INVESTIGATING THE RELATIONSHIP BETWEEN INTERNET PRIVACY CONCERNS AND ONLINE PURCHASE BEHAVIOR.

Mark Brown
Business School
University of Queensland
Australia
m.brown@business.uq.edu.au

Rose Muchira
School of Marketing
Griffith University
Australia
cadmu@hotmail.com

ABSTRACT

Many organizations now emphasize the use of technology that can help them get closer to consumers and build ongoing relationships with them. The ability to compile consumer data profiles has been made even easier with Internet technology. However, it is often assumed that consumers like to believe they can trust a company with their personal details. Lack of trust may cause consumers to have privacy concerns. Addressing such privacy concerns may therefore be crucial to creating stable and ultimately profitable customer relationships. Three specific privacy concerns that have been frequently identified as being of importance to consumers include unauthorized secondary use of data, invasion of privacy, and errors. Results of a survey study indicate that both errors and invasion of privacy have a significant inverse relationship with online purchase behavior. Unauthorized use of secondary data appears to have little impact. Managerial implications include the careful selection of communication channels for maximum impact, the maintenance of discrete "permission-based" contact with consumers, and accurate recording and handling of data.

Keywords: privacy, trust, Internet, consumer, confidentiality.

1. Introduction

In an age where relationship marketing is proclaimed to be one of the few sources of sustainable competitive advantage available to organizations, the Internet has been viewed as both panacea and anathema to marketers interested in fostering ongoing interaction with consumers. Modern relationship marketing is largely technology-driven [Gordon 199]) and often dependent upon high-quality, reliable customer databases from which to draw data and configure information depicting patterns of need within the customer and prospect population [Khalil and Harcar 1999]. Many marketers now focus on using technology, which is supposed to help them get closer to consumers and build ongoing relationships [Campbell 1997]. A critical success factor for customer relationship management is access to customer information. The better the information that is gathered, the better the company is able to meet its customers' needs [Nicovich and Cornwell 1998]. Misuse of collected customer information on the other hand, may lead the customer to have information privacy concerns.

Collecting data about consumers is helpful but perhaps even more important is using the data in a way that does not cause consumers to be concerned. It has been reported that ten percent of Web users never provide information to Web sites that require registration, resulting in a loss of information collected by the marketer [Kehoe, Pitkow, and Morton 1997]. A logical conclusion is that these consumers need to know that they can trust a company with their personal details, that is information that can identify them personally or be of a potentially sensitive nature, for example information regarding possessions, income, or health. Trust is important in relationship building. It contributes to satisfaction and long-term association over and beyond the effects of the economic outcomes of the relationship. Both trust and economic outcomes are conducive to relationship marketing success [Geyskens 1998]. Trust exists when one party has confidence in an exchange partner's reliability and integrity and it extends to all aspects of business and consumer interaction [Campbell 1997]. Lack of trust may also cause consumers to have privacy concerns.

Confidentiality is also an important part of successful relationship marketing. When a consumer trusts a company, they believe that their details are held in confidence and used by the company only in ethical ways. Research has shown that consumers are more concerned about situations where their personal and financial records are sold to other companies without their consent than they are about "relationship marketing" situations, whereby a company collects and uses information to repeatedly contact its own customers [Petrison and Wang 1995]. As such, it is reasonable to conclude that consumers have lesser privacy concerns when relationship marketing is practiced than when companies use their personal information for other purposes.

Successful relationship marketing is very dependent upon consumer perceptions of the organization. When companies trading via the Internet alter, manipulate, or misuse the information they have about consumers, it is possible they may jeopardize the relationship. Similarly, when they send unsolicited e-mail to consumers, they may risk destroying the relationship or the potential for creating one. Research has shown that activities such as sending unsolicited e-mail to consumers are also a reason for consumers to have privacy concerns [Korgaonkar and Wolin 1999]. As such, companies who trade via the Internet should try to gain a better understanding of the online consumer. Consumers are known to be sensitive to certain influences and are apt change their mind about a purchase decision at the last minute [Kotler 1997]. This detail is particularly relevant in the case of Internet users who have more control over the communication and purchase processes. Addressing privacy concerns may be a step in the right direction toward creating good relationships.

