A MARKET-ORIENTED APPROACH TO RESPONSIBLY MANAGING INFORMATION PRIVACY CONCERNS IN DIRECT MARKETING

Sara Dolnicar and Yolanda Jordaan

Marketing communications media technologies have the potential to be intrusive and influence consumers' perceptions of marketing communication. Aggressive direct marketing (DM) is one communication tool that has the potential to lead to consumer concern about information privacy. Concerned consumers change their behavior: They refuse to buy through risky channels or provide information, thus jeopardizing the aim of DM. Responsible DM can prevent such reactions and build trust. Typical measures taken and recommended to protect consumers from privacy violations are of a regulative rather than a market-oriented nature, which is directly opposed to companies' profit-maximization aims. We propose a segmentation-based approach for responsible DM, based on consumer heterogeneity regarding privacy concerns and privacy-related behavior. Using two independent samples from South Africa and Australia, we explore consumers' views on privacy issues and examine the potential of a market-oriented approach to responsible DM.

One of the main objectives of integrated marketing communication (IMC) is to influence consumers' value perceptions and affect their behavior through directed communication. The increasing power of information-processing technology has changed the environment for communication strategy, emphasizing the need to adjust objectives and strategies to changing marketing and communication situations. Communications appealing to the mass market are on the decrease and are being replaced by more direct and highly targeted promotional activities using, among other tools, direct marketing (DM). Computer-based systems have made it easy and affordable for direct marketers to collect, store, use, and share information with others. More marketers rely on consumer databases for day-to-day direct marketing communications when targeting individual customers. In this respect, DM (one of the elements in the IMC mix) has the ability to become more intrusive, raising issues of privacy invasion. Businesses that want to positively promote future growth in the DM industry will have to pay attention to the privacy issue, which is becoming more urgent as more consumers are involved in DM transactions.

A number of studies have investigated consumer privacy concerns, offering recommendations on how involved stakeholders could contribute to protecting consumers from privacy violations. The main emphasis of this stream of research was on understanding consumer privacy concerns and monitoring changes over time. Suggestions on preventing consumer privacy violations that have been both recommended and implemented in the past focus strongly on regulations, laws, and privacy policies. Only rarely has the use of market-driven mechanisms been proposed to support the development of responsible DM.

Consequently, the main aim of this paper is to (1) investigate the usefulness of including market-driven approaches in the portfolio of measures to address consumers' privacy

concerns. More specifically, a segmentation-based approach is suggested in which consumers are grouped according to their privacy concerns. Such a grouping enables companies to target each of those groups in the most appropriate manner by taking their segment-specific privacy concerns into consideration. Furthermore, the study contributes to the existing DM (and IMC) knowledge by (2) investigating South African and Australian consumer views regarding DM activities, information privacy concerns, and responsibilities of key stakeholders in preventing privacy violations (geographical extension of knowledge on consumer-information privacy issues), and (3) investigating the association between consumer privacy concerns and consumer behavior that jeopardizes DM activities, such as refusal to pass on information or boycotting risky purchasing channels (reinvestigation of this association using new variables).

If the level of concern about privacy is found to be high, and if concerned consumers alter their consumer behavior in a way that is detrimental to DM effectiveness, responsible DM becomes "more than an ethical issue" for the company; it becomes an economically rational managerial decision that companies are typically quick to adopt and that does not require the high levels of enforcement cost that laws and regulations cause. The proposed segmentation-based approach offers another avenue for companies to follow in an attempt to improve the way they implement responsible DM to benefit themselves as well as consumers.

It should be noted at this point that we make two assumptions throughout the paper: (1) that the organization has ethical reasons to maintain a positive relationship with customers; and (2) that both communication with customers and actions taken by consumers who perceive that their privacy has been violated (such as complaints, lawsuits, negative word-of-mouth) have associated costs. This is a very reasonable assumption in most cases. In a few instances, however, an organization may not care about the relationship with customers (e.g., spammers) or there may be only marginal cost associated with DM (e.g., bulk e-mail messages). In such cases, the incentive to adopt the demand-driven approach we propose is limited; these cases are therefore beyond the field of application for this study.

LITERATURE REVIEW

DM and the Value of Information

The information exchange between consumers and marketers remains one of the fundamental aspects of successful relationships. The focal point of this exchange is what the customer gives and what he or she receives. To increase the value of the customer offering, marketing communication should affect the consumer's value perception. An increasing number of organizations have added DM to their communications mix in an attempt to increase dialogue (information exchange) with the customer (Tapp 2000). Other factors have also contributed to the growth in DM, including advances in technology, an increase in the demand for information, and the declining effectiveness of traditional media (Evans, Patterson, and O'Malley 2001). DM offers several advantages over other IMC methods, such as DM's ability to target specific customers, its ability to

individualize and personalize messages, its measurability, and its potential to build loyalty through dialogue with customers (Patterson 1998).

The value of consumer information in today's business environment is undeniable. That is probably why DM, the industry from which database marketing evolved, focuses on the collection, storage, and use of consumer information. Direct marketers use consumer preference information to form groups of consumers with similar interests and tastes. In principle, such information used for data mining or DM can be seen as not only beneficial for organizations, but also for the consumer: relevant communication messages are delivered to consumers based on their preferences (Wientzen and Weinstein 1997).

A DM relationship is such that consumers are required to disclose certain facts about themselves to the direct marketer. In turn, direct marketers use the information to personalize communication and target consumers with relevant offers. Direct marketers can also obtain personal information from secondary data sources (such as database publishers) where information is accessible without the individual's knowledge. The rise of e-commerce, combined with sophisticated datamining software, has made it easy and affordable to obtain and share information across a network or to cross-reference information in a meaningful way. The ease of access to a person's file brings up a major disadvantage of databases, namely, the potential infringement of the right to privacy (Forcht and Thomas 1994). Direct marketers, by virtue of their unsolicited telephone calls at dinnertime and their junk mail in the mailbox, are finding themselves at the center of this storm.

As consumers are subject to more marketing communications, there are more opportunities for intrusiveness, and many consumers perceive a threat to their individual privacy owing to the power of information-processing technology used to intrude in their private domain. From a marketing perspective, consumer privacy revolves around the buyer's ability to limit the accumulation and dissemination of personal information relating to a specific DM transaction (Goodwin 1991)· One privacy concern for consumers relates to media intrusiveness. There is evidence that many consumers find the physical intrusion of direct marketers into their homes through unsolicited advertising very annoying (Evans, Patterson, and O'Malley 2001). It is interesting to note that privacy concerns often feature most strongly when consumers perceive that they are targeted with irrelevant DM communications (Evans, Patterson, and O'Malley 2001). Unfortunately, many consumers feel that they have little or no control over the prospecting efforts of organizations and the volume of direct mail, phone calls, and e-mails intruding into their daily lives. This calls attention to direct marketers to behave more responsibly when communicating with consumers. Unless direct marketers begin to implement responsible and ethical information-handling practices, there may be very few customers (or information) to manage in the future. It is surprising that these companies are skillfully using individual information to target consumers on the basis of their interests, but so far have not made use of the same tool to optimize their message from a responsible DM perspective. They are well aware that trying to sell classical concert tickets to a sports buff may not be optimal; thus, they eliminate such inefficient marketing strategies. They do not, however, make use of the same principle to select

consumers who appreciate DM efforts, while deliberately choosing alternative ways of communication with those consumers who dislike such approaches.

Consumer Information Privacy Concerns and Associations with Consumer Behavior

Consumer attitudes about privacy have been researched in various countries and many public opinion surveys. Most privacy studies indicate that information privacy is a very important concern to many consumers. The results of a study by Culnan (1993) show that consumers who believe they do not have control over their personal information are more concerned about privacy. The findings of a study by Nowak and Phelps (1992) indicate that privacy is an important concern and is affected by the type of marketing practice and the specificity of information. Findings from a few studies indicate that consumers believe that some personal information is more private than others (Milne 1997, 2000). It seems that consumers will be less upset when their purchasing-behavior habits are distributed than when their telephone numbers are distributed. Findings from a study by Earp and Baumer (2003) added to this by indicating that consumers are more willing to reveal information about their gender and age than their identification numbers.

