# 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 21$^{st}$ century information revolution, just as electricity was the true heart of the 20$^{th}$ 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.