INFORMATION PRIVACY CONCERNS IN THE CONTEXT OF ELECTRONIC COMMERCE: A STUDY TO MEASURE SENSITIVITY LEVELS OF DIFFERENT TYPES OF PERSONAL INFORMATION AND THE WILLINGNESS OF INTERNET USERS TO SUBMIT PERSONAL INFORMATION

by

SHIUH YONG KONG

B.Sc., University of Minnesota, 1999

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE (BUSINESS ADMINISTRATION)

in

THE FACULTY OF GRADUATE STUDIES

(Management Information Systems Division; Faculty of Commerce and Business Administration)

We accept this thesis as conforming
to the required standard

THE UNIVERSITY OF BRITISH COLUMBIA

August 2001

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at the University of British Columbia, I agree that the Library shall make it freely available for reference and study. I further agree that permission for extensive copying of this thesis for scholarly purposes may be granted by the head of my department or by his or her representatives. It is understood that copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Department of Management Information Systems

The University of British Columbia
Vancouver, Canada

Date August 31st, 2001

ABSTRACT

The purpose of this thesis is to examine one of the information privacy dimensions from the Internet consumers' perspective. Specifically, the goal of this research is to identify the levels of sensitivity of six types of personal information that Internet users are asked to submit to web sites. This research intends to develop a hierarchy of the sensitivity levels based on the results of the study. In addition, this study investigates the willingness of the Internet users to provide their personal information before and after the benefits of submitting the personal information are revealed. In this thesis, the study involved both qualitative and quantitative methodologies. The qualitative methodology involved literature review to identify the scope and content of the research. In the quantitative research, a comprehensive survey targeting the students, faculty, and staff at the University of British Columbia was conducted to answer the research questions. Results of the survey of 108 subjects confirm one of this thesis's hypotheses in which different types of information exhibit contrasting levels of sensitivity. Another important finding from the outcomes of the survey suggests that benefits alone do not induce Internet users to relinquish their personal information in general. Implications of this study and future research directions were summarized at the end.

Keywords: Information Privacy, Privacy, Literature Review, Empirical Study, Survey.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ACKNOWLEDGMENTS

I would like to express my enormous amount of gratitude to Dr. Izak Benbasat for his significant assistance and support in this research. In addition, I would also like to thank Dr. Sandra Robinson for her constructive advice on the survey assessment and methodology and Dr. Richard Rosenberg for his commitment in the thesis committee. Finally, I would like to extend my appreciation to those graduate students at the University of British Columbia for their participation in the pilot studies. And special thanks also goes to Marko Niffka.

With grateful love,
to my mom and dad.

1. OVERVIEW AND SUMMARY

1.1 OVERVIEW

As we shift into a digital information age, the magnitude of information privacy cannot be viewed frivolously. Inability to notice and safeguard the sacred concept of information privacy on the Internet would impede digital information flow and, eventually, lead the Internet economy to hit a new nadir. Unquestionably, information privacy remains as one of the essential issues that we ought to tackle these days.

In order to accomplish the task, this thesis attempts to provide an understanding of one underlying dimension of information privacy concerns. This study looks at the finer characteristics of different types of personal information from the Internet consumers' point of views in the context of electronic commerce. The thesis is organized as follow: Chapter 1 precedes by offering an overview and introduction to the issue of information privacy. Chapter 2 contains an in depth discussion and literature review of scholarly works in the field of information privacy. Chapter 3 proceeds to discuss the study involved to answer the research questions embedded in this thesis. Chapter 4 analyzes the results obtained from the research and finally, Chapter 5 deliberates upon the results attained and concludes with summary and research contributions.

1.2 INTRODUCTION

The number of users participating in business to consumer electronic commerce has been increasing rapidly. This is evidently illustrated by the expanding and significant use of technologies such as electronic mail and the World Wide Web. For instance, Forrester

Research states in a report that by the year 2004, more than 49 million U.S. households will spend US$184 billion online. In addition, the recent eGlobal Report proclaims that there are 130.6 million of active Internet users in the world today. The report further states that the number of Internet users will continue to soar up to 350 million by the year 2003, an astonishing 267% increase from the year 1998 (Profunda Software APS, July 2000).