A recent study revealed that respondents are more willing to provide contact information as opposed to biographical information, and likewise, are more willing to provide biographical information than financial information (Meinert et al. 2006). This suggests that consumers concerned about disclosing biographical information may opt to forgo providing any information, including providing the contact information they may have initially been willing to disclose before their bibliographical information was requested. In short, consumers are willing to trade their personal information in return for specific forms of information, provided there are appropriate benefits and controls in place. Sheehan and Hoy (1999) find that as privacy concerns increase, consumers become less likely to provide personal information to organizations. More recent studies have focused on privacy in an on-line environment. The results of two separate studies indicate that privacy and security concerns are the number one reason Web users are not purchasing over the Web, in part because they have no confidence that the e-commerce legal environment is secure (Earp and Baumer 2003; Udo 2001).

Several studies suggest that consumer behavior is associated with information privacy concerns and is particularly relevant to DM communications. A study investigating DM media used by banks found that the intention to purchase is positively influenced by respondents' favorable attitude toward the DM media used (Page and Luding 2003). Evans, Patterson, and O'Malley (2001) conclude that individuals who feel strongly about privacy attempt to minimize the information held on them and rarely, if ever, provide direct marketers with personal details or request communications from them. The frequency of engaging in protective behavior increases with increasing levels of privacy concerns (Berendt, Gunther, and Spiekermann 2005; Sheehan and Hoy 1999). More specific behavior aimed at protecting privacy was reported in an on-line study suggesting that users will cease Web site access if too much personal information is requested when registering on the site (Chen and Rea 2004). A recent study suggests that consumers

concerned about disclosing personal information may opt to forgo contact with the service provider, instead of providing personal information (Meinert et al. 2006).

From the above-mentioned consumer privacy studies it becomes evident that information privacy is an important issue to consumers and needs to be addressed by marketers in a responsible manner, given the association between privacy concerns and changes in consumption behavior, as well as changes in willingness to build relationships with companies. IMC is an important part of building relationships with customers where all marketing-communication messages should support the establishment, protection, and enrichment of customer relationships (Gronroos 2004).

Several researchers have proposed ways to decrease high levels of consumer privacy concern. Nowak and Phelps (1997) suggest strategies and tactics for alleviating consumer privacy concerns, such as informing consumers of when information is collected, how it will be used, and who will have access to the data, and by offering them opt-out opportunities. Milne and Boza (1999) have established that organizations can improve consumer trust by managing their personal information better, which reduces concern about privacy. Phelps, Nowak, and Ferrell (2000) suggest that privacy concerns can be reduced by providing consumers with more control over the initial gathering and subsequent dissemination of personal information. Although market segmentation has not been proposed as a tool to directly address consumer privacy concerns, Page and Luding (2003) have suggested that general negativity toward DM can be overcome by targeting very fine market segments offering the optimal match between the product the company offers and the consumption needs of the consumer. Ideally, if the promotion is well targeted, the individual will not be annoyed or consider it an invasion of privacy. Since consumers will be less likely to deal with direct marketers whose ethical practices go against their beliefs, comprehensible segments will enable direct marketers to implement better-focused DM communications. We propose an extension of this argument: It is not the product match that should be central to segmentation-based responsible DM; instead, consumers' concerns about privacy issues and their behaviors related to information privacy could be used to define target groups that deliberately should or deliberately should not be approached using DM messages offering products of interest to them. This would be particularly promising if consumers are found to be heterogeneous with respect to their privacy concerns and information privacy-related behaviors. One available segmentation tool used as a purely descriptive tool to report on consumer privacy concerns in the population is the United States Privacy Segmentation Index. This index segments consumers based on their attitudes toward information privacy and represents an attractive starting point for investigating the usefulness of market segmentation for responsible DM. The next section provides detail on the Privacy Segmentation Index.

The Privacy Segmentation Index (PSI)

Many research sources that report on consumer privacy come from nonacademic citations and/or institutions. One example is the Privacy Segmentation Index (PSI) created in 1995 by Harris Interactive, a market research firm based in New York. Harris Interactive is widely known for the Harris Poll, which is quoted by the media several hundred times

every month and is seen as a valuable source of data about American society (see www.harrisinteractive.com).

The PSI is used as a tool to divide the American public into three privacy-sensitive segments (ranging from low to high privacy concern) based on responses to three questions in the format of four-point Likert scales ranging from "strongly disagree" to "strongly agree." The index is repeated yearly, allowing researchers to track changes in opinions relating to privacy attitudes. The data for the latest available Harris Poll on privacy was collected by means of telephone interviews within the United States among a nationwide cross section of 1,010 adults (Taylor 2003). The results are weighed to be representative of the general population.

The first segment of the PSI classifies people with very high concern about privacy and is labeled as "Privacy Fundamentalists." According to the latest available results, this segment represents about 26% of the American public. This group feels very strongly about privacy matters. People in this segment tend to feel that they have lost much of their privacy and they favor the enactment of strong laws to secure privacy rights and ensure organizational discretion. The second group is labeled "Privacy Pragmatists." This segment currently represents about 64% of the American population. This group has strong feelings about privacy and is very concerned about protecting themselves from information misuse. However, they are often willing to allow people to access and use their personal information if they understand the reasons for its use. The final group, the "Privacy Unconcerned," represents about 10% of the population. This group has no real concerns about privacy and does not know what the "privacy fuss" is all about. People in this group have far less anxiety about how other people and organizations use information about them (Taylor 2003).

Although the PSI has not been developed for use by direct marketers, the relation between information privacy concerns and the personal characteristics captured by such segments could be valuable in developing effective and responsible DM strategies. Marketers could customize direct marketing messages according to the level of sensitivity to privacy issues for a given consumer group, and could even exclude highly sensitive segments from direct marketing. Such an approach would be beneficial to consumers, as their wishes would be respected, but it would also be rational from the company's point of view to spend resources wisely and maximize the response probability to direct marketing activities.

AIM OF THE RESEARCH

The concept of intrusiveness has been suggested to influence consumers' perceptions of marketing communication. Moreover, the personal nature of direct marketing communication often causes it to be seen as stepping over the line of discretion and as an invasion of consumers' privacy (Heinonen and Strandvik 2005). Prior work in the area of consumer information privacy indicates that (1) consumers worldwide recognize a problem of lack of information privacy and control over personal information, (2) privacy concerns are likely to be associated with consumers' behavioral changes, and (3)

heterogeneity of consumers with respect to privacy concerns appears to exist and could potentially be used to develop a market-oriented approach to responsible direct marketing that benefits both consumers and companies.

The study by Sheehan and Hoy (1999) served as a starting point on this topic: They found significant correlations between consumers' on-line privacy concerns and their behaviors. Our studies focus mainly on privacy in the commercial rather than the governmental sphere, and address the use of consumer data for DM purposes, excluding other areas of concern such as medical privacy, identity theft, workplace monitoring, intelligence systems, and biometrics.

We conducted two separate empirical studies in two countries: South Africa and Australia. The objectives of our study followed the structure of major findings in prior work: First, we aimed to investigate consumers' views on different dimensions of information privacy as it relates to DM activities for these two countries. (Please note that a cross-cultural comparison between South Africa and Australia is not intended. Two countries are chosen to strengthen the practical illustration of the proposed demand-driven approach using independent contexts and samples.) second, we wanted to investigate the associations between consumer views and behaviors related to consumption and privacy protection. Third, we would assess whether heterogeneity of consumers could be used to develop a segmentation-based approach for responsible direct marketing. The PSI was used as the basis for the last step.

If market segmentation is found to be a useful tool for responsible DM, adaptation of responsible DM by companies would be more likely to yield positive results than would attempting to impose laws and policies on them, because companies have an economic interest in approaching respondents who wish to be approached and who are likely to react to DM in a favorable manner. Approaching consumers with significant privacy concerns and dislike for DM will not lead to sales; it will only result in costs due to wasted resources and negative attitudes, which is not in any company's interest.

CONSUMER VIEWS IN SOUTH AFRICA

Sampling and Data Collection

The target population consisted of all adults older than 18 years residing in South Africa who were listed in the electronic CyberTrade Telephone Directory Service. The sampling frame contains 2.9 million households representing 30.4% of the households (9-5 million) with fixed telephone lines at home (SAARF 2001). A systematic sample was drawn across 19 geographical telephone directories in South Africa: The first number was chosen at random, after which the first number on every 1 lth page in the electronic directory was chosen (selecting every i-th element in succession). The sampling units were the households chosen, and the sample elements were household family members with the following characteristics (elements): individuals age 18 or older; individuals who can understand English or Afrikaans; and individuals who had most recently celebrated their birthdays.

