree strongly	Don't know	Refuse	
46. Consumers have lost all control over how personal information is collected and used by companies.	1	2	3	4	5	6	58
47. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	1	2	3	4	5	6	59
48. Existing laws and organisational practices provide a reasonable level of protection for consumer privacy.	1	2	3	4	5	6	60

Please answer Yes or No to the following questions:

QUESTIONS	YES	NO	Don't know	Refuse	
49. Have you ever refused to give information to a company because you thought it was not really needed or it was too personal?	1	2	3	4	61
50. Have you ever requested a company to remove your name and address from records that they use for marketing purposes?	1	2	3	4	62
51. Have you ever notified a company that you do not want to receive their unrequested advertising material?	1	2	3	4	63
52. Have you ever requested that a company not share your personal information with any other company?	1	2	3	4	64
53. Have you ever requested a company to inform you which measures they use to keep your personal information safe?	1	2	3	4	65
54. Have you ever personally been a victim of a situation you felt was an invasion of your private information?	1	2	3	4	66
55. Are you aware of any options to remove your name from records of companies?	1	2	3	4	67
56. Have you ever purchased anything via the Internet?	1	2	3	4	68
57. Do you make use of Internet banking services?	1	2	3	4	69
58. During the past year, have you personally bought something from a catalogue or brochure sent to you?	1	2	3	4	70
59. During the past year, have you personally bought any product or service offered to you by a telephone call?	1	2	3	4	71
60. During the past year, have you personally called a toll-free (0800) number to order something?	1	2	3	4	72

Finally, I have a few questions that are for classification purposes only and will be treated as confidential.

(Interviewer) If person asks why certain demographic and personal questions are asked?
These questions are used for classification purposes to, for example, determine what the opinions of people in a particular age groups are, and how this differs from people in other age groups. No information (name, tel no, etc) that can identify you, is recorded anywhere on the questionnaire or elsewhere.

61. What is your year of birth? *(enter as a 4-digit number, e.g. 1969)* 73 | | | | | 76

62. What is your home language?

English	01
Afrikaans	02
Xhosa	03
Zulu	04
Setswana	05
Sesotho	06
Sepedi	07
Swati	08
Tshivenda	09
Xitsonga	10
Ndebele	11
Other (specify)	12

77 [ ][ ] 78

63. What is the highest level of education you have completed or the highest qualification you have received?

Lower than Grade 10 (Standard 8)	1
Grade 10 (Standard 8)	2
Grade 12 (Standard 10)	3
Degree/Diploma	4
Post graduate/ Higher diploma	5

[ ] 79

64. Which one of the following best describes your employment status? (*Please select one response only)*

Employed full time	1
Employed part time	2
Self-employed (you work for yourself)	3
Not employed	4
Student	5
Homemaker/Housewife	6
Pensioner/Retired	7
Unfit for work	8

[ ] 80

65. Which of the following categories best describes your personal total monthly income before any deductions?

Less than R2000	1
R2001-R4000	2
R4001-R6000	3
R6001-R8000	4
R8001-R10000	5
R10001-R15000	6
R15000 plus	7

[ ] 81

THANK RESPONDENT; END INTERVIEW

66. GENDER (by means of deduction):

Male	1
Female	2

☐ 82

67. POPULATION GROUP (by means of deduction):

Black / African	1
Coloured	2
Indian / Asian	3
White	4

☐ 83

UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

HUISHOUDINGSVRAELYS - INLIGTINGSPRIVAATHEID

Respondentnommer						1				3
Telefoonkode	4									11

Goeie dag, ek is _____ van die Buro vir Marknavorsing en ons doen navorsing oor belangrike nasionale aangeleenthede. Ek sal graag met die persoon in die huishouding wat die mees onlangste verjaar het wil gesels, gegewe dat hy of sy 18 jaar of ouer is.

Verjaardag-respondent geïdentifiseer	1	Ander respondent geïdentifiseer	2	12

Ek is _____ van die Buro vir Marknavorsing en ons doen navorsing oor belangrike nasionale aangeleenthede. Ek sal u graag 'n paar vrae wil vra. Daar is geen verkeerde of regte antwoorde nie, en alle antwoorde word vertroulik hanteer. U naam sal aan geen van die antwoorde wat u gee, gekoppel kan word nie.

Die studie gaan oor u sienings rakende die vertroulikheid van persoonlike inligting. Wanneer u van ondernemings aankoop, verlang hulle somtyds u persoonlike inligting (soos u naam, adres, telefoonnommer) voordat die kooptransaksie kan plaasvind. En wanneer ondernemings u inligting het, gebruik hulle dit soms om aan u kommunikasie (soos advertensiemateriaal) te stuur. Ek gaan u vra hoe u voel oor ondernemings wat u inligting insamel en gebruik. Onthou, daar is geen regte of verkeerde antwoord nie.

Ek gaan telkens vir u 'n stelling lees, en dan moet u vir my sê of u glad nie met die stelling saamstem nie, tot 'n mate verskil, neutraal is (nie saamstem òf verskil nie), tot 'n mate saamstem, of volkome met die stelling saamstem.

(LEES ELKE ITEM) – Stem u glad nie saam nie, verskil u tot 'n mate, is u neutraal, stem u tot 'n mate saam, of stem u volkome saam?

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
1. Ondernemings vra gewoonlik te veel persoonlike inligting van verbruikers.	1	2	3	4	5	6	7	13
2. Dit pla u nie om 'n klomp persoonlike inligting te verskaf as u dink dit is nodig nie.	1	2	3	4	5	6	7	14
3. Ondernemings samel selde verbruikers se persoonlike inligting in sonder hulle toestemming.	1	2	3	4	5	6	7	15

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
4. U is vol vertroue dat u ondernemings kan verhoed om persoonlike inligting in te samel wat u graag geheim sou wou hou.	1	2	3	4	5	6	7	16
5. Meeste ondernemings samel persoonlike inligting van verbruikers in, sodat produkte en dienste aan hulle voorsien kan word wat beter aan hulle behoeftes sal voldoen.	1	2	3	4	5	6	7	17
6. U is tevrede wanneer ondernemings u persoonlike inligting insamel, sodat hulle produkte en dienste aan u kan bied wat beter aan u behoeftes voldoen.	1	2	3	4	5	6	7	18
7. U is van mening dat meeste ondernemings dit vir verbruikers moontlik maak om toegang te hê tot hulle persoonlike inligting wat deur die ondernemings gehou word.	1	2	3	4	5	6	7	19
8. U voel dit is belangrik om toegang te hê tot die persoonlike inligting wat ondernemings van u hou.	1	2	3	4	5	6	7	20
9. U is van mening dat ondernemings voldoende maatreëls in plek het om te verseker dat alle persoonlike inligting in hulle rekords akkuraat is.	1	2	3	4	5	6	7	21
10. U voel bekommerd dat ondernemings nie genoeg tyd en moeite bestee om te verseker dat u persoonlike inligting akkuraat is terwyl dit in hulle besit is nie.	1	2	3	4	5	6	7	22
11. Persoonlike inligting is veilig terwyl dit in 'n onderneming se rekords gehou word.	1	2	3	4	5	6	7	23
12. U vrees dat u persoonlike inligting nie veilig is terwyl dit in 'n onderneming se rekords gehou word nie.	1	2	3	4	5	6	7	24
13. Meeste verbruikers het beheer oor die wyses waarop hulle persoonlike inligting deur ondernemings gebruik word.	1	2	3	4	5	6	7	25
14. U is tevrede met die beheer wat u het oor die wyses waarop ondernemings u persoonlike inligting gebruik.	1	2	3	4	5	6	7	26