Nevertheless, it has become clear that the privacy issues associated with the use of these new information technologies and applications have not been properly resolved and addressed. Evidently, a recent news on the Cable News Network heightened the problem in which the U.S. government claims that an eminent Web toy retailer deceptively sold customer data (CNNfn, July 10, 2000). Also, according to a Business Week/Harris Poll survey result in 1998, it is reported that a staggering ninety one percent of the American public do not trust or somewhat trust the privacy policies posted by Web site operators. In addition, the survey contends that the top reason people move away from the Web is increased worries about protecting their personal information online (Louis Harris & Associates and Westin, March 1998). Cognizant of the privacy issues today, Business Week also published an Internet privacy cover story in its March 20, 2000 edition. In the issue, it is stated that ninety four percent of the people surveyed express high concern or some concern with the idea of a company using personal information to send unwanted information (Green, et al., 2000). Disturbingly, in its recent cover issue, Time scrutinizes nine dire techniques of collecting and tracking users' movements online and advocates numerous approaches Internet users can embrace to guard themselves (Cohen, 2001).

As a result, the issue of privacy is becoming even more important than before and will become more critical as business to consumer electronic commerce continues to unfold. In view of that, Canada and Europe have moved toward legislative regulations by introducing Bill C-6 and the European Data Protection Directive respectively (Rosenberg, May 16, 2000). The United States of America has recently turned its attention to legislative means after recognizing continuous ineffectiveness in self-regulation among the Web businesses (Kleinbard, March 6, 2000). Nonetheless, one remains skeptical as to whether or not government regulation is the ultimate solution to privacy issues.

On the other hand, many argue that the origin of privacy problems emanates from consumers, not businesses. Generally, Internet users have little or no knowledge or control about their personal information. For example, Internet users do not know what information is being collected and used. Some even depict these consumers as ignorant and careless (Cranor, June/July 1998). To illustrate, Cyber Dialogue reports that forty two percent of cybercitizens have never heard of cookies or do not understand how cookies work (Mabley, 2000). As a result, when Internet users discovered that companies are silently collecting their personal information using the cookies, they began to exacerbate the privacy issue.

Another survey by Arthur Andersen strengthens the above point. The survey reports that Internet users are very concerned about information privacy, yet seventy four percent

contend that they are willing to disclose their Social Security Number in exchange for discounts or free shipping (Kuchinskas, September 12, 2000). Essentially, this implies that there is no co-exist or little understanding between Internet users and Web businesses. Consequently, conflicts of interest arise. The discussion above apparently suggests that there is a grave needs to establish 'two-linked' communication between Internet users and businesses. As a recent article in Business Week puts it best: Internet users have the right to define what privacy rules are and how to enforce them (Business Week, March 20, 2000).

1.3 RESEARCH PERSPECTIVES

RESEARCH MOTIVATION

The above elaboration epitomizes the vital essence of privacy problems. Apparently, there is no trust between governments, consumers, and businesses. Governments and consumers persistently accuse businesses of using digital personal information to generate exorbitant profits. In contrast, businesses claim that consumers are ignorant and do not understand the genuine realm of electronic commerce. These businesses insist that governments' intervention in privacy issues would inflict profound gaffe to the economics of electronic commerce (CNN, March 2, 2001).

The businesses' edict is reasonably explicable. Internet users may not be conveniently having access to sophisticated products or services offered by web sites if austere laws are introduced to tackle privacy issues. Businesses may be compelled to reduce or slash services, which might not be in the best interest of Internet consumers.

Studies or research of information privacy concerns in the context of electronic commerce have received little attention to this day. More specifically, very few research has been conducted to understand the needs of the Internet consumers as well as the needs of digital businesses. Most journals focus on the pros and cons of the adoption of privacy law. And many studies on Internet privacy have been diverted to the field of developing technical solutions such as the Platform for Privacy Preferences (P3P).

Therefore, this study tries to understand one dimension of the Internet privacy issue from the consumers' perspective. It would be impractical for this lone study to investigate all dimensions of the Internet privacy concern.