The data collection was conducted by means of telephone interviews. It must be pointed out that data collection in South Africa is challenging because of the country's unique composition. In a country with 11 official languages, English is recognized as the language of commerce and science, but it is only spoken by 8% of South Africans at home as a first language (Statistics South Africa 2001). However, telephone interviews were the preferred method of data collection because of the low levels of Internet access (precluding an on-line survey), the large number of people living in rural areas (precluding personal interviews), and the high illiteracy rate (precluding a mail survey). All phone calls were made between 08:00 and 21:00 from Mondays to Saturdays and lasted between 15 and 25 minutes. One adult was interviewed per household. These individuals were randomly selected using the "last birthday" technique. Trained interviewers from the Bureau of Market Research (BMR) conducted the telephone interviews and the BMR's central office edited the completed questionnaires. Study results cannot be generalized to South Africa as a whole, as only households with listed numbers in the Telkom telephone directory service are represented.

A total of 2,233 telephone numbers were dialed to reach the target of 800 completed interviews. The response rate for the survey was 39%, excluding the disconnected and unreachable numbers. Based on the number of contacts with eligible households, the overall cooperation rate was 59%· Table 1 contains the sociodemographic profile of the South African respondents. As expected, the sample lacks representativity for the South African population. This can have implications for the descriptive analysis of the South African data. It does not, however, have major consequences on the main results of our study, which investigate heterogeneity and associations between constructs. Neither of these research questions requires that the sample be representative, particularly if the size of the segments is not interpreted as a population proportion. Any potential bias of results due to the sample structure will be explicitly stated in the respective parts of the results section.

Measurement Instrument

The measurement instrument included 66 questions and consisted of four sections: a 5-point Likert scale measurement containing 45 information privacy concern items; a 4-point Likert scale measurement containing 3 items from the PSI; 12 binary "yes-no" items measuring consumers' protective behaviors, experiences of privacy invasion, knowledge of specific data practices, and Internet and DM behaviors; and finally, certain basic sociodemographic questions. The scale items for Questions 1 to 60 were drawn from several previous studies relating to consumer information privacy (Campbell 1997; Culnan 1993, 1995; Harris Interactive 2000, 2002a, 2002b; Harris Interactive and Westin 1998, 2000; Milne and Boza 1999; Nowak and Phelps 1992; Sheehan 1999; Stone et al. 1983; Taylor, Vassar, and Vaught 1995; Vidmar and Flaherty 1985).

Questions 1 to 45 (for the privacy concern scale) contained the main constructs designed to measure information privacy concerns. Eight main dimensions were included in the survey: data collection, data storage and security, data use, data disclosure and dissemination, solicitation, privacy protection policies, legislation and government

protection, and behavioral intentions. The 45 privacy concern items were subjected to a scale purification process and showed both reliability and validity after the 45 items were reduced to 25 items. Details on the scale purification process fall beyond the scope of this paper, but can be reviewed in Jordaan (2004).

Results

The collected data was first analyzed in a descriptive manner to determine South African respondents' levels of concern about consumer privacy issues. Table 2 shows the percentage of respondents who indicated that they strongly agree with the statements from the privacy concern scale. Given that the respondents were asked to respond to questions on an ordinal scale for which it cannot be assured that the answer options are equidistant, frequencies rather than means and standard deviations are provided. The statements are arranged by the level of agreement expressed by the respondents (strongest to weakest agreement level). Please note that these are population proportions that could be affected by the fact that the sample is not fully representative.

As can be seen from Table 2, the strong agreement levels (items from 75% to 82%) relate to privacy protection. This indicates that the vast majority of respondents intend to take action if they suspect that their information is not protected and that there is a strong level of agreement among South Africans that clear privacy policies should exist to protect consumers. Whereas responses relating to privacy protection statements indicate a high level of homogeneity among consumers, this is not the case for statements relating to information misuse, which revolve around consumers' evaluations of the actual extent of misuse that is occurring. It seems that about half the respondents are concerned about misuse, with around 40% believing that companies use information for activities other than the intended purpose and that personal information is not safe while stored in the company database. The statements relating to solicitation capture the way respondents feel about being contacted by companies, and again, a rather high level of heterogeneity can be observed. While one-third of the respondents explicitly express that they are not interested in being contacted to learn about new products and services from companies with which they have not done business before, one-fifth seem very pleased to receive information from such companies. This supports the claim that responsible marketing would benefit from using different strategies with different customers. In some cases, the responsible reaction by a company may be to stop sending advertising material to certain consumers, whereas for other consumers, this may actually be counterproductive, as it is not their wish that communication be ceased. When one looks at the statements relating to government protection, high homogeneity and agreement exist among the South African respondents regarding views on the responsibility of government to ensure consumer privacy. About 70% of the respondents believe that government is a relevant stakeholder in the consumer privacy debate and that public policy should be driving increased protection of consumers from the misuse of their personal information.

In sum, Table 2 illustrates that there is substantial concern among South African respondents regarding consumer information privacy. Furthermore, it appears that there is heterogeneity in these consumers' views on many of the statements used in the survey,

particularly in their evaluations of how much misuse actually occurs, as well as in their preferences regarding direct advertising communications.

The second step in the data analysis was to investigate the potential of harvesting heterogeneity of consumers for responsible DM activities. For this, an exploratory post hoc segmentation analysis was undertaken based on respondents' behavioral statements. Respondents were asked whether they had engaged in any of the following behaviors relating to information privacy: shopping through catalogues; shopping over the telephone; shopping using a toll-free number; shopping via the Internet; Internet banking; refused to give personal information; notified not to receive unrequested advertising material; requested removal of information from company database; requested not to share information with others; and requested to be informed about measures used to keep information safe. In addition, respondents were asked whether they felt they have been a victim of privacy invasion and whether they are aware of options on how to remove their personal information from company records.

All 12 variables were used to investigate behavioral heterogeneity. All 800 respondents were grouped in segments based on their response patterns to these behavioral questions. Topology-representing networks (Martinetz and Schulten 1994) were used for the actual grouping task because this clustering algorithm has performed best in a Monte Carlo simulation comparison of algorithms (Buchta et al. 1997). To determine which number of clusters should be retained, 30 repetitions of cluster numbers from 3 to 10 were computed and the stability of assigning pairs of respondents to each of the clusters repeatedly was used as an evaluation criterion. The five-cluster solution emerged as most stable. The resulting profiles of the behavioral segments in South Africa are provided in Figure 1. The columns in Figure 1 represent the percentage of segment members who stated that they had engaged in each of the listed behaviors; the black horizontal bar indicates the same percentage for the total sample. Segments are therefore described by interpreting the deviations of the columns to the bars.

As can be seen from Figure 1, Segment 1 is characterized by demonstrating a range of protective behaviors. "Risky shopping behavior" (referring to behavior where personal information is disclosed to marketers) for this group is mainly on the Internet and the majority of members stated that they had already been victims of privacy invasion. Segment 2 does not indicate having engaged in any of the behaviors. Responses for this segment have to be interpreted with caution, as they could reflect response styles, and not just the accurate statements of respondents who indeed do not engage in any of the listed behaviors. Segment 3 has a very interesting behavioral profile. Again, a majority of these respondents have experienced privacy invasion. As opposed to Segment 1, however, members of this group have an average or below average usage of risky shopping techniques and very high levels of protective behavior. Segment 4 is characterized by essentially refusing to give out any information. This could explain why members of this segment do not engage in risky shopping behavior and have no need to take any other measures to protect their personal information. Finally, Segment 5 is characterized by above average protective behavior and use of shopping techniques that expose private information. Given that the sample is not fully representative of the South African

population, population proportions for the market segments have not been provided. The existence of the segments as such is not affected by the sample structure.

From the above-mentioned behavioral profiles it becomes evident that the heterogeneity in behavior presents useful managerial opportunities. Furthermore, the resulting segmentation solution discriminates very well between respondents with regard to consumer views and sociodemographics (tables and test values are available from the authors). These results support an earlier postulation by Milne and Gordon (1994), who suggested that consumers differ in their attitudes toward different forms of direct marketing and that attitudinal and behavioral information should be used to refine marketing strategies for different consumers. This reiterates the fact that using consumer heterogeneity to actively manage consumer privacy issues may have value for management.