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
15. U is van mening dat ondernemings gereeld verbruikers se inligting gebruik vir ander doeleindes as waarvoor dit ingesamel is.	1	2	3	4	5	6	7	27
16. U gee nie om wanneer ondernemings u persoonlike inligting vir ander doeleindes gebruik as die doel waarvoor dit aanvanklik ingesamel is nie.	1	2	3	4	5	6	7	28
17. U is van mening dat verbruikers se persoonlike inligting dikwels deur ondernemings misbruik word.	1	2	3	4	5	6	7	29
18. U is bekommerd oor die moontlike misbruik van u persoonlike inligting deur ondernemings.	1	2	3	4	5	6	7	30
19. Ondernemings maak gereeld persoonlike inligting aan ander ondernemings bekend sonder die toestemming van die individue aan wie die persoonlike inligting behoort.	1	2	3	4	5	6	7	31
20. U is ongemaklik wanneer ondernemings u persoonlike inligting met ander ondernemings deel sonder om eers u toestemming te vra.	1	2	3	4	5	6	7	32
21. U is van mening dat ondernemings gereeld persoonlike inligting van hulle verbruikers met ander ondernemings deel, sodat hierdie ander ondernemings produkte en dienste aan verbruikers kan aanbied.	1	2	3	4	5	6	7	33
22. U voel dit is onaanvaarbaar wanneer 'n onderneming u persoonlike inligting met ander ondernemings deel, sodat daardie ondernemings hulle produkte en dienste aan u kan aanbied.	1	2	3	4	5	6	7	34
23. Ondernemings gee altyd aan hulle kliënte 'n geleentheid om te vra dat hulle name en adresse van die rekords wat aan ander ondernemings verkoop word, geskrap word.	1	2	3	4	5	6	7	35
24. U is bekommerd wanneer ondernemings u nie 'n geleentheid gee om u naam en adres te verwyder van enige van hulle rekords wat hulle aan ander ondernemings gee nie.	1	2	3	4	5	6	7	36

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
25. Ondernemings stuur te veel ongevraagde advertensiemateriaal aan verbruikers waarin hulle nie belang stel nie.	1	2	3	4	5	6	7	37
26. Dit hinder u dat u so baie ongevraagde advertensiemateriaal ontvang waarin u nie belangstel nie.	1	2	3	4	5	6	7	38
27. Te veel ondernemings skakel verbruikers by die huis om aan hulle produkte en dienste te verkoop.	1	2	3	4	5	6	7	39
28. U gee nie om wanneer u telefoonoproepe tuis ontvang van ondernemings wat produkte en dienste aan u wil verkoop nie.	1	2	3	4	5	6	7	40
29. Verbruikers stel nie belang om inligting oor nuwe produkte en dienste van ondernemings te ontvang met wie hulle nog nie vantevore besigheid gedoen het nie.	1	2	3	4	5	6	7	41
30. U is ingenome wanneer u inligting oor nuwe produkte en dienste ontvang vanaf ondernemings met wie u nog nie voorheen besigheid gedoen het nie.	1	2	3	4	5	6	7	42
31. Wetgewing behoort 'n onderneming te verhoed om u persoonlike inligting aan ander ondernemings beskikbaar te stel sonder u toestemming.	1	2	3	4	5	6	7	43
32. U sal 'n onderneming versoek om u persoonlike inligting van hulle rekords te verwyder indien u vermoed dat hulle besig is om dit te misbruik.	1	2	3	4	5	6	7	44
33. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê, ten einde voorsiening te maak vir kliënte wat nie graag ongevraagde advertensie materiaal wil ontvang nie.	1	2	3	4	5	6	7	45
34. Die regering moet ondernemings beperk om slegs dié inligting in te samel wat nodig is vir 'n spesifieke transaksie.	1	2	3	4	5	6	7	46

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
35. U sal enige inisiatiewe ondersteun wat u in staat sal stel om ongevraagde advertensie materiaal wat ondernemings aan u stuur, te stop.	1	2	3	4	5	6	7	47
36. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê, wat aandui dat geen persoonlike inligting aan ander ondernemings voorsien sal word sonder die goedkeuring van hulle kliënte nie.	1	2	3	4	5	6	7	48
37. Die regering moet meer doen om die veiligheid van persoonlike inligting te beskerm.	1	2	3	4	5	6	7	49
38. U sal versoek dat u persoonlike inligting verwyder moet word van enige ondernemingsrekords indien hulle die inligting aan ander verkoop word.	1	2	3	4	5	6	7	50
39. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê wat die redes aandui waarom hulle mense se persoonlike inligting insamel.	1	2	3	4	5	6	7	51
40. Die regering moet die gebruik van persoonlike inligting deur ondernemings beperk tot slegs dié doel waarvoor dit ingesamel is.	1	2	3	4	5	6	7	52
41. U sal 'n onderneming se pogings ondersteun wat sal verseker dat u persoonlike inligting veilig gehou word.	1	2	3	4	5	6	7	53
42. Ondernemings moet onafhanklike ouditfirmas gebruik om te bevestig dat hulle verbruikers se persoonlike inligting gebruik, soos beloof in die ondernemings se beleid vir die beskerming van privaatheid.	1	2	3	4	5	6	7	54
43. Die regering moet 'n beperking plaas op ongevraagde advertensiemateriaal wat aan verbruikers gestuur word.	1	2	3	4	5	6	7	55
44. U sal weier om u persoonlike inligting aan 'n onderneming te voorsien wat nie redes kan verskaf waarom hulle u persoonlike inligting wil hê nie.	1	2	3	4	5	6	7	56

STELLING	Stem glad nie saam nie	Verskil tot 'n mate	Neutraal	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
45. Ondernemings moet 'n 'n beleid vir die beskerming van privaatheid hê, wat aandui hoe hulle die kliënt se inligting sal beskerm terwyl dit in hulle besit is.	1	2	3	4	5	6	7	57

STELLINGS (sonder 'n middelpunt)	Stem glad nie saam nie	Verskil tot 'n mate	Stem tot 'n mate saam	Stem volkome saam	Weet nie	Weier	
46. Verbruikers het alle beheer oor die wyse waarop ondernemings persoonlike inligting insamel en gebruik, verloor.	1	2	3	4	5	6	58
47. Meeste besighede hanteer die persoonlike inligting wat hulle oor verbruikers insamel, op 'n behoorlike en vertroulike wyse.	1	2	3	4	5	6	59
48. Bestaande wetgewing en ondernemingspraktyke voorsien 'n redelike mate van beskerming vir verbruikersprivaatheid.	1	2	3	4	5	6	60

Beantwoord asseblief JA of NEE op die volgende vrae:

VRAAG	JA	NEE	Weet nie	Weier	
49. Het u al ooit geweier om inligting aan 'n onderneming te gee omdat u gedink het dit nie regtig nodig was nie, of dat dit té persoonlik was?	1	2	3	4	61
50. Het u al ooit versoek dat 'n onderneming u naam en adres van die rekords wat hulle vir bemarkingsdoeleindes gebruik, moet verwyder?	1	2	3	4	62
51. Het u al ooit 'n onderneming in kennis gestel dat u nie van hulle ongevraagde advertensiemateriaal wil ontvang nie?	1	2	3	4	63
52. Het u al ooit versoek dat die persoonlike inligting wat u aan 'n onderneming voorsien het, nie aan enige ander onderneming beskikbaar gestel mag word nie?	1	2	3	4	64
53. Het u al ooit 'n onderneming versoek dat hulle u moet inlig oor die maatreëls wat hulle gebruik om u persoonlike inligting veilig te hou?	1	2	3	4	65
54. Was u persoonlik al ooit 'n slagoffer van 'n situasie wat u gevoel het 'n skending van u private inligting was?	1	2	3	4	66
55. Is u bewus van enige wyses om u naam van die rekords van ondernemings te verwyder?	1	2	3	4	67
56. Het u al ooit enigiets deur middel van die Internet aangekoop?	1	2	3	4	68
57. Maak u gebruik van Internet-bankdienste?	1	2	3	4	69

VRAAG	JA	NEE	Weet nie	Weier	
58. Het u persoonlik, gedurende die afgelope jaar, iets gekoop uit 'n katalogus of brosjure wat aan u gestuur is?	1	2	3	4	70
59. Het u persoonlik, gedurende die afgelope jaar, enige produkte of dienste wat telefonies aan u aangebied is, gekoop?	1	2	3	4	71
60. Het u gedurende die afgelope jaar 'n tolvry (0800) nommer geskakel om iets te bestel?	1	2	3	4	72

Ten laaste het ek 'n paar vrae wat slegs vir klassifikasiedoeleindes is en wat vertroulik hanteer sal word.