RESEARCH QUESTIONS

The goal of this research is to identify the levels of sensitivity of different types of personal information that Internet users are asked to submit to the web sites. In addition, this research intends to develop a hierarchy of the sensitivity levels based on the results of the study. Furthermore, this study investigates the willingness of the Internet users to provide their personal information before and after the benefits of submitting them are revealed. This research is designed to answer the following questions:

1) **Is there a relationship between the types of information requested and the information privacy concerns? If there is a relationship, what are the relationships?**

2) **Does knowing the benefits of submitting certain types of personal information affect or alter the willingness of the Internet users to offer different types of personal information?**

These research questions are depicted by Figure 1 and Figure 2 respectively.

1.4 RESEARCH METHODOLOGY

LITERATURE RESEARCH

The research was divided into three phases. First, a thorough literature review of appropriate publications and scholarly work was used to identify the scope and content of this study. The first body of literature is used as the primary foundation. Throughout this qualitative method, the study attempts to examine the general history and roots of the right of privacy. In addition, previous research on information privacy were scrutinized in order to seek a preliminary understanding of information privacy concerns in this digital age. The second body of the literature review aims to build the theoretical foundation and hypotheses of this thesis.

QUANTITATIVE RESEARCH

The second phase started out with three pilot studies in order to test and validate the modified survey instrument. This survey instrument was used in the third and final phase in which a comprehensive survey targeting students and faculty/staff at the University of British Columbia was conducted. Statistical analyses were performed to examine the relationship between different types of personal information and information privacy concerns. Additionally, the analyses were also used to determine any statistical

significance in the subjects' willingness of submitting different types of personal information before and after the benefits were revealed. Finally, results and findings were summarized.

2. LITERATURE REVIEW

2.1 PRIVACY HISTORY AND BACKGROUND

A brief review of literature on the issue of privacy has seemingly indicated that the privacy enigma can be traced back into the 1800s. In 1890, Professor Louis D. Brandeis and Samuel D. Warren published "The Right to Privacy" in the Harvard Law Review (Culnan, 1993). In the historic article, Brandeis and Warren stipulated that individuals have "the right to be left alone." The landmark article represented the initial attempt to lay out an articulated legal theory of definition and limitations of a "right to privacy." According to Brandeis and Warren, each individual is entitled by common law to "the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Brandeis and Warren, 1890).

Then, in 1960, William D. Prosser published "Privacy (A Legal Analysis)" in the California Law Review. The article strengthened Brandeis and Warren's theory with a more complex analysis of his "four distinct torts" that define the right to privacy: disclosure, intrusion, false light, and appropriation (Bier, 1980). Unlike Brandeis and Warren, Prosser claims that privacy "comprises four distinct kinds of invasion of four different interests of the plaintiff." Prosser's torts included: public disclosure of embarrassing private facts about the individual; intrusion upon the individual's seclusion

or solitude, or into his private affairs; publicity that places the individual in a false light in the public eye; and appropriation, for another person's advantage, of the individual's name or likeness. These four distinct torts apparently suggest that the issue of privacy is more complex than the initial lone theory developed by Brandeis and Warren (Bier, 1980). Clearly, the works by Brandeis, Warren, and Prosser greatly contributed and shaped the recognition of the right to privacy today.

However, these days, telecommunication and information technologies have been evolving so rapidly that the law cannot keep pace with all the new ramifications. For instance, Laudon notes that current legal framework for protecting privacy will be obsolete in the future as we advance into highly evolved technological environment (Laudon, 1996). Nevertheless, current privacy advocates continue to urge the government to regulate the Internet market. Yet, the regulation method creates disputes among all the parties involved. To illustrate, in his article, Rosenberg describes how the European Data Protection Directive will indirectly influence the North American economy. Due to this fact, North American politicians are concerned about the future of electronic commerce in the United States and Canada (Rosenberg, 1998). For instance, the U.S. Congress was recently enraged by the European Union's decision to impose austere standards by blacklisting companies from other countries that do not have strong privacy laws (CNN, March 9, 2001).