Finally, the association between consumer views (as captured by the privacy scale) and consumer behavior is investigated. The process involved a summation of all responses (some were reverse-coded) in the privacy scale and the computation of analysis of variance (ANOVA), given the binary nature of the behavioral variables. These results are not affected by the deviation of the sample and population structure, as this process measures associations of behavioral subgroups with privacy attitudes. A number of behavioral variables were found to be significantly associated with respondents' information privacy views at the 95% significance level. Respondents who have shown the following behaviors/experience in the past were more negative about the current state of privacy protection and demanded that more measures be taken to ensure privacy: refusing to pass on private information; requesting removal of information; notifying companies that they should not send them advertising material; shopping via the Internet; and having been a victim of privacy invasion. This confirms that when companies use customers' information without permission, consumers see it as a misuse. This finding supports the results of a study by Sheehan and Hoy (1999), who also report that respondents' opting-out behavior (requesting removal from mailing lists) is positively correlated with privacy concerns. Consumers' willingness to get in touch with companies directly to notify them not to send material suggests that they will take protective action if they feel that direct marketers are not dealing with their personal information in a responsible or ethical way. This has already been evidenced by the strong positive reaction from consumers when the "do-not-call lists" were introduced in the United States.

No differences were detected in dependence of respondents: requesting that data not be shared with other companies; requesting information on measures taken to protect their privacy; and shopping via the telephone.

Respondents who were aware of options to remove personal information from an organization's database and respondents who have purchased through catalogues and brochures showed lower levels of privacy concerns. Of particular interest here was the negative association between awareness of how to remove data and lower concern levels. This negative association suggests that corporate measures should be taken to inform

customers of information-deletion options, which would likely reduce consumers' concerns about information privacy.

In sum, the analysis of consumer privacy concerns in South Africa indicates that there is substantial concern about consumer privacy issues among consumers in South Africa. Consumers display high levels of heterogeneity in their privacy concerns as well as in their information privacy-related behavior, which could potentially be used to actively manage responsible DM practices.

CONSUMER VIEWS IN AUSTRALIA

Sampling and Data Collection

The target population for this part of the study included all adults above age 18 residing in Australia. The sampling frame consisted of individuals participating in an established on-line Internet panel. Data was collected by Pureprofile, a permission-based electronic DM service based in Sydney, Australia. Pureprofile sent the questionnaire to a random sample of 2,500 panelists across Australia, assuming a response rate of 40% to the 17- to 20-minute-long questionnaire. The Pureprofile panel is representative of the Australian population based on the Australian Bureau of Statistics census data, although bias is likely because all panelists have on-line access. The questionnaire was programmed in HTML and made available on-line to the panel members. Respondents received eight Australian dollars to participate in the study-a standard procedure when collecting data through Pureprofile (with the compensation amount depending on the average time required to complete the survey). A total sample of 1,055 respondents resulted from this survey (42% response rate). see Table 3 for sociodemographics of the Australian respondents based on the 2001 census.

Measurement Instrument

The survey conducted in Australia was based on the South African study. The replication study used a large number of items from the original questionnaire: items related to information privacy concerns; items from the PSI; binary items measuring consumers' actual protective behavior, experiences of privacy invasion, knowledge of specific data practices, and Internet and DM behaviors; and sociodemographic questions. The only change to the South African questionnaire was in the sociodemographic criteria relating to education and income variables, to better capture the Australian marketplace.

Results

The views of Australian respondents are shown in Table 4. The highest agreement levels are reached on items relating to privacy protection, which capture the view that companies should have privacy policies in place to protect their customers. Companies should therefore undertake their DM activities in a responsible manner; otherwise, respondents' behavioral intentions will be to take action if they feel that their personal information is misused. The responsibility assigned to the government is clearly visible:

About two-thirds of respondents feel that public policymakers should assure that personal information is protected. Views on the role of the government are thus highly heterogeneous in the Australian sample, with about half of the respondents expressing concern about the misuse of their information and slightly more than one-third expressing their skepticism about how companies treat their data.

In sum, Australians demonstrate a generally high level of concern regarding privacy issues. There seems to be a substantial amount of heterogeneity with regard to consumer privacy concerns, however. For instance, 47% of respondents state that they receive too much unrequested advertising material, indicating that about half of them feel very strongly that they do not wish to be sent information, whereas the other half does not feel as strongly or is not bothered, with some possibly even welcoming the information. The managerial consequence of this is that the responsible marketing action may not be to cease sending information to all consumers. Instead, it would be optimal to use the differences in preferences and provide information to those who are interested while not mailing to those customers who do not wish to receive information. By doing so, responsible marketing is not in contradiction with economic rationale.

An exploratory post hoc segmentation analysis was undertaken next using the same methodology and stability analysis as described for the South Africa study. The four-cluster solution emerged as most stable and was therefore used for interpretation of behavioral heterogeneity. The resulting segments are very distinct regarding information privacy-related behavior, consumer views, and sociodemographics (segment profiles, tables including background variables, and test values are available from the authors), supporting the notion that heterogeneity of consumers may provide a useful basis for developing customized responsible DM strategies.

Finally, the association between Australian consumer views and consumer behavior was investigated. Again, the process involved a summation of all responses in the privacy scale, after which ANOVA were computed to assess the association between attitudes toward privacy issues and market-relevant behavior.

The following behaviors/experience were found to be significantly (at a 95% level) associated with higher levels of privacy concerns: refusal of information; notifying company that do not want to receive advertising material; request not to share information with others; and (not unexpectedly) having experienced violation of one's privacy. No association was found regarding the request to obtain information about how the protection of personal information is ensured, the use of the Internet for shopping, or the use of Internet banking.

Respondent awareness of how information can be deleted from the company database is associated with lower privacy concerns. This reflects the findings in the South African sample, which points to an excellent opportunity for responsible direct marketers to reduce privacy concerns among their customers. Furthermore, respondents who shop through catalogues, brochures, toll free numbers, and the telephone in general show lower privacy concerns.

Both the South African and Australian study (despite the independent contexts and samples) show that (1) significant privacy-related concerns exist among consumers, (2) concerns about privacy are associated with protective consumer behavior, and (3) consumers have heterogeneous views and behaviors regarding certain aspects of information privacy and DM. As mentioned previously, this opens up opportunities for different communication strategies directed toward different consumer segments based on varying privacy concerns and behaviors. In the next section, we therefore assess the usefulness of an existing tool for segmenting consumers (the PSI, which was discussed in the literature review) based on their privacy concerns, with the purpose of actively managing consumers' privacy concerns and thus increasing the level of responsible DM behavior.

ASSESSMENT OF THE U.S. PSI FOR RESPONSIBLE DM

As discussed in the literature review, the Privacy Segmentation Index (PSI) is a tool used to divide the American public into three privacy-sensitive segments: "Fundamentalists" (high concern); "Pragmatists" (medium concern); and "Unconcerned" (low concern). The distribution of respondents into a segment is based on responses to three statements: (1) "consumers have lost all control over how personal information is collected and used by companies"; (2) "most businesses handle the personal information they collect about consumers in a proper and confidential way"; and (3) "existing laws and organizational practices provide a reasonable level of protection for consumer privacy." Respondents who strongly agree or slightly agree with the first statement and strongly disagree or slightly disagree with the second and third statements are grouped into one segment. Respondents who strongly disagree or slightly disagree with the first statement and strongly agree or slightly agree with the second and third statements are grouped into the second segment. All the remaining options form the third segment.

To assess how useful the PSI index is, we assigned the South African and Australian respondents to the respective segments. Table 5 shows the results, as well as a tentative comparison with the United States.

Interesting to note from Table 5 is the similar distribution of respondents in each privacy-sensitive segment. This immediately raises questions about whether respondents of all three countries really feel the same about privacy, and whether the classification index is able to guide businesses or regulators regarding how to communicate with consumers in each segment. To answer this question, we must assess how well the grouping discriminates with regard to consumer views, sociodemographics and, most important, behavior. The results are provided in Table 6 (for consumer views and scociodemographics) and Figure 2 (for behavioral variables). Table 6 includes the percentage of members of each of the three segments who agree strongly with the consumer views listed in the first column. For the sociodemographic information at the end of Table 6, the percentages for each category listed are provided. Chi-squared tests were computed to assess whether or not the three segments differ with regard to each of those variables. The p values of the $\chi^{sup\ 2}$ tests are provided in the last column. Most p values are highly significant (uncorrected and Bonferroni-corrected for multiple testing),

thus indicating that the PSI is indeed a valuable tool for grouping consumers into segments based on their privacy concerns. This will enable direct marketers to develop different marketing communications for consumers who are concerned about the handling of their personal information.