(Onderhoudvoerder) Indien 'n persoon vra waarom sekere demografiese en persoonlike vrae gevra word?
Dit word vir klassifikasiedoeleindes gebruik om, byvoorbeeld te bepaal wat die sienings van persone in bepaalde ouderdomsgroepe is en hoe dit van dié in ander oudersdomsgroepe verskil. Geen inligting (naam, tel no ens) wat u kan identifiseer, word op die vraelys of elders aangeteken nie.

61. In watter jaar is u gebore? *(teken aan as a 4-syfer nommer, bv. 1969)* 73 [ ][ ][ ][ ] 76

62. Wat is u huistaal?

Engels	01
Afrikaans	02
Xhosa	03
Zulu	04
Setswana	05
Sesotho	06
Sepedi	07
Swati	08
Tshivenda	09
Xitsonga	10
Ndebele	11
Ander (spesifiseer)	12

77 [ ][ ] 78

63. Wat is die hoogste vlak van opleiding wat u voltooi het of die hoogste kwalifikasie wat u verwerf het?

Laer as Graad 10 (Standerd 8)	1
Graad 10 (Standerd 8)	2
Graad 12 (Standerd 10)	3
Graad/Diploma	4
Nagraadse kwalifikasie/ Hoër diploma	5

[ ] 79

64. Watter een van die volgende beskryf u werkstatus die beste? *(Merk slegs een respons)*

Voltyds indiens	1
Deeltyds indiens	2
Selfindiensgeneem (u werk vir uself)	3
Het nie werk nie	4
Student	5
Tuisteskepper/Huisvrou	6
Pensioentrekker/Afgetree	7
Ongeskik vir werk	8

[ ] 80

65. Watter van die volgende kategorieë beskryf u persoonlike maandelikse inkomste voor enige aftrekkings, die beste?

Minder as R2000	1
R2001-R4000	2
R4001-R6000	3
R6001-R8000	4
R8001-R10000	5
R10001-R15000	6
R15000 plus	7

[ ] 81

BEDANK DIE RESPONDENT; EINDIG DIE ONDERHOUD

66. GESLAG (deur middel van afleiding):

Manlik	1
Vroulik	2

[ ] 82

67. BEVOLKINGSGROEP (deur middel van afleiding):

Swart	1
Kleurling	2
Indiër / Asiër	3
Blank	4

[ ] 83

APPENDIX 2

INFORMATION PRIVACY QUESTIONNAIRE FOR PRE-TESTING

HOUSEHOLD QUESTIONNAIRE – INFORMATION PRIVACY – PRE-TESTING

Respondent number					
Telephone code					

Hello, I'm _____ from the Bureau of Market Research and we are conducting research about important national issues. I would like to speak to the person in the household who most recently celebrated his or her birthday, provided he or she is 18 years or older.

"Birthday" respondent identified	1	"Other" respondent identified	2

I'm _____ from the Bureau of Market Research and we are conducting research about important national issues. I would like to ask you a few questions. There are no right or wrong answers, and all your answers are treated as confidential. Your name will not be connected to the answers you provide.

When you buy from companies, they sometimes require some of your personal information (such as your name, address, telephone number) before the sale can take place. And when they have your information, they sometimes use this to send you communication (like advertising material). I am going to ask you questions on how you feel about companies who collect and use your information. Remember, there are no right or wrong answers.

Each time I am going to read you a statement. Please tell me whether you disagree strongly, disagree slightly, neither agree nor disagree, agree slightly or agree strongly with each statement.

(READ EACH ITEM) – do you disagree strongly, disagree slightly, neither agree nor disagree, agree slightly, or agree strongly?

	Disagree strongly	Disagree slightly	Neither agree nor disagree	Agree slightly	Agree strongly	Don't know	Refuse
1. Companies generally ask for too much personal information from consumers.	1	2	3	4	5	6	7
2. Legislation should prevent a company from sharing my personal information with other companies without my permission.	1	2	3	4	5	6	7
3. I am confident that I can prevent companies from collecting personal information that I would like to keep secret.	1	2	3	4	5	6	7

	Disagree strongly	Disagree slightly	Neither agree nor disagree	Agree slightly	Agree strongly	Don't know	Refuse
4. Companies always provide their customers with the opportunity to request the removal of their names and addresses from records that are sold to other companies.	1	2	3	4	5	6	7
5. Most companies collect personal information from consumers in order to provide them with products and services to better suit their needs.	1	2	3	4	5	6	7
6. I would request a company to remove my personal information from their records if I suspected that they were misusing my information.	1	2	3	4	5	6	7
7. Companies must have privacy protection policies to make provision for customers who would not like to receive unrequested advertising material.	1	2	3	4	5	6	7
8. Too many companies call consumers at their homes to sell products and services to them.	1	2	3	4	5	6	7
9. I feel it is important to have access to the personal information companies keep of me.	1	2	3	4	5	6	7
10. Companies have adequate measures in place to ensure that all personal information in their records is accurate.	1	2	3	4	5	6	7
11. Consumers are not interested in getting information about new products and services from companies with which they have not done business before.	1	2	3	4	5	6	7
12. Personal information is not safe while stored in a company's records.	1	2	3	4	5	6	7
13. Companies should have privacy protection policies indicating that no personal information will be provided to other companies without consent from their customers.	1	2	3	4	5	6	7
14. I would support any initiatives that will enable me to stop companies from sending me unrequested advertising material.	1	2	3	4	5	6	7

	Disagree strongly	Disagree slightly	Neither agree nor disagree	Agree slightly	Agree strongly	Don't know	Refuse
15. I am satisfied about the control I have over the ways companies use my personal information.	1	2	3	4	5	6	7
16. Government should restrict companies to collect only the information needed for a specific transaction.	1	2	3	4	5	6	7
17. Companies never collect personal information for one reason and then use it for another purpose.	1	2	3	4	5	6	7
18. Most companies allow their consumers to have access to their personal information kept by the companies.	1	2	3	4	5	6	7
19. Government should do more to protect the safety of personal information.	1	2	3	4	5	6	7
20. I am concerned about the possible misuse of my personal information by companies.	1	2	3	4	5	6	7
21. I would request to having my personal information removed from any company's records if they sell the information to others.	1	2	3	4	5	6	7
22. Companies regularly share personal information with other companies without the permission of the individuals to whom the information belong.	1	2	3	4	5	6	7
23. I feel concerned that companies do not devote enough time and effort to ensure that my personal information is accurate while in their possession.	1	2	3	4	5	6	7
24. Companies should have privacy protection policies indicating the reasons for collecting personal information from consumers.	1	2	3	4	5	6	7
25. I feel it is unacceptable when a company shares my personal information with other companies so that they can offer their products and services to me.	1	2	3	4	5	6	7
26. Companies seldom collect personal information from consumers without their permission.	1	2	3	4	5	6	7