Although Canada has moved toward implementing the Bill C-6 law, the United States is still in its infancy stage to legislate the Internet market. Initially, the Bill C-6 Law

imposes privacy standards on federally regulated organizations. However, it is well noted that the private sectors will adhere with the Bill in the near future. Under the Bill, it will be obligatory to receive the consents of individuals before utilizing the personal information in commercial activities. Therefore, the enactment of the Bill C-6 law will have enormous implications for businesses throughout Canada (Industry Canada's e-commerce web site).

In its latest yearly online privacy report[1], the Federal Trade Commission recommends that legislation is needed in the United States after discovering only twenty percent of the busiest commercial web sites implement all four fair information practice principles, which were initially proposed in 1998 (Federal Trade Commission, May 22, 2000). These four core principles of privacy, as a guideline for self-regulation in the industry, are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security (Federal Trade Commission, 1999). These four core principles are explained in Table 1.

In spite of these efforts to legislate the Internet market place, some believe that the ability to regulate the privacy issue is not enough. Laudon notes that the legal literature itself is highly critical of the current existing approach to protect privacy (Laudon, 1996). For instance, the pro-self regulation folks argue that the ability to capture the breakers of privacy law is very limited (Wang, et al., 1998). This is due to the fact that the Internet is a boundless world. In addition, there are thousands or millions of private computerized communications that travel across multi-national networks. Thus, the capability to

[1] A copy of the report can be obtained from FTC's web site (www.ftc.gov/privacy).

handle and scrutinize this information is arduous. Furthermore, privacy laws are convoluted issues. Laws applicable in one country do not necessarily apply to other countries as well. Such law protection may have little effect on the Internet where all governments are having trouble in implementing a regulatory environment where it is often ambiguous in which country and under what jurisdiction an Internet transaction takes place. Westin (1967) has proposed that countries are different in their view of information privacy concerns. This proposition has been tested and supported empirically by Milberg, et al. (1995).

The above discussion apparently suggests that the law has experienced both conceptual and practical difficulties in applying legal rules to the Internet. Prominent legal scholars, such as Gavison, are skeptical, as they believe law is limited in guaranteeing privacy. Gavison (1980) contends that there is a feeling of lack of privacy even though laws such as The Privacy Acts of 1974 and The Supreme Court declaration on privacy are in place in the U.S. Laudon (1996) further strengthens this proposition by arguing in his study the vulnerability and limitations of current privacy laws in the U.S. to preserve consumer privacy. In another key literature, Morrison and his colleague (2000) examine the role of trust for electronic commerce and point out that privacy laws as punishment could contribute to systems failure.

Accordingly, privacy educators have been proposing several alternatives to resolve the problem. Kevin Mabley, director of research at the Cyber Dialogue, believes that the solution for the privacy issue lies between consumer education and industry self-

regulation. Mabley (2000) further asserts that the company position "is that a *consumer-centric* approach (one that makes it easier for consumers to find what they are looking for rather than simply making it easier for marketers to sell products) is the sine qua non to maintaining self-regulation in our industries." Additionally, in their article, Straub and Collins (1990) share the same view in which they insist that the privacy of an individual "can be best protected through self-regulating policies and procedures."

In addition, Laudon (1996) proposes a national information market as an alternative in his study. The basic idea behind this national information market is to let individuals to control and decide how their personal information will be used. Moreover, the personal information can be bought and sold in the market in which the profits proceed directly to the consumers' pocket. Laudon equates the scheme of this alternative to that of a financial industry such as banks (Laudon, 1996).

Also, technological solutions have been hammered lately as conceivable resolutions to the privacy issue. For instance, the World Wide Web Consortium (W3C) will soon release The Platform for Privacy Preferences (P3P) to the public. Fundamentally, the P3P behaves like a middleperson between the Internet users and the Web sites. P3P's primary function is to understand and simplify the privacy policy posted on the Web sites. Specifically, P3P compares as well as expresses web sites' practices to the Internet users. Therefore, Internet users can opt to continue or halt their participation on the web sites (Cranor, 1998).

Likewise, Ackerman and Cranor (1999) propose an artificial intelligence system called "Privacy Critics" that can assist consumers. Resembling the P3P, Privacy Critics provides feedback and suggestions to Internet users. The system observes the information and alerts the users of possible problems based on the data obtained from a database such as the CyberPrivacy Advocacy Group's database (Ackerman, 2000). However, privacy advocates have been highly critical of the idea behind these technological solutions. Operationally, technology has to be in place, though it is not much of a yardstick.