2. Privacy and the Internet

The Internet has proven a fertile ground for marketing and advertising and, by extension, has significant implications for privacy. It readily offers all of the tools needed by an organization attempting to fully embrace relationship marketing and possesses unique customer data-gathering capabilities. The Internet serves as a platform for online companies to create favorable relations with consumers. For example, a firm's corporate image may be enhanced without consumers actually knowing much about the company's resources. Furthermore, the Web's technology allows businesses to use it for several purposes such as being an information retrieval source, a sales tool, a distribution channel, and a customer support tool [Peterson, Balasubramanian, and Bronnenberg 1997; Sandberg 1998]. Each of these functions adds value for consumers.

Although similar in some respects, the Internet is different from traditional direct marketing channels in three main ways: 1) increased data creation and collection, 2) globalization of information and communications, and 3) lack of centralized control mechanisms [Berman and Mulligan 1999]. These differences can be used advantageously but at the same time they have the capacity to create problems both for online companies and consumers. An Internet user's every movement is potentially a piece of marketing information. Such information has almost unlimited value as it can be passed from firm to firm and can be matched to numerous databases yielding infinite permutations of consumer profiles [Prabhaker 2000]. These databases may be available only to authorized users or the Web site collecting it may make it available to other companies. For example, Equifax, one of the largest credit bureaus in the U.S., makes the credit records of more than 160 million consumers available to more than 50,000 businesses.

Research has found that a substantial percentage of the population is to some degree concerned about threats to privacy [Petrison and Wang 1995], with threats to privacy stemming from new digital technologies, free markets, and the virtually unlimited exchange of electronic information [Lester 2001]. Public opinion polls indicate that consumers are very concerned about what companies know about them, how companies obtain information, what companies do with the information they collect, and the accuracy of the information they use [Nowak and Phelps 1995]. Consumers appear to be particularly concerned about privacy online [Kehoe, Pitkow, and Morton 1997].

The ethics of privacy is a particularly controversial topic. Miller and Weckert [2000] developed an ethical framework with which to view privacy concerns. Though their study specifically addressed workplace surveillance and monitoring, several of their conclusions may be extended to the arena of electronic commerce. Among other contentions, they propose that individual privacy is a moral right and that people should have the power to exclude and repel attempts to be interfered with. They argue that privacy is a desirable condition with information regarding ownership of personal objects or income to be held in private by an individual. Internet vendors, therefore, should not have the right to gather personal information without an individual's knowledge or consent and sell it to other entities [Stead and Gilbert 2001]. Vendors' arguments of better service for customers through the use of this information may also be questionable, given that many consumers may object to the type of service that these vendors propose [Stead and Gilbert 2001].

A factor likely to exacerbate the online privacy debate is the expected rise in official and unofficial surveillance using so-called "location services" that can pinpoint the whereabouts of mobile technology users. In conjunction

with automated software, similar in nature to the FBI's Carnivore program that can be used to monitor an array of electronic communications, the threat to individual privacy assumes even greater significance.

A lack of rules and effective legislation governing privacy has been one of the major criticisms of the Internet. However, various attempts have been made to regulate online privacy and implement monitoring controls. For example, the American Congress is proposing an Online Privacy Act that would have significant impact on a wide variety of businesses [Savino 2002]. Such efforts, themselves, have not been without controversy. Many companies have protested that such proposed changes will impede market activity ([e.g., Brostoff 2002] and may disadvantage consumers.

Ultimately, online consumers are not employees. They have a moral right to not be monitored by companies. There is no real greater good to be achieved by doing so, as may be the case for monitoring employees whose online behavior can be detrimental to an organization in terms of efficiency, corporate image, and profitability. Companies who choose to violate an individual's right to privacy often use that information simply for profit. At worst, it can even be stolen from them.

Given that online businesses appear to have a moral obligation to take privacy issues seriously, our research is concerned with identifying how these enterprises may benefit from implementing various privacy policies. Recognition of the need for this research comes in the form of increased legislative efforts by governments and other bodies to regulate the use and flow of potentially sensitive information regarding individual consumers. It is important therefore, to outline the scope of privacy and identify just what kind of behavior or actions constitute an impingement upon an individual's privacy.