While the discriminatory power of the PSI for both sociodemographics and consumer views is good, it fails to explain behavior very well, as can be seen in Figure 2. Here the profiles derived from the analysis are indeed not very distinct. The "Pragmatics" segment demonstrates an average profile. "Fundamentals" have been victims of privacy invasion more frequently than average, and undertake slightly more protective measures. The "Unconcerned" group exhibits slightly stronger shopping behavior through channels that could lead to privacy invasion. In sum, one can conclude that the discriminatory power of the PSI for behavior is not very good: Only four behavioral variables are significantly different for the three groups formed by the PSI, after Bonferroni correction of χ^sup 2^ p values for multiple testing was performed. These variables included refused information, requested removal of information, notified company not to receive unrequested advertising material, and had been a victim of privacy invasion.

In fact, the PSI appears to mainly discriminate between "Fundamentalists," who protect themselves more because they have experienced privacy invasion before, and those who have not. While the PSI is very valuable in grouping respondents on the basis of only three questions and arriving at a consumer grouping that discriminates very well with respect to consumer views and sociodemographic characteristics, the usefulness of the index could be further increased by improving its association with consumer behavior. In the next section, we therefore suggest a refined PSI to improve the discriminatory power for behavior.

A REFINED PRIVACY SEGMENTATION INDEX (REFPSI)

We propose an extension of the PSI classification by including three behavioral variables in addition to the three belief variables used at present. Variables suitable for such an extension are items that have proven to discriminate well between behavioral market segments. Given that behavioral segmentations have been developed for both the South African and Australian samples, such variables can easily be identified with three variables emerging as highly discriminatory for behavioral segments. These variables (Internet banking, shopping via catalogues, and refusing information) were therefore included in the RefPSI (see Figure 1 and interpretation thereof).

The same segmentation procedure was followed as for the behavioral segmentations. Cluster numbers from 2 to 10 were explored. A total of 30 replications of the partitioning algorithm were computed for each number of clusters to assess the stability of solutions. Based on this stability analysis, the 6-cluster solution was chosen. Segment profiles based on the variables used to develop the grouping are provided in Figure 3.

In Figure 3, it is clear that Segment 1 represents a group of trusting consumers who believe that companies and the government protect consumer privacy sufficiently. They

do not, however, expose themselves much to any of the shopping behaviors that could lead to misuse of personal information. Segment 2 is not as optimistic. People in this group believe that consumers have lost control, and more frequently than average, they have refused to give companies their personal information. Their concern and protective behavior may well stem from the fact that they are heavy users of Internet banking (all members of this group use Internet banking). Segment 3 is very similar to Segment 2, except that members of this group engage not only in Internet banking, but all of them also purchase products through catalogues, thus engaging in a wider portfolio of risky shopping behavior, as compared with Segment 2. Segment 4 trusts companies and pubic policymakers for protection and does not use Internet banking, but makes slightly more use of catalogue shopping options than the average consumer. Segment 4 believes that consumers have lost control over their personal information and engages in less risky shopping behavior than the average consumer. Segment 5 members do not use Internet banking and believe that consumers have lost control over their information. Furthermore, they believe that companies do not handle their personal information properly and that the government does not have legislation in place to protect their personal information. Finally, Segment 6 engages in various forms of risky shopping behavior, but trusts that companies and the government will protect them.

In addition to the item-by-item analysis of the segments described above, an ANOVA was conducted to test whether the overall privacy concern scores differ across groups. This difference was highly significant ($F = 28$, $df = 5$, $p < .001$), with Segment 2 being most concerned about information privacy, followed by Segment 5 and Segment 3. Segments 4 and 6 were found to be the least concerned, which is in line with the segment profiles revealed above.

The proposed, extended segmentation discriminates very well between segments with respect to sociodemographics, consumer privacy concerns, and behavior, as shown in Table 7 and Figure 4. Table 7 contains percentages of segment members and p values based on χ^sup 2^ tests.

As can be seen from Table 7, the segments differ highly significantly in their views on information privacy concerns. This basically reflects the pattern that was obtained by using the unrefined original version of the PSI, and indicates that the segments are highly distinct with respect to their privacy concerns. In addition, the sociodemographic characteristics discriminate between the segments better than was the case for the original PSI. All the sociodemographical variables for South Africa differ between segments, and, except for ancestry, this is the case for the Australian sample as well. However, this has to be seen as a side effect of the refined segmentation. The real aim was to improve behavioral discrimination, which is illustrated in Figure 4. A simple visual comparison of Figures 2 and 4 indicates that the RefPSI discriminates better in terms of privacy-related consumer behavior than the original PSI does (χ^sup 2^ tests on all behavioral variables are highly significant at the 95% level), thus making it more relevant for managerial use in the context of responsible DM.

In sum, it appears that the refined PSI has some potential as a market-oriented tool for responsible DM given that (1) distinct market segments can be identified with respect to privacy concerns and privacy-related behavior; (2) targeted DM based on both a product interest segmentation and a privacy concern segmentation is easy to implement; and (3) it is in the company's interest to avoid wasting resources on customers who are highly concerned about privacy and will not react to DM approaches, as well as to find better ways to communicate with those customers with milder levels of concern or more discriminated information privacy concerns.

USING REFPSI FOR RESPONSIBLE DM

To implement the proposed market-oriented approach to responsible DM, information is needed on how to assign individuals to each of the constructed segments. Two approaches are put forward: the rules-based approach and the distancebased approach. Of course, the basic requirement is that the six questions used to classify respondents are available within the data set. Although this may appear to be a major limitation, these questions are less dangerous and intrusive to ask people on first contact than much of the personal information requested by companies. It is therefore quite feasible to collect these additional six pieces of information needed for marketoriented responsible DM.

Rules-Based Approach

Following the mechanism of the PSI, a set of rules can be developed that assigns each respondent to one of the privacy concern segments. Table 8 presents the assignment rules for new respondents to the RefPSI segments. The first six columns provide the items/questions in the survey to be used to construct the grouping. For each one of the segments (shown in column 7), the answer pattern of respondents is prescribed in the table.

This rules-based approach allows an a priori assignment that is reasonably precise in its ability to assign respondents to groups and to assign only pure types. Consequently, respondents who do not demonstrate one of the above patterns will form another group of "other respondents." If it is preferable for a company to be able to assign each of their customers to exactly one of the six segments, the distance approach should be used.

Distance Approach

If every single respondent from a new survey has to be assigned to one of the six segments, the distance of each new respondent to each of the segment's centroids can be computed, and the respondent can be assigned to the segment that best matches his or her response pattern. The centroids for the six segments are provided in Table 9.

If, for instance, a respondent agrees with the first question, disagrees with the second, third, fourth, and fifth, and agrees with the last question, the numerical response pattern would be 1-0-0-0-0-1. This response pattern could not be classified based on the rule-based approach outlined above, as none of the segments have precisely this pattern of

response. If, however, the vector distance between each of the centroids given in the above table and the new respondent's pattern were computed, it would clearly demonstrate the lowest distance to Segment 5. The advantage of this approach is that each new respondent is assigned to one of the segments. This may be very important for companies that would like to communicate with every customer, and can now select the optimal communication message based on consumers' privacy concern patterns. The disadvantage, on the other hand, is that the segments are not as clear as they are when the rule-based assignment approach is chosen, as they become blurred by the heterogeneity of respondents.

In sum, it is proposed that the PSI is refined by including three behavioral variables in addition to the original three belief variables. This refined segmentation results in six distinct clusters-distinct in their privacy concerns and privacy-related behaviors, as well as in sociodemographics. Such distinct segments can be used for responsible DM, where not only consumers' product interests are used for targeting, but also their preferences regarding DM and the use of their personal information. Using the market segmentation approach for responsible DM has a higher probability of adoption by companies, because it follows the economic rationale of not spending resources on individuals who prefer not to be contacted or who have major privacy concerns, as opposed to enacting laws restricting direct marketers that are perceived as being opposed to their profit-maximization interest. The descriptive data analyses as well as the market segmentation presented in this paper have several implications for different stakeholder groups, which are discussed below.