	Disagree strongly	Disagree slightly	Neither agree nor disagree	Agree slightly	Agree strongly	Don't know	Refuse
27. I am concerned when companies do not provide me with an opportunity to remove my name and address from any records that it provides to other companies.	1	2	3	4	5	6	7
28. I am satisfied when companies collect my personal information as a means to provide me with products and services which better suit my needs.	1	2	3	4	5	6	7
29. Companies should use independent auditing firms to confirm that they use the personal information of consumers as promised in the companies' privacy policies.	1	2	3	4	5	6	7
30. It bothers me that I receive so many unrequested advertising material that is of no interest to me.	1	2	3	4	5	6	7
31. I do not mind when companies use my personal information for other purposes than those provided when they collected my information.	1	2	3	4	5	6	7
32. I would support a company's efforts that will ensure that my personal information is safely kept.	1	2	3	4	5	6	7
33. I am uncomfortable when companies share my personal information with other companies without asking my permission first.	1	2	3	4	5	6	7
34. Companies regularly share personal information of consumers with other companies, so that these other companies could offer products and services to consumers.	1	2	3	4	5	6	7
35. I do not mind when I receive telephone calls at my home from companies wanting to sell products and services to me.	1	2	3	4	5	6	7
36. Most consumers have control over the ways their personal information is used by companies.	1	2	3	4	5	6	7
37. Government should limit companies' use of personal information to only that purpose for which it was collected.	1	2	3	4	5	6	7

	Disagree strongly	Disagree slightly	Neither agree nor disagree	Agree slightly	Agree strongly	Don't know	Refuse
38. Consumers' personal information is often misused by companies.	1	2	3	4	5	6	7
39. I do not mind to provide a lot of personal information if I think it is necessary.	1	2	3	4	5	6	7
40. Government should limit unrequested advertising material sent to consumers.	1	2	3	4	5	6	7
41. I am pleased when I receive information about new products and services from companies with which I have not done business before.	1	2	3	4	5	6	7
42. Companies send consumers too many unrequested advertising material that is not of interest to them.	1	2	3	4	5	6	7
43. Companies should have privacy protection policies indicating how they will protect the customer's information while it is in their possession.	1	2	3	4	5	6	7
44. I fear that my personal information may not be safe while stored in a company's records.	1	2	3	4	5	6	7
45. I would refuse to provide my personal information to a company who can not provide reasons why they want to collect my personal information.	1	2	3	4	5	6	7

Please answer Yes or No to the following questions:

	YES	NO	Don't know	Refuse
46. Have you ever refused to give information to a company because you thought it was not really needed or it was too personal?	1	2	3	4
47. Have you ever requested a company to remove your name and address from records that they use for marketing purposes?	1	2	3	4
48. Have you ever notified a company that you do not want to receive their unrequested advertising material?	1	2	3	4
49. Have you ever requested that a company not share your personal information with any other company?	1	2	3	4
50. Have you ever requested a company to inform you which measures they use to keep your personal information safe?	1	2	3	4
51. Have you ever personally been a victim of a situation you felt was an invasion of your private information?	1	2	3	4

	YES	NO	Don't know	Refuse
52. Are you aware of any options to remove your name from records of companies?	1	2	3	4
53. Have you ever purchased anything via the Internet?	1	2	3	4
54. Do you make use of Internet banking services?	1	2	3	4
55. During the past year, have you personally bought something from a catalogue or brochure sent to you?	1	2	3	4
56. During the past year, have you personally bought any product or service offered to you by a telephone call?	1	2	3	4
57. During the past year, have you personally called a toll-free (0800) number to order something?	1	2	3	4

To what extent do you agree or disagree with each of the following statements? (READ EACH ITEM) – do you disagree strongly, disagree slightly, agree slightly, or agree strongly?

	Disagree strongly	Disagree slightly	Agree slightly	Agree strongly	Don't know	Refuse
58. Consumers have lost all control over how personal information is collected and used by companies.	1	2	3	4	5	6
59. Most businesses handle the personal information they collect about consumers in a proper and confidential way.	1	2	3	4	5	6
60. Existing laws and organisational practices provide a reasonable level of protection for consumer privacy.	1	2	3	4	5	6

Finally, I have a few questions that are for classification purposes only and will be treated as confidential.

(Interviewer) If person asks why certain demographic and personal questions are asked?
We do so to properly generalise survey results to the greater population. Your answers will help us to ensure that we have sufficient variety among our respondents. As you may already know, we never disclose the identity of any one individual, therefore we do not ask your name or surname in this survey. Your answers will always be kept strictly confidential.

61. What is your year of birth? _____ *(please enter as a four-digit number, e.g. 1969)*

62. What is your home language?

English	1
Afrikaans	2
Xhosa	3
Zulu	4
Setswana	5
Sesotho	6
Sepedi	7
Swati	8
Tshivenda	9
Xitsonga	10
Ndebele	11
Other (specify)	12

63. What is the highest level of education you have completed or the highest qualification you have received?

Lower than Grade 10 (Standard 8)	1
Grade 10 (Standard 8)	2
Grade 12 (Standard 10)	3
Degree/Diploma	4
Post graduate/ Higher diploma	5

64. Which one of the following best describes your employment status? *Please select one response only.*

Employed full time	1
Employed part time	2
Self-employed (you work for yourself)	3
Not employed	4
Student	5
Homemaker/Housewife	6
Pensioner/Retired	7
Unfit for work	8

65. Which of the following categories best describes your personal total monthly income before any deductions?

Less than R2000	1
R2001-R4000	2
R4001-R6000	3
R6001-R8000	4
R8001-R10000	5
R10001-R15000	6
R15000 plus	7

66. BY OBSERVATION: Gender

Male	1
Female	2

THANK RESPONDENT; END INTERVIEW

HUISHOUDINGSVRAELYS – INLIGTINGSPRIVAATHEID – VOORTOETSING

Respondentnommer					
Telefoonkode					

Goeie dag, ek is _____ van die Buro vir Marknavorsing en ons doen navorsing oor belangrike nasionale aangeleenthede. Ek sal graag met die persoon in die huishouding wat die mees onlangste verjaar het wil gesels, gegewe dat hy of sy 18 jaar of ouer is.

"Verjaardag" respondent geïdentifiseer	1	*"Ander" respondent geïdentifiseer*	2

Ek is _____ van die Buro vir Marknavorsing en ons doen navorsing oor belangrike nasionale aangeleenthede. Ek sal u graag 'n paar vrae wil vra. Daar is geen verkeerde of regte antwoorde nie, en alle antwoorde word vertroulik hanteer. U naam sal aan geen van die antwoorde wat u gee, gekoppel word nie.

Wanneer u van ondernemings aankoop, verlang hulle somtyds u persoonlike inligting (soos u naam, adres, telefoonnommer) voordat die kooptransaksie kan plaasvind. En wanneer ondernemings u inligting het, gebruik hulle dit soms om aan u kommunikasie (soos advertensiemateriaal) te stuur. Ek gaan u vra hoe u voel oor ondernemings wat u inligting insamel en gebruik. Onthou, daar is geen regte of verkeerde antwoord nie.

Ek gaan telkens vir u 'n stelling lees, en dan moet u vir my sê of u glad nie met die stelling saamstem nie, slegs gedeeltelik met die stelling verskil, nie saamstem of verskil nie, gedeeltelik saamstem, of volkome met die stelling saamstem.

(LEES ELKE ITEM) – Stem u glad nie saam nie, verskil u gedeeltelik stem nie saam nie en verskil ook nie, stem gedeeltelik saam, stem volkome saam?