3. Defining Privacy

Privacy means many things to many people and different things in different contexts. It can be the expectation of anonymity, the expectation of fairness and control over personal information, and the expectation of confidentiality [Berman and Mulligan 1999]. Stone and Stone [1990] characterized privacy as a state or condition in which an individual has the ability to (a) control the release or subsequent dissemination of information about him or herself, (b) regulate the amount and nature of social interaction, and (c) exclude or isolate himself or herself from unwanted auditory or visual stimuli. Culnan [1995] defined privacy as the ability of individuals to control the access others have to personal information about them. Privacy concerns have also been defined as follows:

- The use of personal information freely given by individuals to businesses in the process of making a purchase – "Why do you want that information?"
- The transfer of personal information to third parties – "Where did you get my details from?"
- Access to private information on finances or health – "Business shouldn't have this kind of information" [Prabhaker 2000]

In this study, privacy concerns are limited to the concerns consumers have in regard to companies' possession of personal information. Accordingly, a working definition of privacy adopted for this research is that proposed by Campbell [1997] - the ability of individuals to determine the nature and extent of information about them which is being communicated to others.

4. Aspects of Privacy Concern

This research examines consumer privacy concerns within the framework of the model presented by Smith, Milberg, and Burke [1995]. The authors suggest that consumer information privacy concerns can be divided into two sets of variables: 1) contextual issues relating to the type of information and the organization collecting the data and 2) issues stemming from individual differences between consumers. The focus of this study is on the privacy concerns individuals have with online companies or Web sites, therefore only contextual issues will be considered.

Smith, Milberg, and Burke [1995] categorize contextual privacy issues into five major areas as follows:

- Collection: the perception that too much data are being collected.
- Unauthorized secondary use: personal data collected for one purpose are used for another without permission.
- Errors: personal data are accidentally or deliberately altered, corrupting the integrity of a database.
- Improper access: unauthorized individuals access personal data.
- Invasion: unsolicited and unwanted communications to consumers.

Of these five broad areas of concern, three have been frequently identified in the direct marketing literature as being of primary concern to consumers. They include unauthorized secondary use of data, invasion of privacy, and

errors [Milne, Beckman, and Taubman 1996; Nowak and Phelps 1995; Petrison and Wang 1995]. Given the overt similarities of direct marketing and the marketing of products via the Internet, our study addresses those issues that have been previously demonstrated to concern the consumer the most.

5. Unauthorized Secondary Use of Data

As e-commerce grows, so does the lack of confidentiality. Consumers have little control over how their personal details are used. When consumers shop online, ever-increasing amounts of personal information move about in cyberspace [Carroll 1999]. By merging different databases and employing sophisticated data manipulation techniques, it is possible to develop profiles that reveal an enormous amount of information regarding an individual consumer's personal characteristics, lifestyle, and political and social activities [Nowak and Phelps 1995]. This data can then be sold or exchanged between companies to get comprehensive details of a consumer. According to recent estimates, over 450 companies in the US generate most of their sales revenue by gathering and selling consumer information and data [Nowak and Phelps 1995].

Personal information has become a commodity to be bought, sold and traded. Profitability has become more important than privacy [Gillmor 1998; Kakalik and Wright 1996]. Internet technology has made it very easy to collect such vast amounts of individual information with digital networks now making it possible to link all this information [Prabhaker 2000]. For example, in 1991, the Lotus Development Corporation intended to produce and sell a CD-ROM called Lotus Marketplace: Households. Using data from the Equifax credit bureau, the CD-ROM contained information on the buying patterns and estimated incomes of more than 120 million Americans. A maelstrom of public protest forced the cancellation of this product [Branscomb 1994]. There are many such companies across a range of industries that will sell personal information for profit.

Internet users tend to value confidentiality and may not want to give out personally identifying details. They are more likely to provide data that does not identify them as individuals. To illustrate, one study found that when presented with scenarios involving the provision of personal data to Web sites, respondents were much less willing to provide information when personally identifiable information was requested [Cranor, Reagle, and Ackerman 1999]. The most important factor in this decision was whether or not the information would be shared with other companies and organizations.