Yet, the protection of information privacy issues is beyond all this fancy software as security is not synonymous with privacy. Likewise, legal protection does not promise that the Internet is unhindered from information privacy crime. A recent Cyber Dialogue Online Privacy Survey reports that consumers are actually willing to share their personal information but not without giving consent (Mabley, 2000). However, very little research has been done to investigate and identify individuals' perceptions and needs of information privacy, although numerous surveys or polls have been conducted. These surveys tend to uncover ordinary concerns and display general statistics of the Internet users, though one can interpret (under assumptions) the sketchy figures to analyze Internet users' perceptions of information privacy concerns (Louis Harris and Associates, Inc., 1990; 1992; Westin, 1998).

2.2 PREVIOUS SCHOLARLY RESEARCH ON INFORMATION PRIVACY

Lately, research on the issue of information privacy has been emerging continuously in the IS field and literature. The following are some prior research papers that attacked this consumer issue from the electronic commerce perspective. These studies mentioned below gravitate toward exploring different dimensions of consumers' privacy concerns.

In her study, Culnan investigated the secondary use of personal information toward certain direct marketing practices (Culnan, 1993). Culnan concluded that consumers will have a more positive attitude toward mail shopping[2], develop better strategies to deal with unwanted mails, and have a lower concern for privacy (measured as loss of control) if they are less sensitive about secondary uses of personal information (Culnan, 1993). The study apparently suggests that organizations should avoid handling information for secondary use, albeit secondary information use is legal. In this case, secondary information use can be deemed as an invasion of privacy from the consumers' point of view (Culnan, 1993).

On the other hand, the work, by Milberg, et al., looks at the relationship between values, nationality, privacy concerns, and regulatory approaches (Milberg, et al., 1995). The study attempts to understand if national differences in privacy concerns must be weighed in order to develop IS applications in an organization. Their paper shows that international organizations ought to take national differences into account by developing privacy solutions specific for each of the countries involved (Milberg, et al., 1995). Apparently, this study also demonstrates that information privacy concern varies across

[2] Mail shopping includes direct mail, phone, and catalog.

countries, nationalities, and regulatory policy approaches. For example, in the study, countries with "no regulation" exhibit a lower level of information privacy concerns than that of "moderate regulated" countries (Milberg, et al., 1995).

In addition to this research, Wang, et al. (1998) summarize a taxonomy for consumer privacy concerns from the Internet marketing standpoint in their article[3], which can be used to explain, classify, and analyze the information privacy concerns that occur commonly in the electronic marketplace. For example, according to Table 3, the Internet marketing activity, preference tracking, usually causes consumer privacy concerns such as improper access, improper collection, and improper monitoring. In addition to the taxonomy, Wang, et al. (1998) explains the relationships between privacy enhancing technologies and information privacy concerns. The relationships can be utilized to assess the effectiveness of different types of information privacy protection available to counteract the privacy issues[4] (Wang, et al., 1998).

Another research, by Culnan and Armstrong (1997), explores one of the conditions under which Internet consumers are willing to disclose their personal information. Culnan and Armstrong argue that consumers are more willing to disclose their personal information if the consumers know that there are fair procedures to protect individual privacy in the organization (Culnan and Armstrong, 1997). These fair procedures are consistent with the Federal Trade Commission's Four Fair Information Practice Principles.[5] Specifically, Culnan and Armstrong (1997) have empirically verified that privacy concerns do not

[3] Refer to Table 2 for the taxonomy
[4] Refer to Table 3 for the relationships.
[5] See Table 1

differentiate customers who are willing to be profiled from those who are unwilling to have their personal information used this way if customers are told that fair information practices are deployed in the organization (Culnan and Armstrong, 1997). The study concludes that businesses will gain more advantages by observing the fair procedures to protect individual information privacy (Culnan and Armstrong, 1997).