	Stem glad nie saam nie	Verskil gedeel-telik	Stem nie saam of verskil nie	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
1. Ondernemings vra gewoonlik vir te veel persoonlike inligting van verbruikers.	1	2	3	4	5	6	7
2. Wetgewing behoort 'n onderneming te verhoed om my persoonlike inligting aan ander ondernemings beskikbaar te stel sonder my toestemming.	1	2	3	4	5	6	7
3. Ek is vol vertroue dat ek ondernemings kan verhoed om persoonlike inligting in te samel wat ek graag geheim sou wou hou.	1	2	3	4	5	6	7

	Stem glad nie saam nie	Verskil gedeel-telik	Stem nie saam of verskil nie	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
4. Ondernemings gee altyd aan hulle kliënte 'n geleentheid om te vra dat hulle name en adresse van die rekords wat aan ander ondernemings verkoop word, geskrap word.	1	2	3	4	5	6	7
5. Meeste ondernemings samel persoonlike inligting van verbruikers, in sodat produkte en dienste aan hulle voorsien kan word wat beter aan hulle behoeftes sal voldoen.	1	2	3	4	5	6	7
6. Ek sal 'n onderneming versoek om my persoonlike inligting van hulle rekords te verwyder indien ek vermoed dat hulle besig is om my inligting te misbruik.	1	2	3	4	5	6	7
7. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê, ten einde voorsiening te maak vir kliënte wat nie graag ongevraagde advertensie materiaal wil ontvang nie.	1	2	3	4	5	6	7
8. Te veel ondernemings skakel verbruikers by die huis om aan hulle produkte en dienste te verkoop.	1	2	3	4	5	6	7
9. Ek voel dit is belangrik om toegang te hê tot die persoonlike inligting wat ondernemings van my hou.	1	2	3	4	5	6	7
10. Ondernemings het voldoende maatreëls in plek om te verseker dat alle persoonlike inligting in hulle rekords akkuraat is.	1	2	3	4	5	6	7
11. Verbruikers stel nie belang om inligting oor nuwe produkte en dienste van ondernemings te ontvang met wie hulle nog nie vantevore besigheid gedoen het nie.	1	2	3	4	5	6	7
12. Persoonlike inligting is nie veilig terwyl dit in 'n onderneming se rekords gehou word nie.	1	2	3	4	5	6	7
13. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê wat aandui dat geen persoonlike inligting aan ander ondernemings voorsien sal word sonder die goedkeuring van hulle kliënte nie.	1	2	3	4	5	6	7
14. Ek sal enige inisiatiewe ondersteun wat my in staat sal stel om ongevraagde advertensie material wat ondernemings aan my stuur, te stop.	1	2	3	4	5	6	7

	Stem glad nie saam nie	Verskil gedeel-telik	Stem nie saam of verskil nie	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
15. Ek is tevrede met die beheer wat ek het oor die wyses waarop ondernemings my persoonlike inligting gebruik.	1	2	3	4	5	6	7
16. Die regering moet ondernemings beperk om slegs dié inligting in te samel wat nodig is vir 'n spesifieke transaksie.	1	2	3	4	5	6	7
17. Ondernemings samel nooit inligting in vir 'n bepaalde rede en gebruik dit dan vir 'n ander doel nie.	1	2	3	4	5	6	7
18. Meeste ondernemings maak dit vir verbruikers moontlik om toegang te hê tot hulle persoonlike inligting wat deur die ondernemings gehou word.	1	2	3	4	5	6	7
19. Die regering moet meer doen om die veiligheid van persoonlike inligting te beskerm.	1	2	3	4	5	6	7
20. Ek is bekommerd oor die moontlike misbruik van my persoonlike inligting deur ondernemings.	1	2	3	4	5	6	7
21. Ek sal versoek dat my persoonlike inligting verwyder moet word van enige ondernemingsrekords indien die inligting aan ander verkoop word.	1	2	3	4	5	6	7
22. Ondernemings maak gereeld persoonlike inligting aan ander ondernemings bekend sonder die toestemming van die individue aan wie die persoonlike inligting behoort.	1	2	3	4	5	6	7
23. Ek voel bekommerd dat ondernemings nie genoeg tyd en moeite bestee om te verseker dat my persoonlike inligting akkuraat is terwyl dit in hulle besit is nie.	1	2	3	4	5	6	7
24. Ondernemings moet 'n beleid vir die beskerming van privaatheid hê wat die redes aandui waarom hulle mense se persoonlike inligting insamel.	1	2	3	4	5	6	7
25. Ek voel dit is onaanvaarbaar wanneer 'n onderneming my persoonlike inligting met ander ondernemings deel sodat dié ondernemings hulle produkte en dienste aan my kan aanbied.	1	2	3	4	5	6	7

	Stem glad nie saam nie	Verskil gedeel-telik	Stem nie saam of verskil nie	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
26. Ondernemings samel selde verbruikers se persoonlike inligting in sonder hulle toestemming.	1	2	3	4	5	6	7
27. Ek is bekommerd wanneer ondernemings my nie 'n geleentheid gee om my naam en adres van enige van hulle rekords wat hulle aan ander ondernemings gee, te verwyder nie.	1	2	3	4	5	6	7
28. Ek is tevrede wanneer ondernemings my persoonlike inligting insamel sodat hulle produkte en dienste aan my kan bied wat beter aan my behoeftes voldoen.	1	2	3	4	5	6	7
29. Ondernemings moet onafhanklike ouditfirmas gebruik wat bevestig dat hulle verbruikers se persoonlike inligting gebruik soos beloof in die ondernemings se beleid vir die beskerming van privaatheid.	1	2	3	4	5	6	7
30. Dit hinder my dat ek so baie ongevraagde advertensiemateriaal waarin ek nie belangstel nie, ontvang.	1	2	3	4	5	6	7
31. Ek gee nie om wanneer ondernemings my persoonlike inligting vir ander doeleindes gebruik as die doel waarvoor dit aanvanklik ingesamel is nie.	1	2	3	4	5	6	7
32. Ek sal 'n ondernemings se pogings ondersteun wat sal verseker dat my persoonlike inligting veilig gehou word.	1	2	3	4	5	6	7
33. Ek is ongemaklik wanneer ondernemings my persoonlike inligting met ander ondernemings deel sonder om eers my toestemming te vra.	1	2	3	4	5	6	7
34. Ondernemings deel gereeld persoonlike inligting van hulle verbruikers met ander ondernemings, sodat hierdie ander ondernemings produkte en dienste aan verbruikers kan aanbied.	1	2	3	4	5	6	7
35. Ek gee nie om wanneer ek telefoonoproepe tuis ontvang van ondernemings wat produkte en dienste aan my wil verkoop nie.	1	2	3	4	5	6	7
36. Meeste verbruikers het beheer oor die wyses waarop hulle persoonlike inligting deur ondernemings gebruik word.	1	2	3	4	5	6	7