Other research has suggested that companies that collect consumer information for their own marketing purposes can immediately build trust with their customers by prominently displaying privacy policies. Conversely, those companies that do not have a policy statement are likely to cause Web users some concern because they do not know how the information will be used [Allen, Kania, and Yaeckel 1998]. It may be that guarantees of confidentiality will encourage consumers to be more prepared to identify themselves and ultimately purchase online.

One notable study found that in order to protect their privacy, significant numbers of people falsify information online [Kehoe, Pitkow, and Morton 1997]. They do this because they seriously value their anonymity. The most common reason for not registering at a site was the lack of statements about how the information will be used. Consumers are not willing to take the risk of providing details to companies that may later on-sell the data. Additionally, the study showed that most users would rather not access a site than reveal personal information. There are numerous sites where a user must register in order to access the site and/or to make a purchase. It might be inferred that consumers who have doubts about a Web site's use of their personal information will prefer not to access that site rather than divulge their personal details. Furthermore, they may be less likely to purchase from these sites. Therefore:

H1: There will be a significant negative relationship between consumers' attitude toward unauthorized use of secondary data and their purchasing of products via the Internet.

6. Invasion

There is growing anecdotal evidence that lack of privacy protection is a major barrier to consumer participation in electronic commerce [Berman and Mulligan 1999; Sheehan and Hoy 1999]. Furthermore, it has been suggested that one of the strongest steps individuals can take as a result of privacy concerns is to restrict or withdraw purchase of goods and services through direct marketing channels [Campbell 1997]. A significant aspect of privacy concern is invasion [Attaran 2000]. It involves contacting consumers who have not requested such contact and is often done repeatedly. Non-transactional privacy concerns such as receiving junk e-mail and unsolicited messages have been identified as of concern to consumers [Korgaonkar and Wolin 1999]. We suggest that consumers who have experienced online invasion of privacy are less inclined to purchase products via the Internet. It is hypothesized that:
H2: There will be a significant negative relationship between consumers' experience of online invasion of privacy and their purchasing of products via the Internet.

7. Errors

Customer data is collected in many different ways, either directly or indirectly. Firms using interactive technologies are well equipped to track down exactly what consumers are doing in cyberspace, including what they stop to look at, what they buy, what they inquire about, and what they read [Nowak and Phelps 1995]. The Internet generates an elaborate trail of data detailing every stop a person makes on the Web. Technologies such as cookies that are written directly onto a hard drive enable Web sites to surreptitiously collect information about online activities and store it for future use [Berman and Mulligan 1999].

Web sites collect considerable personal information both explicitly, through registration pages, survey forms, order forms and on-line contests, and by using software in ways that are less obvious to online consumers [Federal Trade Commission 1999]. Companies can also collate information submitted by users with data automatically transmitted by a user's Web browser and other software to provide a detailed picture of an individual [Foust 2000].

Consumer data collected by online companies has proved extremely valuable because it not only enables merchants to market products and services that are increasingly tailored to their visitors' interests, but also permits companies to boost their revenues by selling advertising space on their Web sites [Federal Trade Commission 1999]. Companies such as Double-click use this detailed transactional information to provide targeted online advertising. Others, such as Adfinity, combine "mouse-droppings" or "click-stream data" with personal information collected from other sources into fully identifiable profiles of the individual's online and off-line behavior [Berman and Mulligan 1999]. In the process of combining these reports, it is likely that inaccurate details will be recorded. This is reflected when consumers receive unsolicited e-mail or advertising material with incorrect information about them or that is clearly irrelevant to their profile. It is therefore hypothesized that:

H3: There will be a significant negative relationship between consumers' experience of inaccuracy or manipulation of personal data and their purchasing of products via the Internet.

8. Methodology

8.1 Questionnaire Development

The questionnaire used for data collection consisted of a combination of multivariate and univariate measurement instruments as well as measures of key demographic factors. The dependent variable, prior purchase, was measured using a single-item measure indicating how many times a consumer had made a product purchase and full payment completely via the Internet.

The scale used to measure unauthorized secondary use of data was replicated from Moorman, Deshpande, and Zaltman (1993). They developed the scale to measure factors affecting confidentiality in market research. The scale was slightly modified to reflect confidentiality of personal information collected via the Internet. A Cronbach's alpha of 0.89 was recorded, which suggests a reliable scale for use in this study.