IMPLICATIONS FOR KEY STAKEHOLDERS

Consumer Privacy as a Responsible Businesses Issue

When DM transactions are viewed as an implied social contract, consumers provide personal information in exchange for receiving solicitations and other information, based on an expectation that their personal information will be managed and protected in a responsible fashion. If the consumer considers marketing communication as disturbing, it may negatively affect attention to and perception of the marketing message. The findings suggest to companies that the majority of South African and Australian respondents expect companies to communicate why they want to collect consumers' personal information, how this information will be protected, and how it will be shared with others. It is very clear from the survey results that direct marketers must provide consumers with more opportunities to engage in consensual information exchange, whereby consumers could indicate what type of information they wish to provide and release for marketing purposes, and to which organizations that information could be disseminated. The results seem to indicate that there is still a gap between business practices and consumer concern as reported by Milne in 2001. Direct marketers pride themselves on managing databases effectively. Surely, if databases empower direct marketers to have better-targeted communications, these same databases should include customers' privacy needs and wants as they pertain to communication from direct marketers. A well-managed database-marketing program should help identify privacy

concerns because this would allow the marketer to target only those consumers with some interest in the offer, in a way or at a time that is acceptable to them.

Quite alarming is the high level of concern reported in the two privacy studies relating to the dissemination of information-an activity that is standard practice for many direct marketers. More than three-quarters of both the South African and Australian respondents felt strongly that they do not want their information shared with third parties without their permission, with up to 80% intending to request that their information be removed from the database if sold to others. Direct marketers have to manage the chain of trust they create when they share customer information with other marketers. Milne and Boza (1999) even suggested that building trust may be more effective than trying to reduce privacy concern. Their findings indicate that respondents who trusted their organizations highlighted positive experiences and reputations of the organizations, including how the organization shares information with third parties. Schoenbachler and Gordon (2002) note that having a clear and credible privacy notice helps direct marketers build a positive reputation with consumers. One solution could be to develop a framework that balances consumer privacy concerns with the information needs of the organization(s) involved. As a first step, direct marketers could make a commitment to customers to obtain their permission before disclosing personal information to third parties.

The segments uncovered in this study demonstrate the usefulness of investigating patterns of consumer sensitivity with respect to information privacy. These segments, and possibly segments direct marketers might choose to construct using their own consumer data, can provide organizations with the enhanced ability to develop communications that will align information-handling practices with consumers' concerns. Figure 1 identified different segments based on respondents' information privacy-related behavior and showed how privacy differences create communication opportunities. For example, Segment 1 contains respondents who are keen Internet users, although they exhibit strong protective behavior and will act negatively if they feel violated. This signals to direct marketers that this segment is very willing to become involved in DM activities through certain channels, but that members of this group should be handled with care if the company wants to build long-term relationships. This includes not bombarding these consumers with advertising materials, since more than two-thirds of them have notified companies that they should not send them any unrequested advertisements. Knowing which consumers are sensitive to which issues of information privacy, and how they react when not confident of the company's information protection practices can reduce the number of hostile, uninterested, and inappropriate prospects, leading to an improvement in targeting efforts. To take responsibility means that DM communications to targeted segments should be consistent with the segment's expectations, values, and norms. Aligning communications with consumers' concerns is essential if organizations want to break through the communications barrier and capitalize on the potential reputational benefits of acting responsibly. Indeed, there is a benefit to improving the effectiveness of communicating the organization's privacy protection behavior if consumer power is to be engaged and purchase behavior influenced. The suggested refined PSI provides a framework for companies that want to act responsibly by segmenting their market

according to consumers' preferences regarding DM and the use of their personal information.

Organizations have to recognize that they will not lose customers if they offer privacy protection options; rather, they will be setting the scene for a trusting relationship. It is clear that members of Segment 3 (see Figure 1) have a low involvement in DM activities, probably because they do not feel they can trust companies. With 72% of these respondents reporting that they have been victims of privacy invasion, it seems they have good reason not to get involved in the DM activities of companies. Unless direct marketers can collect, store, transfer and retrieve customer information in a responsible way, consumers will adopt protective behaviors aimed at limiting contact with direct marketers. Findings from this study confirmed prior findings that there are significant associations between privacy-related consumer behavior and privacy concerns: concerned consumers adopt protective behaviors such as refusing to provide personal information, requesting removal of information from databases, and notifications not to send unrequested advertising material-all of which are negative consequences from a company perspective. This is demonstrated by Segment 3 (see Figure 1), with 77% of these respondents asking not to receive unrequested advertising material, 82% requesting not to share information, and 65% asking that companies remove their details from the company database. Some studies have indicated that despite their strong opinions and privacy preferences, many consumers are unable to act accordingly (Berendt, Gunther, and Spiekermann 2005; Sheehan and Hoy 1999). Nevertheless, although many consumers may not act directly (e.g., by removing their name from a database or placing their name on a do-not-call list), many act indirectly by providing incomplete or inaccurate information, by communicating concern to friends and family, or by showing withholding behavior in avoiding purchases from DM companies. This is demonstrated by Segment 2 (see Figure 1) whose members have never refused to provide their personal information to companies or requested that companies not share their information, but have acted indirectly by not purchasing through any DM channels. Given that consumer concern affects behavior, direct marketers need to communicate their protective information-handling practices to consumers to work toward reducing direct and indirect negative behavior.

Successful IMC should keep the brand image consistent across the advertising channels. Figures 1, 3, and 4 indicate that many consumers are not utilizing DM channels (Internet and catalogues/brochures) to their full potential. This may be because of the relationship between past direct marketing experience and multichannel buying, which is affected by the nature and quality of the direct marketing experience (Schoenbachler and Gordon 2002). This suggests that customers' privacy preferences in the DM channels should be respected to enable establishment of a consistent brand identity throughout the organization. Advertising efforts should thus focus on customers, rather than channels. This will enable organizations to market to customers based on their channel preferences, including their privacy preferences in the direct channels. When the organization's focus is customer-centric, it will design communication strategies that are relevant to the customer's needs and preferences. Alleviating information privacy concerns will increase consumer trust, which may lead to an increase in multichannel shopping.

Findings from one poll provided food for thought when it revealed that perceived marketing responsibility had more influence on consumers than advertising (Gaines 1998). From Tables 2 and 4 it is evident that both the South African and Australian consumers (70% +) want organizations to act responsibly by implementing privacy protection policies. Organizations that accept and fulfill their privacy-related obligations through the implementation of privacy protection policies should find it easier to develop close business relationships with customers who prefer them to competitors that do not make privacy a priority.

Direct marketers can consider educating consumers on how to protect their information, how to query information held in an organization's database, and how to remove their information if they want to. Inspecting the different segments in Figure 4 shows that many consumers are not educated on how to protect their personal information. Several segments score below average on protective behavior such as notifying companies not to send advertising material, requesting removal of information, and requesting not to share information. If consumers are better educated, they should be able to take better precautions to protect themselves against privacy invasion. In an on-line environment, for example, users can install firewalls, check for fraudulent Web sites, remove information from Web sites, read on-line privacy policies, opt-out of third-party information sharing, and check for cookies (Milne, Rohm, and Bahl 2004). To this end, both consumers and direct marketers may need to be better educated about what is acceptable and what is not acceptable in the future.

Responsibility from a Public Policy Perspective

The information revolution opens up important public policy issues, as organizations increasingly build comprehensive consumer databases and apply sophisticated data-mining techniques to target consumers. One issue that came out very strongly in both the South African and Australian studies was the public's choice to have their information privacy protected by government. The majority of respondents indicated that they expect government to limit businesses' collection and use of personal information only to that needed for a specific transaction, and that government must do more to protect the safety of personal information. Consumers' high expectations for government protection suggest that the public will embrace protective legislation. It is interesting to note the extremely high expectations of the South African respondents that government should protect them. This may be indicative of the current public policy situation there: South Africa is in the process of developing privacy legislation, but proper legislation is not yet in place. In all probability, this accounts for the very strong opinions expressed on government protection.

Many organizations are reactive in their management of privacy issues, waiting for an external threat before they implement cohesive policies. Milne and Culnan (2004) suggest that clear privacy notices seem to be a tool that can help consumers to decide whether to interact and/or disclose information to an on-line marketer. It is a well-known fact that DM industries all over the world intend to demonstrate a belief that self-regulation is the answer to local consumer and government privacy concerns.