	Stem glad nie saam nie	Verskil gedeel-telik	Stem nie saam of verskil nie	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
37. Die regering moet die gebruik van persoonlike inligting deur ondernemings beperk tot slegs dié doel waarvoor dit ingesamel is.	1	2	3	4	5	6	7
38. Verbruikers se persoonlike inligting word dikwels deur ondernemings misbruik.	1	2	3	4	5	6	7
39. Dit pla my nie om 'n klomp persoonlike inligting te verskaf as ek dink dit is nodig nie.	1	2	3	4	5	6	7
40. Die regering moet 'n beperking plaas op ongevraagde advertensiemateriaal wat aan verbruikers gestuur word.	1	2	3	4	5	6	7
41. Ek is ingenome wanneer ek inligting oor nuwe produkte en dienste ontvang vanaf ondernemings met wie ek nog nie voorheen besigheid gedoen het nie.	1	2	3	4	5	6	7
42. Ondernemings stuur aan verbruikers te veel ongevraagde advertensiemateriaal waarin hulle nie belang stel nie.	1	2	3	4	5	6	7
43. Ondernemings moet 'n 'n beleid vir die beskerming van privaatheid hê wat aandui hoe hulle die kliënt se inligting sal beskerm terwyl dit in hulle besit is.	1	2	3	4	5	6	7
44. Ek vrees dat my persoonlike inligting nie veilig is terwyl dit in 'n onderneming se rekords gehou word nie.	1	2	3	4	5	6	7
45. Ek sal weier om my persoonlike inligting aan 'n onderneming te voorsien wat nie redes kan verskaf waarom hulle my persoonlike inligting wil hê nie.	1	2	3	4	5	6	7

Beantwoord asseblief JA of NEE op die volgende vrae:

	JA	NEE	Weet nie	Weier
46. Het u al ooit geweier om inligting aan 'n onderneming te gee omdat u gedink het dit nie regtig nodig was nie, of dat dit té persoonlik was?	1	2	3	4
47. Het u al ooit versoek dat 'n onderneming u naam en adres van die rekords wat hulle gebruik vir bemarkingsdoeleindes, moet verwyder?	1	2	3	4
48. Het u al ooit 'n onderneming in kennis gestel dat u nie van hulle ongevraagde advertensiemateriaal wil ontvang nie?	1	2	3	4

	JA	NEE	Weet nie	Weier
49. Het u al ooit versoek dat die persoonlike inligting wat u aan 'n onderneming voorsien het, nie aan enige ander onderneming beskikbaar gestel mag word nie?	1	2	3	4
50. Het u al ooit 'n onderneming versoek dat hulle u moet inlig oor die maatreëls wat hulle gebruik om u persoonlike inligting veilig te hou?	1	2	3	4
51. Was u persoonlik al ooit 'n slagoffer van 'n situasie wat u gevoel het 'n skending van u private inligting was?	1	2	3	4
52. Is u bewus van enige wyses om u naam van die rekords van ondernemings te verwyder?	1	2	3	4
53. Het u al ooit enigiets deur middel van die Internet aangekoop?	1	2	3	4
54. Maak u gebruik van Internet-bankdienste?	1	2	3	4
55. Het u persoonlik, gedurende die afgelope jaar, iets gekoop uit 'n katalogus of brosjure wat aan u gestuur is?	1	2	3	4
56. Het u persoonlik, gedurende die afgelope jaar, enige produkte of dienste wat telefonies aan u aangebied is, gekoop?	1	2	3	4
57. Het u gedurende die afgelope jaar 'n tolvry (0800) nommer geskakel om iets te bestel?	1	2	3	4

In hoe 'n mate verskil u of stem u saam met die onderstaande stellings?
(LEES ELKE ITEM) – Stem u glad nie saam nie, verskil u gedeeltelik, stem u gedeeltelik saam of stem u volkome saam?

	Stem glad nie saam nie	Verskil gedeel-telik	Stem gedeel-telik saam	Stem volkome saam	Weet nie	Weier
58. Verbruikers het alle beheer oor die wyse waarop ondernemings persoonlike inligting insamel en gebruik, verloor.	1	2	3	4	5	6
59. Meeste besighede hanteer die persoonlike inligting wat hulle insamel oor verbruikers op 'n behoorlike en vertroulike wyse.	1	2	3	4	5	6
60. Bestaande wetgewing en ondernemingspraktyke voorsien 'n redelike mate van beskerming vir verbruikersprivaatheid.	1	2	3	4	5	6

Ten laaste het ek 'n paar vrae wat slegs vir klassifikasiedoeleindes is en wat vertroulik hanteer sal word.

(Onderhoudvoerder) Indien 'n persoon vra waarom sekere demografies en persoonlike vrae gevra word?
Ons doen dit sodat ons die resultate van hierdie opname kan veralgemeen na die groter populasie. U antwoorde help ons om te verseker dat ons genoegsame verskeidenheid van ons respondente het. Soos u alreeds mag weet, maak ons nooit die identiteit van enige individu bekend nie, en daarom vra ons nie u naam of van in hierdie opname nie. Al u antwoorde word ook as hoogs vertroulik hanteer.

61. In watter jaar is u gebore? _____ *(teken aan as a vier-syfer nommer, bv. 1969)*

62. Wat is u huistaal?

Engels	1
Afrikaans	2
Xhosa	3
Zulu	4
Setswana	5
Sesotho	6
Sepedi	7
Swati	8
Tshivenda	9
Xitsonga	10
Ndebele	11
Ander (spesifiseer)	12

63. Wat is die hoogste vlak van opleiding wat u voltooi het of die hoogste kwalifikasie wat u verwerf het?

Laer as Graad 10 (Standerd 8)	1
Graad 10 (Standerd 8)	2
Graad 12 (Standerd 10)	3
Graad/Diploma	4
Nagraadse kwalifikasie/ Hoër diploma	5

64. Watter een van die volgende beskryf u werkstatus die beste? *Merk slegs een respons.*

Voltyds indiens	1
Deeltyds indiens	2
Selfindiensgeneem (u werk vir uself)	3
Het nie werk nie	4
Student	5
Tuisteskepper/Huisvrou	6
Pensioentrekker/Afgetree	7
Ongeskik vir werk	8

65. Watter van die volgende kategorieë beskryf u persoonlike maandelikse inkomste voor enige aftrekkings, die beste?

Minder as R2000	1
R2001-R4000	2
R4001-R6000	3
R6001-R8000	4
R8001-R10000	5
R10001-R15000	6
R15000 plus	7