Invasion of privacy was measured using a three-item scale developed by Korgaonkar and Wolin (1999). They used the scale to measure non-transactional privacy concerns of online users. Cronbach's alpha for this scale was reported as 0.76, indicating the reliability of the measure.

These summated scales were chosen as they were deemed the most suitable for this study after a check for face validity. They have also been shown to be reliable in previous studies. To operationalize errors in recorded data, we measured whether consumers had experienced a situation where their details have been altered using a nominal univariate item.

Table 1: Selected Items From Questionnaire Representing Constructs of Unauthorized Secondary Use, Invasion of Privacy, Errors, and Prior Purchase.

1.	I detest the fact that the web is becoming a haven for electronic junk mail.
2.	My personal details are safe with online companies.
3.	I wish I had more control over unwanted messages sent by businesses on the web.
4.	I dislike the fact that marketers are able to find out personal information about online shoppers.
5.	I believe the information I share with online companies will not be shared with other companies.
6.	Online companies will keep confidential what they learn about me from my activities on their site.
7.	How often have companies you have dealt with over the Internet passed on your personal details to a third party?
8.	How often have your personal details been incorrectly altered or modified in some way without your approval by companies you have dealt with over the Internet?
9.	How many times have you actually purchased something via the Internet and made full payment online?

8.2 Sampling and Analysis

Data were collected by survey questionnaire using a convenience sample of two hundred and ten undergraduate and postgraduate students at an Australian east coast university. Though the sample is relatively homogenous in terms of demographics and lifestyles, thereby enhancing internal validity, it may also have reduced the external validity of the research. However, such a convenience sample was deemed appropriate because the purpose of the study was not to provide point and interval estimates of the variables but to test the relationships among them. They are therefore considered adequate for this purpose [Calder, Phillips, and Tybout 1981]. Furthermore, the relative youth of the sample is not inappropriate as Internet usage is prevalent among younger consumers, with as many as forty percent of all Internet users falling within the 18-34 age category [CyberAtlas 2001]. Of the total number of questionnaires given out, one hundred and ninety six were received. Of this, one hundred and eighty six questionnaires were usable. This represented a response rate of 88.6%.

Hypotheses 1, 2, and 3 were tested using a three-way analysis of variance (ANOVA). Independent variables were unauthorized use of secondary data, invasion of privacy, and errors. Prior purchase frequency was treated as the dependent variable.

8.3 Results

Of the 186 useable responses, ninety-one respondents were male and ninety-five were female. This is an almost equal distribution indicating no gender bias. Both summated scales for attitudes toward invasion of privacy and unauthorized secondary use of data demonstrated Cronbach's alpha measures of 0.6, which is considered an acceptable level for social research [Malhotra, Hall, Shaw, and Crisp 1996].

Hypothesis 1 proposed that there will be a significant negative relationship between consumers' attitude toward unauthorized use of secondary data and their purchase of products via the Internet. The summated mean for the scale was 3.73 (1=Strongly Disagree; 7=Strongly Agree). Analysis of variance was used to determine whether the relationship was significant, the results of which are displayed at Table 2. No significant relationship was found and Hypothesis 1 is therefore rejected (F=2.318; df 1,185; p > .05).

Hypothesis 2 suggested that there will be a significant negative relationship between consumers' attitude toward online invasion of privacy and their purchasing of products via the Internet. The summated mean of the invasion of privacy scale was found to be 5.48 (on a seven-point scale). This suggests that consumers generally have a high concern over being contacted by companies online without prior permission. ANOVA results demonstrated a significant relationship between invasion of privacy and online purchase frequency (F=8.706; df 1,185; p < .05).

Hypothesis 3 claimed that Internet users who have had prior experience online, where personal data has been accidentally or deliberately altered are less prone to purchase products online. The extent to which consumers had experienced this altering of details was measured using a single, univariate item. A significant relationship between altering personal details and online purchase was found (F=2.420; df 5,181; p < .05). Hypothesis 3 is therefore accepted. No significant interactions were found between the independent variables.

Table 2. Three-Way Analysis of Variance to Examine Main Effects of Invasion of Privacy, Unauthorized Use of Secondary Data, and Errors on Prior Purchase.