Improvements in technology create new privacy issues for direct marketers, however, because they enable companies to collect more personal information without the consumer's knowledge. This may lead to a need for additional forms of self-regulation such as proactive independent verification by qualified accredited organizations (Milne 2001). Effective self-regulation requires visible steps, such as implementing periodic consumer reviews to ensure the accuracy of database information. It is essential that consumers be made aware of self-regulatory actions and that they are educated about information practices in general. Most of the segments presented in Figures 1,2, and 4 show low levels of awareness regarding options to remove personal information from companies' databases, despite the fact that media preference services are offered by most associations in direct marketing industries. This confirms the view by Milne and Rohm (2000) that more work is needed by the industry to increase consumer knowledge of data collection practices and awareness of name-removal procedures. Without such commitment, it is likely that consumers will continue to voice their discontent over irresponsible marketing-information practices and will look, instead, for governmental protection and legislative action. This is exactly what respondents asked for in this study: Between 56% and 71% of respondents want government to restrict information collection, between 61% and 72% expect government to do more to protect information, and between 65% and 70% want government to limit the use of information by companies.

Milne and Boza's (1999) study suggested that instead of reducing privacy concerns, organizations should build trust and give control to consumers. This should go hand-in-hand with clear communication of policies and building a reputation for fairness. Organizations need to not only communicate their privacy policies, but also provide proof of their compliance. Unfortunately, the high level of information privacy concern that has emerged over the past decade may demonstrate that self-regulation programs have failed to provide enforcement mechanisms and that consumers now expect government to address the issue. It is very interesting that one of the findings from this study indicates that those who are less aware of options to remove their personal information from company records are more concerned about privacy. This negative association should signal to direct marketers that their mail and telephone preference lists are not communicated clearly to consumers, and that this protective mechanism is not serving its purpose. Providing consumers with an opportunity to remove their name from a mailing list is essential to uphold good customer relationships (Milne 1997). If organizations fail to self-regulate effectively, legislation is likely to be enacted to force compliance.

Consumer Privacy as a Global Issue

Although the research did not focus on consumer privacy from a global perspective, it is important to note that privacy concerns not only have implications for local businesses, but also impact on individual countries, as globalization represents a reality for many stakeholder groups. Increasing global interdependence means possible negative consequences for those businesses and/ or countries that rely on the unimpeded flow of personal information and that cannot claim to protect the data of consumers in ways that

match the standard of the trading partner. With privacy becoming an important trade issue, information privacy concerns can create a barrier to international trade (Agre and Rotenberg 1998). Countries and businesses must realize that a lack of proper data protection can have adverse consequences for future transactions. Much international legislation forbids the transfer of personal data to a country (such as South Africa) that does not provide a level of protection similar to its own. Therefore, it is quite likely that some organizations may be denied access to information from their own subsidiaries.

There is an increasing perception that adequate privacy protection is a necessary condition for being on the global information highway. The beginning of the information age has increased the importance of personal data protection to a level where governments and international organizations around the world have to pay attention to privacy legislation. Many countries have legislated regulations concerning the use of consumer data, of which Australia is one. Unfortunately, enforcement of regulations is often somewhat lacking, or in some countries, such as South Africa, even nonexistent. A lack of proper regulatory frameworks may have far-reaching implications if an international business or country fails to comply with existing global regulations. It is thus evident that it is not only individuals who are developing strong expectations regarding government's future role in the protection of information-handling practices (refer to the expectations about government in Table 2); the global community is also putting pressure on international businesses and countries to take appropriate action.

CONCLUSIONS

Communication is the process by which individuals share meaning. Only if each participant fully understands the needs and wants of the other's communication will dialogue occur and relationships develop. The studies in this paper investigated consumers' views on information privacy as well as associations between consumer privacy concerns and consumption-related and privacy protective-related behaviors using independent samples from South Africa and Australia. The key findings are that (1) the level of privacy concern is high, although (2) there is a substantial amount of heterogeneity among respondents both with regard to information privacy concerns and privacy-related consumer behavior. Furthermore, (3) the level and nature of privacy concerns are associated with specific privacy-related behaviors-both actively protective behaviors (e.g., requesting deletion of private information from the company's database) and passively protective behaviors (avoiding shopping over the telephone). Based on these findings, the usefulness of a market-oriented approach to responsible DM was investigated.

Based on the two data sets examined, it appears that the use of three items capturing privacy concern dimensions and three items capturing behavioral information lead to a very distinct consumer privacy segmentation of consumers. This could be used by companies, not only to target the right people with the right product, but also to target the right people with the right approach in terms of information privacy (and to avoid targeting very sensitive segments altogether, such as Segment 4 in Figure 1, of which 100% of the respondents refused to provide personal information). Such a market-

oriented approach to responsible marketing would be a very useful addition to the mainly regulations-driven toolbox of measures designed to prevent information privacy violations. In addition, it fits in with the economic rationale of companies, for it improves the effectiveness of their communication with consumers. Surely, if 69% to 77% of respondents (see Segments 1 and 3 in Figure 1) indicate that they do not want to receive unrequested advertising material, it will not be cost-effective to communicate with these individuals. The likelihood of companies wishing to adopt a more market-oriented approach is thus expected to be higher than the motivation to abide by rules, regulations, and policies that appear counterproductive from a profit-maximization point of view. Marketing communication thus has the ability to interface effectively with key stakeholders.

Additional insights into the behavioral segments uncovered in this study could be gained if organizations collected individual-level data that would permit more detailed profiling of segment members. A multinomial logit model could then be computed to determine which of the profiling variables predicts segment membership best. This would enable market-oriented use of DM, even if the customer is not yet in the database of the company, because the discriminating profiling variables (such as media behavior, for instance) could be used to target segments.

The heterogeneity perspective proposed in this study can also be extended in other directions. For instance, assuming availability of appropriate data, customers could be segmented using their stated preference for various kinds of DM communications as a segmentation base. This could lead to segments that wish to receive catalogues by conventional mail and special offer notices by e-mail, but do not want to be called at home. Again, this would represent an economical and responsible approach to DM by saving on communication cost that is not likely to lead to a response and would help companies maintain a positive relationship with customers by supplying what they appreciate and omitting contact that they perceive as unsolicited and unwelcome.

The presented study has a number of limitations. First, neither the South African sample nor the Australian sample was entirely representative of the two countries because the sampling frames do not provide a complete and accurate listing of all individuals. second, although this study found several significant correlations between consumers' privacy concerns and behavior, we cannot infer causal relationships between privacy concerns and behaviors, as no experimental manipulations were undertaken in this study. It is suggested that future research focus more on specific behaviors, as well as on their causal relationship with privacy concerns over time. Third, the effectiveness and likelihood of corporate adoption of the proposed approach were not investigated as part of the study. Finally, the information privacy concerns investigated in these two studies were very prevalent and conducted in a general commercial environment across a broad spectrum of DM activities. One may find a different picture for separate DM activities and/or channels (such as e-mail).

Future research efforts could compare the effectiveness of privacy protection activities such as privacy policies, selfregulation, and legislation. Those efforts could be compared

with the effectiveness of the suggested segmentation-based responsible DM approach, which benefits consumers by increasing the protection of their personal information while also being in line with the profit-maximizing aim of companies. Responsible companies could refrain from contacting individuals with high levels of privacy concerns or who demonstrate high levels of protective behaviors; by doing so, they would save resources likely to be wasted due to a lack of responsiveness to DM activities from those customers. Furthermore, DM campaigns could be developed specifically for such segments, customizing the message to their privacy concerns and providing the information needed to weaken such concerns and build trust. In addition, future researchers could investigate the difference between established relationships (where customers may have more leeway) and cold calls. Another area of further research would be to study consumer heterogeneity in the context of privacy violation in a low-cost setting, such as sending bulk e-mails. This field presents an entirely new challenge, as it is very different in nature, with the recipient possibly not perceiving such a strong intrusion of his or her privacy due to public availability of e-mail addresses on the Internet. Also, in this situation, companies that are not ethically motivated to protect consumer privacy have virtually no incentive to do so.