66. DEUR MIDDEL VAN WAARNEMING: Geslag

Manlik	1
Vroulik	2

BEDANK DIE RESPONDENT; EINDIG DIE ONDERHOUD

APPENDIX 3

ROTATED SIX-FACTOR LOADING MATRIX

ROTATED SIX-FACTOR LOADING MATRIX FOR ALL VARIABLES

	FACTOR 1	FACTOR 2	FACTOR 3	FACTOR 4	FACTOR 5	FACTOR 6
1	0.331	-0.131	0.162	0.088	-0.086	0.092
2	0.061	-0.066	0.237	0.079	0.114	-0.092
3	0.098	-0.065	-0.018	-0.073	-0.033	-0.026
4	0.031	0.078	-0.040	-0.089	0.285	0.052
5	-0.055	0.063	0.121	-0.080	0.317	-0.123
6	0.181	-0.230	0.137	0.042	0.195	-0.024
7	-0.060	-0.131	0.024	0.054	0.331	0.061
8	-0.040	0.456	-0.095	-0.045	-0.072	0.033
9	0.166	-0.127	0.085	-0.002	0.477	0.017
10	0.321	0.002	0.058	0.082	0.069	0.026
11	0.353	-0.038	0.037	0.067	0.597	-0.033
12	0.466	0.006	0.035	0.153	0.337	0.023
13	0.146	0.056	0.056	0.119	0.561	-0.078
14	0.184	-0.008	0.017	0.000	0.690	-0.084
15	0.660	0.107	0.000	0.017	0.187	-0.081
16	-0.206	0.153	0.172	0.012	0.290	0.195
17	0.768	0.017	0.011	0.018	0.099	0.035
18	0.620	0.198	0.009	0.058	0.129	0.008
19	0.786	0.124	-0.001	-0.079	0.149	-0.002
20	0.118	0.574	-0.018	0.071	0.102	0.086
21	0.677	0.099	0.051	-0.028	-0.133	-0.022
22	0.087	0.440	0.163	-0.011	0.012	-0.004
23	0.007	0.017	-0.086	0.046	0.451	0.048
24	-0.084	0.369	-0.006	0.098	0.158	0.144
25	0.137	0.138	0.722	0.120	-0.149	-0.105
26	0.112	0.014	0.767	0.088	-0.126	0.064
27	0.094	0.060	0.533	-0.111	0.040	0.112
28	-0.060	0.072	0.535	-0.125	0.248	0.019
29	-0.040	0.031	0.642	-0.011	-0.139	0.022
30	-0.137	-0.089	0.669	-0.047	0.183	-0.037
31	-0.030	0.286	-0.012	0.624	0.049	-0.135
32	0.029	0.745	0.013	0.087	0.006	-0.021
33	0.074	0.551	0.225	0.054	-0.091	-0.017
34	-0.041	-0.040	0.008	0.790	-0.003	0.123
35	0.116	-0.050	0.585	0.313	-0.049	0.051
36	-0.052	0.409	0.006	0.236	0.055	0.310
37	0.028	0.055	-0.056	0.809	0.014	0.050
38	0.014	0.452	0.094	0.181	0.056	0.297
39	0.047	0.647	-0.119	0.130	-0.037	0.105
40	-0.011	0.061	-0.030	0.832	0.059	0.026
41	0.037	0.119	0.018	-0.050	0.054	0.960
42	0.312	-0.131	0.056	0.306	-0.239	0.197
43	0.285	-0.197	0.249	0.463	-0.138	-0.007
44	0.096	0.591	0.004	-0.029	-0.007	0.117
45	0.027	0.413	0.049	0.044	-0.084	0.400

APPENDIX 4

ROTATED FIVE-FACTOR LOADING MATRIX

ROTATED FIVE-FACTOR LOADING MATRIX FOR ALL VARIABLES

	FACTOR 1	FACTOR 2	FACTOR 3	FACTOR 4	FACTOR 5
1	-0.075	0.311	0.169	0.133	-0.084
2	-0.112	0.065	0.238	0.063	0.121
3	-0.086	0.099	-0.018	-0.068	-0.032
4	0.106	0.029	-0.044	-0.087	0.281
5	0.008	-0.042	0.117	-0.126	0.321
6	-0.235	0.171	0.141	0.062	0.201
7	-0.087	-0.070	0.023	0.073	0.329
8	0.461	-0.025	-0.100	-0.085	-0.079
9	-0.112	0.159	0.082	0.013	0.479
10	0.020	0.313	0.060	0.097	0.073
11	-0.042	0.351	0.035	0.061	0.603
12	0.033	0.457	0.036	0.163	0.343
13	0.018	0.156	0.050	0.087	0.566
14	-0.046	0.192	0.011	-0.027	0.694
15	0.051	0.665	0.001	0.005	0.194
16	0.273	-0.219	0.170	0.028	0.280
17	0.035	0.753	0.017	0.046	0.103
18	0.193	0.620	0.009	0.056	0.132
19	0.114	0.781	0.005	-0.071	0.150
20	0.617	0.130	-0.023	0.028	0.094
21	0.074	0.676	0.058	-0.021	-0.131
22	0.433	0.103	0.160	-0.059	0.009
23	0.054	0.005	-0.089	0.044	0.448
24	0.461	-0.086	-0.009	0.083	0.151
25	0.074	0.150	0.711	0.088	-0.134
26	0.049	0.105	0.765	0.106	-0.122
27	0.121	0.082	0.535	-0.088	0.035
28	0.088	-0.061	0.535	-0.137	0.247
29	0.038	-0.043	0.645	-0.008	-0.139
30	-0.100	-0.138	0.672	-0.057	0.186
31	0.229	-0.003	-0.014	0.544	0.062
32	0.712	0.058	0.005	0.006	0.004
33	0.535	0.093	0.219	-0.006	-0.091
34	0.057	-0.053	0.008	0.811	0.007
35	-0.012	0.106	0.589	0.330	-0.042
36	0.602	-0.070	0.002	0.258	0.045
37	0.112	0.025	-0.057	0.805	0.027
38	0.612	0.003	0.093	0.200	0.042
39	0.709	0.059	-0.125	0.084	-0.042
40	0.109	-0.010	-0.034	0.818	0.073
41	0.603	-0.044	0.026	0.168	0.010
42	-0.011	0.279	0.065	0.376	-0.234
43	-0.185	0.273	0.255	0.489	-0.124
44	0.638	0.105	-0.003	-0.060	-0.015
45	0.633	0.001	0.050	0.093	-0.102

APPENDIX 5

INITIAL FOUR-FACTOR LOADING MATRIX

INITIAL FOUR-FACTOR LOADING MATRIX CONTAINING ALL 45 ITEMS

	FACTOR 1	FACTOR 2	FACTOR 3	FACTOR 4
1	-0.101	0.237	0.163	0.194
2	-0.091	0.137	0.234	0.051
3	-0.114	0.064	-0.022	-0.039
4	0.119	0.182	-0.046	-0.136
5	0.033	0.141	0.114	-0.187
6	-0.221	0.278	0.135	0.052
7	-0.030	0.131	0.025	-0.001
8	0.440	-0.072	-0.103	-0.084
9	-0.077	0.415	0.080	-0.050
10	0.002	0.335	0.050	0.125
11	-0.014	0.647	0.034	0.002
12	0.033	0.619	0.026	0.160
13	0.071	0.453	0.053	0.005
14	-0.002	0.538	0.017	-0.115
15	-0.018	0.708	-0.014	0.069
16	0.340	-0.035	0.168	-0.063
17	-0.048	0.729	0.003	0.140
18	0.131	0.633	-0.004	0.119
19	0.014	0.770	-0.010	0.022
20	0.614	0.177	-0.035	0.013
21	-0.032	0.515	0.046	0.108
22	0.416	0.096	0.150	-0.051
23	0.104	0.256	-0.085	-0.044
24	0.501	0.014	-0.010	0.026
25	0.074	0.060	0.704	0.138
26	0.061	0.020	0.763	0.151
27	0.118	0.085	0.528	-0.076
28	0.120	0.079	0.521	-0.181
29	0.049	-0.121	0.642	0.018
30	-0.048	-0.023	0.659	-0.096
31	0.315	0.066	-0.013	0.505
32	0.706	0.057	-0.006	-0.005
33	0.517	0.030	0.209	0.018
34	0.184	0.010	0.014	0.763
35	0.036	0.086	0.590	0.350
36	0.655	-0.016	-0.003	0.212
37	0.227	0.096	-0.055	0.765
38	0.650	0.039	0.089	0.168
39	0.704	0.035	-0.135	0.077
40	0.237	0.087	-0.028	0.756
41	0.637	-0.023	0.021	0.136
42	-0.016	0.147	0.059	0.443
43	-0.155	0.203	0.254	0.538
44	0.613	0.088	-0.013	-0.058
45	0.638	-0.053	0.042	0.095

APPENDIX 6

AVERAGE VARIANCE EXTRACTED

CALCULATION OF THE AVERAGE VARIANCE EXTRACTED (AVE)

$$\text{Variance extracted} = \frac{\text{Sum of squared standardised loadings}}{\text{Sum of squared standardised loadings} + \text{Sum of indicator measurement error}^{a}}$$

[a]Indicator measurement error can be calculated as 1-(standardised loading)^2

Sum of squared standardised loadings:

General privacy = $0.8399^2 + 0.8129^2 + 0.887^2 = 2.153007$

Misuse = $0.7851^2 + 0.7851^2 + 0.7642^2 = 1.816766$

Solicitation = $0.7325^2 + 0.802^2 + 0.8099^2 = 1.835698$

Government protection = $0.7655^2 + 0.6705^2 + 0.7473^2 = 1.594018$

Sum of measurement error:

General privacy = 0.294568 + 0.339194 + 0.21321 = 0.846993

Misuse = 0.383618 + 0.383618 + 0.415998 = 1.183234

Solicitation = 0.463444 + 0.356796 + 0.344062 = 1.164302

Government protection = 0.41401 + 0.55043 + 0.441543 = 1.405982

Variance extracted computation:

General privacy = 2.153007 / (2.153007 + 0.846993) = 0.717669

Misuse = 1.816766 / (1.816766 + 1.183234) = 0.605589

Solicitation = 1.835698 / (1.835698 + 1.164302) = 0.611899

Government protection = 1.594018 / (1.594018 + 1.405982) = 0.531339

APPENDIX 7

KOLGOMOROV-SMIRNOV TESTS FOR NORMALITY

KOLGOMOROV-SMIRNOV TESTS FOR NORMALITY

		Privacy protection (factor 1)	Information misuse (factor 2)	Solicitation (factor 3)	Government protection (factor 4)
Behaviour groups	No protection	0.0000	0.0066	0.0022	0.0000
	Limited protection	0.0000	0.0000	0.0000	0.0000
	Protection	0.0000	0.0000	0.0004	0.0000
Victim of privacy invasion groups	Victim	0.0000	0.0000	0.0000	0.0000
	Not a victim	0.0000	0.0000	0.0000	0.0000
Awareness of name removal groups	Aware	0.0000	0.0000	0.0000	0.0000
	Not aware	0.0000	0.0000	0.0000	0.0000
Internet user groups	Internet users	0.0000	0.0001	0.0076	0.0000
	Internet non-users	0.0000	0.0000	0.0000	0.0000
Direct shopping groups	Direct shoppers	0.0000	0.0000	0.0000	0.0000
	Non-direct shoppers	0.0000	0.0000	0.0000	0.0000
Age groups	18-39 years	0.0000	0.0000	0.0000	0.0000
	40+ years	0.0000	0.0000	0.0000	0.0000
Language groups	English	0.0000	0.0000	0.0000	0.0000
	Afrikaans	0.0000	0.0000	0.0000	0.0000
	Black African	0.0000	0.0014	**0.0822**	0.0000
Educational groups	Low education	0.0000	0.0001	0.0000	0.0000
	Medium education	0.0000	0.0000	0.0000	0.0000
	High education	0.0000	0.0000	0.0000	0.0000
Employment groups	Employed	0.0000	0.0000	0.0000	0.0000
	Not employed	0.0000	0.0000	0.0000	0.0000
Income groups	Low income	0.0000	0.0000	0.0005	0.0000
	Middle income	0.0000	0.0000	0.0000	0.0000
	High income	1.0000	0.0000	0.0001	0.0000
Gender groups	Male	0.0000	0.0000	0.0001	0.0000
	Female	0.0000	0.0000	0.0000	0.0000

APPENDIX 8

ASSESSING HOMOGENEITY OF VARIANCE USING F_{MAX} IN CONJUNCTION WITH SAMPLE-SIZE

ASSESSING HOMOGENEITY OF VARIANCE USING F_{MAX} IN CONJUNCTION WITH SAMPLE-SIZE RATIOS

GROUPS	SUB-GROUPS	N	Privacy protection (factor 1) variances	Information misuse (factor 2) variances	Solicitation (factor 3) variances	Government protection (factor 4) variances
Behaviour groups	No protection	181	0.42106	0.872224	1.170626	0.577123
	Limited protection	305	0.12786	1.228614	1.259034	0.717302
	Protection	141	0.259546	0.675696	0.807103	0.622729
	F_{max}		3.293143	1.818293	1.559942	1.242893
	Sample-size ratios		0.5 : 1	2.1 : 1	2.1 : 1	1.6 : 1
Victim of privacy invasion groups	Victim	196	0.163838	0.607012	0.858015	0.582764
	Not a victim	431	0.287795	1.087396	1.2447	0.685002
	F_{max}		1.756584	1.791392	1.450673	1.175436
	Sample-size ratios		2.1 : 1	2.1 : 1	2.1 : 1	2.1 : 1
Awareness of name removal groups	Aware	145	0.229994	1.372824	1.705827	1.260781
	Not aware	482	0.255576	0.913237	0.963155	0.444567
	F_{max}		1.111231	1.50325	1.771083	2.835975
	Sample-size ratios		3.3 : 1	0.3 : 1	0.3 : 1	0.3 : 1
Internet user groups	Internet users	139	0.204378	0.780119	0.844354	0.648965
	Internet non-users	488	0.263177	1.087117	1.227077	0.656656
	F_{max}		1.2877	1.393527	1.453274	1.011851
	Sample-size ratios		3.5 : 1	3.5 : 1	3.5 : 1	3.5 : 1
Direct shopping groups	Direct shoppers	287	0.178292	1.190746	1.395881	0.783528
	Non-direct shoppers	340	0.307914	0.895714	0.855668	0.540398
	F_{max}		1.727018	1.329382	1.631335	1.449911
	Sample-size ratios		1.1 : 1	0.8 : 1	0.8 : 1	0.8 : 1
Age groups	18-39 years	279	0.305392	1.092673	1.080766	0.554432
	40+ years	346	0.200535	0.979438	1.188651	0.727936
	F_{max}		1.522887	1.115612	1.099822	1.31294
	Sample-size ratios		0.8 : 1	0.8 : 1	1.2 : 1	1.2 : 1
Language groups	English	261	0.189537	0.89719	0.996413	0.757799
	Afrikaans	226	0.194411	1.169659	1.27582	0.550552
	Black African	140	0.425663	0.994411	1.052992	0.610049
	F_{max}		2.245808	1.303691	1.280413	1.376435
	Sample-size ratios		0.5 : 1	0.8 : 1	0.8 : 1	1.3 : 1
Educational groups	Low education	154	0.423838	1.0964	1.404172	0.691419
	Medium education	233	0.178884	1.087986	1.1379	0.607407
	High education	238	0.199968	0.786267	0.911298	0.683269
	F_{max}		2.369351	1.394437	1.540848	1.138313
	Sample-size ratios		06 : 1	0.6 : 1	0.6 : 1	0.6 : 1

Employment groups	Employed	372	0.242873	1.005665	1.067663	0.759672
	Not employed	254	0.261279	1.050404	1.25864	0.499704
	F_{max}		1.075787	1.044487	1.178873	1.520244
	Sample-size ratios		0.6 : 1	0.6 : 1	0.6 : 1	1.4 : 1
Income groups	Low income	206	0.347137	1.01973	1.2725	0.607099
	Middle income	213	0.204431	1.068268	1.190751	0.481196
	High income	155	0.223469	0.731065	0.869366	0.697528
	F_{max}		1.698066	1.461248	1.463709	1.449572
	Sample-size ratios		0.9 : 1	1.3 : 1	1.3 : 1	0.7 : 1
Gender groups	Male	237	0.326623	1.133265	1.18392	0.974425
	Female	390	0.199946	0.977978	1.11915	0.440867
	F_{max}		1.633559	1.158783	1.057874	2.210246
	Sample-size ratios		0.6 : 1	0.6 : 1	0.6 : 1	0.6 : 1

Note: The above-calculated F_{max} values (a value as great as 10 is acceptable) in conjunction with the sample-size ratios (within a ratio of 4 to 1 from the largest cell variance to the smallest) indicate an acceptable degree of homogeneity of variance.