Effect	**Type III Sum of Squares**	***df***	**Mean Square**	***F***	**p**
Main Effect					
1. Errors	17.36	5,181	3.47	2.42	0.04
2. Unauthorized Use of Data	3.32	1,185	3.32	2.32	0.13
3. Invasion of Privacy	12.49	1,185	12.49	8.71	0.00
Interactions					
1 x 2	3.36	3,183	1.12	0.78	0.51
1 x 3	4.19	3,183	1.40	0.97	0.41
2 x 3	2.29	1,185	2.29	1.59	0.21
1 x 2 x 3	0.71	3,183	0.24	0.16	0.92
Corrected Model	43.05	17	2.53	1.77	0.04

n=186

R Squared = .165 (Adjusted R Squared = .071)

9. Discussion and Managerial Implications

Researchers have examined unauthorized secondary use of data in direct marketing studies but few, if any, have analyzed it in the context of the Internet. The literature suggests that confidentiality is one of the privacy concerns consumers regard highly. For instance, it is claimed that consumers are concerned when their personal and financial information records are sold to other companies [Wang and Petrison 1993].

In this study, however, unauthorized secondary use of data was found to not have a significant impact on individuals' online purchase behavior. The mean of 3.7 for participant responses indicated an overall lack of strong feeling in either direction for this variable. Clearly, many consumers are concerned by this aspect of Internet usage, although it appears that the concern is not so great as to deter people from actually making a purchase via the medium. One explanation for this outcome might be the age of the sample. Various studies [e.g. Campbell 1997; Milne et al. 1996] have found that age is an important factor in analyzing privacy concerns since younger age groups tend to have lower privacy concerns than older age groups. Another explanation might be that consumers are already used to this phenomenon to some extent in traditional marketing channels, including direct mail. Mailing lists are frequently made available to third parties without consumers being aware of precisely who has their details. It may be just an accepted (although perhaps disagreeable) way of doing business.

The implication for online product providers is that guarantees of confidentiality (i.e. not passing on customers' details) may not have any influence on consumers' product acquisition decisions. Furthermore, it may be that additional revenue streams could be unlocked by the sale of such data to interested parties, without any negative effect on conventional sales. Certainly, caution must be applied in interpreting these results as some customer segments are likely to be more sensitive to unauthorized secondary use of data than others. Further research should be conducted in this area to identify which consumers and/or product categories are most sensitive to the resale of customers' personal data.

Invasion of privacy is an important issue in direct marketing and has been shown to affect consumers' purchase behavior. When confronted with invasion of privacy concerns, consumers have been shown to restrict their purchase of goods through direct marketing channels [Berman and Mulligan 1999; Campbell 1997; Mand 1998]. The findings of this study are consistent with others from the direct marketing literature. It appears that consumers who receive unwanted and unsolicited communications from companies via the Internet are less likely to purchase products online.

The managerial implications for firms engaged in e-retailing are clear. If a company wishes to sell its products online, then communication channels should be selected carefully. Spam e-mail is unlikely to be very effective and unless contact can be established through “legitimate” and relevant means, consumers are likely to disregard any prompting to purchase. They may even develop hostility toward the firm thereby limiting the possibility of continuing dialog or creating mutually beneficial relationships. The concept of “permission marketing” certainly appears to be supported by the current research.

Hypothesis 3 proposed that Internet users who have had prior experience online, where personal data was accidentally or deliberately altered demonstrate lower levels of online purchase. The hypothesis was accepted and supports previous research suggesting that consumers are concerned about what companies do with the information they collect and the accuracy of the information they use [Nowak and Phelps 1995]. Managers should focus efforts on accurately recording and storing data that is relevant to consumers. An example of a transgression that might offend consumers is a simple e-mail sent out to a prospect or customer with the wrong name on it.

Despite their stated concern for individual privacy, online consumers are in many cases very quick to provide significant amounts of personal information, if given an incentive. A free T-shirt or entry into a promotional contest is often all it takes to get many Web users to part with personal details [Tweney 1998]. Customers may be willing to furnish such information if they feel the reward justifies that loss of privacy. For example, E-Trade was effective in gaining customer information by offering 500 free air miles in exchange. After receiving the information, the customer received a certificate good for the first $50 investment [McKim 1999].