Information privacy is not an issue that will be resolved quickly; it requires a multifaceted approach involving a combination of education, self-regulation efforts, privacy policies and legislation, and the proposed market-driven approach to responsible IMC, more specifically, DM. It is therefore vital for consumers, industry, and government to accept the challenge and commit to an enhanced protective environment, especially since all parties will be worse off if the urgency of the matter is not accepted and addressed. Information privacy is, and will remain, an important issue cutting across a wide range of factors, from the individual level to governmental policy development and legislation, to global trade. For a DM industry whose heart is a database and whose lifeblood is communication with customers, failure to address these privacy and security issues is potentially life threatening. The personal information provided by customers is a treasure that should be handled with respect and care, as this is a marketer's greatest asset.

This project was supported by Ernst and Young: Retail and Consumer Products Division in South Africa and the Faculty of Commerce Special Initiatives Fund at the University of Wollongong, Australia.

REFERENCES

Agre, Philip E., and Marc Rotenberg (1998), Technology and Privacy: The New Landscape, Cambridge: MIT Press.

Berendt, Bettina, Oliver Gunther, and Sarah Spiekermann (2005), "Privacy in E-Commerce: Stated Preferences Vs. Actual Behaviour," Communications of the ACM, 48 (4), 101-106.

Buchta, Christian, Evgenia Dimitriadou, Sara Dolnicar, Friedrich Leisch, and Andreas Weingessel (1997), "A Comparison of Several Cluster Algorithms on Artificial Binary Data Scenarios from Travel Market Segmentation," working paper no. 7, SFB Adaptive Information Systems and Modelling in Economics and Management Science, Vienna University of Economics and Business Administration, Vienna.

Campbell, Alexandra J. (1997), "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy," Journal of DM, 11 (3), 44-57.
Chen, Kuanchin, and Alan I. Rea, Jr. (2004), "Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques, "Journal of Computer Information Systems, 44 (Summer), 85-92.
Culnan, Mary J. (1993), "How Did They Get My Name: An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," MIS Quarterly, 17 (3), 341-362.
____ (1995), "Consumer Awareness of Name Removal Procedures: Implications for DM," Journal of DM, 9 (2), 10-19.
Earp, Julia B., and David Baumer (2003), "Innovative Web Use to Learn About Consumer Behavior and Online Privacy," Communications of the ACM., 46 (April), 81-83.
Evans, Martin, Maurice Patterson, and Lisa O'Malley (2001), "The DM-Direct Consumer Gap: Qualitative Insights," Qualitative Marketing Research: An International Journal, 4 (D, 17-24.
Forcht, Karen A., and Daphyne S. Thomas (1994), "Information Compilation and Disbursement: Moral, Legal and Ethical Considerations," Information Management and Computer Security, 2 (2), 23-28.
Gaines, Charles (1998), "Next Step Is Cause Marketing: Businesses Start Own Non-Profits," Marketing News, 32 (21), 4.
Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right, "Journal of Public Policy and Marketing, 19 (Spring), 149-166.
Grönroos, Christian (2004) "The Relationship Marketing Process, "Journal of Business and Industrial Marketing, 19 (2), 99-113.
Harris Interactive (2000), "Poll on Americans' Fears on the Internet," presented at Privacy and American Business's Eighth Annual National Conference on "Managing the New Privacy Revolution," Washington, DC, March 20-22.
___ (2002a), "Online Consumer Behaviour and Concerns After September 11: A 2-Wave Survey," study no. 15938, presented at Privacy and American Business's Eighth Annual National Conference on "Managing the New Privacy Revolution," Washington, DC, March 20-22.
___ (2002b), "Privacy On and Off the Internet: What Consumers Want," presented at Privacy and American Business's Eighth Annual National Conference on "Managing the New Privacy Revolution," Washington, DC, March 20-22. Privacy and American Business, study no. 15229, 1-127.
Harris Interactive and Alan F. Westin (1998), "Privacy Concerns and Consumer Choice," Privacy and American Business (November), 1-122.
___ and ___ (2000), "The IBM-Harris Multi-National Consumer Privacy Survey," Privacy and American Business, 7(1), 1-16.
Heinonen, Kristina, and Tore Strandvik (2005), "Communication as an Element of Service Value," International Journal of Service Industry Management, 16(2), 186-198.
Jordaan, Yolanda (2004), "Exploring and Validating Consumers' Information Privacy Concerns," Management Dynamics, 13 (2), 2-12.

Martinetz, Thomas, and Klaus Schulten (1994), "Topology Representing Networks," Neural Networks, 1 (5), 507-522.
Meinert, David B., Dane K. Peterson, John R. Criswell, and Martin D. Grassland (2006), "Privacy Policy Statements and Consumer Willingness to Provide Personal Information," Journal of Electronic Commerce in Organizations, 4 (January/ March), 1-17.
Milne, George R. (1997), "Consumer Participation in Mailing Lists: A Field Experiment," Journal of Public Policy and Marketing, 16 (2), 298-309.
___ (2000), "Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue," Journal of Public Policy and Marketing, 19(1), 1-6.
___ (2001), "The Effectiveness of Self-Regulated Privacy Protection: A Review and Framework for Future Research," Handbook of Marketing and Society, Paul N. Bloom and Gregory T. Gundlach, eds., Thousand Oaks, CA: Sage, 462-485.
___, and Maria-Eugenia Boza (1999), "Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices," Journal of Interactive Marketing, 13 (1), 5-24.
___, and Mary J. Culnan (2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy 'Notices," Journal of Interactive Marketing, 18 (3), 15-29.
___, and Mary E. Gordon (1994), "A Segmentation Study of Consumers' Attitudes Toward Direct Mail," Journal of Direct Marketing, 8 (2), 45-52.
___, and Andrew J. Rohm (2000), "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives," Journal of Public Policy and Marketing, 19(2), 238-249.
___,___, and Shalini Bahl (2004), "Consumers' Protection of Online Privacy and Identity," Journal of Consumer Affairs, 38 (2), 217-232.
Nowak, Glen J., and Joseph E. Phelps (1992), "Understanding Privacy Concerns: An Assessment of Consumers' Information-Related Knowledge and Beliefs," Journal of DM, 6 (4), 28-39.
___, and ____ (1997), "DM and the Use of IndividualLevel Consumer Information: Determining How and When Privacy Mutters," Journal of DM, 11 (4), 94-108.
Page, Carole, and Ye Luding (2003), "Bank Managers' DM Dilemmas: Customers' Attitudes and Purchase Intention," International Journal of Bank Marketing, 21 (3), 147-163.
Patterson, Maurice (1998), "DM in Postmodernity: Neo-Tribes and Direct Communications," Marketing Intelligence and Planning, 16(1), 68-74.
Phelps, Joseph E., Glen Nowak, and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," Journal of Public Policy and Marketing, 19 (D, 27-42.
Schoenbachler, Denise D., and Geoffrey L. Gordon (2002), "Multichannel Shopping: Understanding What Drives Channel Choice," Journal of Consumer Marketing, 19(1), 42-53.
Sheehan, Kim B. (1999), "An Investigation of Gender Differences in On-line Privacy Concerns and Resultant Behaviors," Journal of Interactive Marketing, 13 (4), 24-38.
___, and Mariea G. Hoy (1999), "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns, "Journal of Advertising, 28 (3), 37-51.

South African Advertising Research Foundation (SAARF) (2001), AMPS2001B, available from SAARF, South Africa, www .saarf.co.za.
Statistics South Africa (2001), Census 2001, available from Statistics South Africa at www.statssa.gov.za/census01/html/ default.asp.
Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner, and Stephen McClure (1983), "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organisations," Journal of Applied Psychology, 68 (3), 459-468.
Tapp, Alan (2000), Principles of Direct and Database Marketing, 2d ed., London: Pearson Education.
Taylor, Curtis R. (2003), "Consumer Privacy and the Market for Customer Information," Rand Journal of Economics, 35 (4), 631-650.
Taylor, Raymond E., John A. Vassar, and Bobby C. Vaught (1995), "The Beliefs of Marketing Professionals Regarding Consumer Privacy," Journal of DM, 9 (4), 38-46.
Udo, Godwin J. (2001), "Privacy and security Concerns as Major Barriers for E-Commerce: A Survey Study," Information Management and Computer security, 9(4), 165-174.
Vidmar, Neil, and David H. Flaherty (1985), "Concern for Personal Privacy in an Electronic Age,"'Journal of Communication, 35 (2), 91-103.
Wientzen, Robert, and Lauren Weinstein (1997), "Private Lives: Public Records," Computerworld, 31 (36), 88-89.