However, the way in which personal data is handled appears to be critical. Although passing information on to third parties does not seem to influence purchase behavior, contacting consumers without permission and maintaining inaccurate records does. It is clearly important for companies or Web sites to treat consumer privacy concerns seriously if they want to encourage customer loyalty and increase sales. Most commercial research suggests that it is still a minority of Internet users who go beyond merely browsing for information to actually purchasing goods and services online. The decision appears to be influenced to some degree by their privacy concerns, in addition to other factors. It is evident therefore, that before consumers become more accepting of the erosion of their privacy they will have to be convinced that the result provides some real benefit to them [Petrison and Wang 1995].

10. Limitations and Future Research

One limitation of the study lies in the use of a student sample. However, given that young people have been shown to have lesser privacy concerns than older people [Campbell 1997; Milne et al. 1996], and the fact that two of the three hypotheses were supported, it is suggested that the results might be tentatively applied to a wider population. Furthermore, as an exploratory study, the major purpose was to establish if there were any significant relationships between the privacy constructs and online purchase behavior. Use of a random representative sample may nevertheless provide different results and is an option for future research.

Another limitation lies in the measurement of attitudes toward online privacy in general. Consumers may behave differently when making purchase decisions concerning specific Web sites or product categories. Future research may focus how consumers respond to a specific Web site in the light of privacy concerns. However, we were of the view that research that is too specific may suffer from the inapplicability of results to a wider range of circumstances.

REFERENCES

Allen, C., Kania, D. and Yaeckel, B., *Internet World: Guide to One -to -One Web Marketing,* Wiley, New York, 1998.

Attaran, M., "Managing Legal Liability of the Net: a Ten Step Guide for IT Managers", *Information Management and Computer Security*, Vol.8, Issue 2, 2000.

Berman, J. & Mulligan, D., "Privacy in the Digital Age: Work in Progress", *Nova Law Review*, Vol. 23, No. 2, 1999.

Branscomb, A.W., *Who Owns Information?* Basic Books, New York, 1994.

Brostoff, S., "Insurers Oppose Net Privacy Bill", *National Underwriter*, Vol. 106, No. 9:3, 2002.

Calder, B.J., Phillips, L.W. and Tybout, A.M., "Designing Research for Application", *Journal of Consumer Research*, Vol. 8 No. 2:197-207, 1981.

Campbell, A., "Relationship Marketing in Consumer Markets: A Comparison of Managerial and Consumer Attitudes About Information Privacy", *Journal of Direct Marketing,* Vol. 11, No. 8:44-57, 1997.

Carroll, K., " E-Commerce Success May Depend On Online Privacy", *Telephony,* Vol. 237, No. 17: 46-48, 1999.

Cranor, L.F., Reagle, J., and Ackerman, M.S., "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy", *AT&T Labs-Research Technical Report TR 99.4.3*, 14th April, Available at http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm, 1999.

Culnan, M., "Consumer Awareness of Name Removal Procedures: Implications for Direct Marketing," *Journal of Direct Marketing*, Vol. 9, No. 2: 12-18, 1995.

CyberAtlas, *Demographics: Asians Among Most Wired Americans*, December 18, Available at http://cyberatlas.internet.com/big_picture/demographics/article/0,,5901_942621,00.html#table2, 2001.

Federal Trade Commission,"Privacy Policies On-line: Improving for Consumers", *Consumers Research Magazine*, Vol. 82, No. 10: 26-30, 1999.

Foust, J., "Protecting Your Privacy Online", *Technology Review*, Vol. 103, No. 2: 30-31, 2000.

Geyskens, I., "Generalizations about Trust in Marketing Channel Relationships using Meta-Analysis", *International Journal of Research in Marketing*, Vol. 15, No. 3: 223-48, 1998.

Gillmor, D., "Violating Privacy is Bad Business", *Computerworld,* Vol. 32, No. 12: 38-9, 1998.

Gordon, Ian, *Relationship Marketing: New Strategies, Techniques and Technologies to Win the Customers You Want and Keep Them Forever*, John Wiley and Sons, Toronto, 1998.

Kakalik, J. and Wright, M., "Responding to Privacy Concerns of Consumers", *Review of Business*, Vol.18, No. 1: 15-18, 1996.

Kehoe, C., Pitkow, J. and Morton, K., *Eighth WWW User Survey*, Available at http://www.cc.ptech. edu/gvu/user_surveys/survey-1997-10, 1997.

Khalil, O. M. and Harcar, T. D., "Relationship Marketing and Data Quality Management", *SAM Advanced Management Journal*, Vol. 64, No. 2: 26-33, 1999.

Korgaonkar, P and Wolin, L., "A Multivariate Analysis of Web Usage", *Journal of* A*dvertising Research*, Vol. 39, No. 2: 53-70, 1999.

Kotler, P., *Marketing Management: Analysis, Planning, Implementation and Control,* 9th edition, Prentice - Hall, New Jersey, 1997.

Lester, T., "The Reinvention of Privacy", *The Atlantic Monthly*, March, pp. 27-39, 2001.

Malhotra, N. K., Hall, J., Shaw, M. and Crisp, M., *Marketing Research: An Applied Approac*h, Prentice-

Hall, Sydney, 1996.
Mand, A., "Portals Plug Privacy Push", *Mediaweek*, Vol. 8, No. 38: 58, 1998.
McKim, R., "Information: the Newest Currency", *Target Marketing*, Vol. 22, No. 7: 36-7, 1999.
Miller, Seumas and Weckert, John, "Privacy, the Workplace, and the Internet", *Journal of Business Ethics*, Vol. 28, No. 3: 255-265, 2000.
Milne, G. R., Beckman, J. and Taubman, M. L., "Consumer Attitudes Towards Privacy and Direct Marketing in Argentina", *Journal of Direct Marketing,* Vol. 10, No. 1: 22-29, 1996.
Moorman, C., Deshpande, R. and Zaltman, G., "Factors Affecting Trust in Market Research Relationships", *Journal of Marketing*, Vol. 57, No. 1: 81-101, 1993.
Nicovich, S. and Cornwell, T. B., "An Internet Culture?: Implications for Marketing", *Journal of Interactive Marketing*, Vol.12, No. 4: 22-33, 1998.
Nowak, G. and Phelps, J., "Understanding Privacy Concerns: An Assessment of Consumer Information – Related Knowledge and Beliefs", *Journal of Direct Marketing,* Vol. 6, No. 4: 28-39, 1992.
Peterson, R.A., Balasubramanian, S. and Bronnenberg, B.J., "Exploring the Implications of the Internet for Consumer Marketing", *Journal of the Academy of Marketing Science*, Vol. 25, No. 4: 329-46, 1997.
Petrison, L.A. and Wang, P., "Exploring the Dimensions of Consumer Privacy: An Analysis of Coverage in British and American Media" *Journal of Direct Marketing,* Vol. 9, No. 4: 19-37, 1993.
Prabhaker, P. R., "Who Owns the Online Consumer?", *Journal of Consumer Marketing,* Vol. 25, No 4: 329-346, 2000.
Sandberg, J., "It Isn't Entertainment that Makes the Web Shine, It's Dull Data", *Wall Street Journal*, July 20, 1998.
Savino, William M., "Protecting Online Privacy", *Marketing Management*, Vol. 11, No. 5: 49-51, 2002.
Sheehan, K.B. and Hoy, M..G., "Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns", *Journal of Advertising,* Vol. 28, No. 3: 37-61, 1999.
Smith J, Milberg, S. and Burke, S., "Information Privacy and Marketing Practices: The Role of Consumer Concerns." Unpublished working paper, 1995.
Stead, Bett Ann and Gilbert, Jackie, "Ethical Issues in Electronic Commerce", *Journal of Business Ethics*, Vol. 34, No. 2: 75-85, 2001.
Stone, E. F. and Stone, D. L., "Privacy in Organization: Theoretical Issues, Research Findings and Protection Mechanisms", in *Research in Personnel and Human Resources Management*, Vol. 8: 349-411, 1990.
Tweney, D., "The Consumer Battle over Online Information Privacy Has Just Begun", *InfoWorld,* Vol. 20, No. 25: 66, 1998.
Wang, P. and Petrison, L., "Direct Marketing Activities and Personal Privacy: A Consumer Survey", *Journal of Direct Marketing,* Vol. 7, No. 1: 7-19, 1993.