In developing a model of consumers' perceptions of the invasion of information privacy, Stewart and her colleagues (2001) posit that concern and attitude toward information privacy concerns and practice are influenced by several attributes, namely constructs of self-esteem, consumer alienation, and computer anxiety. They further examine and refine the model to describe the reasons why consumers respond positively or negatively to the organizations' use of their personal information. The model is confirmed and validated by their research and their key findings suggest that Internet users deemed organizations, as opposed to information technology, responsible for the use of personal information (Stewart, et al., 2001)

The discussion above apparently illustrates that information privacy is an extensive and growing field. Organizations attempting to extract digital information from web sites these days need to refine their understanding of the needs and concerns of Internet users. While research is under way to assist these organizations, many more of the complex factors from the Internet users' perspective in regard to privacy issue are still unexplored. Accordingly, this study is designed to explain one of the many complex factors, which is the sensitivity level of different types of personal information. The study hopes to

identify information to aid Internet organizations to gain better awareness and responsibility in extracting and handling different types of personal information.

3. RESEARCH OVERVIEW

3.1 THEORETICAL BACKGROUND

Hierarchy of personal information.

The first part of the study tries to understand and form a hierarchy of sensitivity levels of different types of personal information. Woodman, et al., (1982) have noted in their study that corporate employees viewed personal data as not equally sensitive. Their survey reveals the notion that corporate employees' perceptions and attitudes toward company information handling policies appeared to be influenced by different types of personal information. They also further identify that "certain types of data that have previously been argued to be sensitive (e.g., medical data) may not be considered so if their use appears relevant to the nature of the data" (Woodman, et al., 1982). It is the intention of this study to measure the relevance of sensitivity levels of different types of personal information in the context of electronic commerce activities.

In addition, some studies also propose that information privacy concern may be connected to different types of personal information (Stone and Stone, 1990; Culnan, 1993). Culnan (1993) in her study of exploring consumer attitudes toward secondary information use found that 71 percent of responses put down financial information as the type of personal information that should never be shared without written consent from the

individual.[6] This is followed by information on lifestyle (23 percent), demographic information (18 percent), medical information (17 percent), individual's buying practices (8 percent), no personal information should be shared without permission (12 percent), and any information could be shared (4 percent) (Culnan, 1993). Her study apparently suggests that privacy concern is context-sensitive based on different types of personal information.[7]

Westin and Publisher (1997) also identified in their survey that there is a major increase, from 42 percent in 1990 to 59 percent in 1995, in the percentage of people refusing to disclose their personal information to businesses or companies due to the notion that the information requested was not needed or was too personal. This leads us to examine in this study what types of personal information Internet users deem to be sensitive or too personal.

An objective of this study is to develop a hierarchy of sensitivity levels of different types of personal information in the context of electronic commerce activities. In addition, this study also tries to understand the different dimensions of different types of personal information. Smith, et al. (1996) show that privacy concerns can be categorized into four dimensions: Collection, Errors, Unauthorized Secondary use, and Improper Access. These dimensions are explained in Table 4.

[6] Subjects were given an open-ended question
[7] However, the study is measuring the context sensitivity from only one dimension, which is Secondary Use of personal information.

Users' willingness to submit personal information.

Generally, most privacy reports convey the fact that Internet users are very concerned about the issue of privacy. The Equifax Report on Consumers in the Information Age further highlights this pivotal matter. It mentions that Americans are increasingly concerned over having to reveal personal information on the Internet. However, the report further reveals that despite the trepidation voiced over having to disclose personal information, most American acknowledge that "they would be upset if they were denied the opportunities which are only made possible through the collection and use of personal information."[8] Hoffman, et al., (1999) convey the same view. In their research, it is suggested that Internet users do grasp the importance of their personal data to Web marketers and actually reported to being interested to submit the information (Hoffman, et al., 1999). However, conditions under which Internet users are willing to submit personal information have not been empirically investigated. It is not known what factors induce Internet users to relinquish personal information.

Similarly, John Hagel and Marc Singer (1999) argue in their book that "relationship marketing focuses companies largely on collecting additional information about the customers they do have." However, the intent to gather personal information from the customers is not a simple task. Media hype continues to escalate consumers' paranoia regarding privacy risk on the net (Cohen, 2001). As a result, this remains one of the marketer's dilemmas in this digital information age. The authors further indicate that in this period of technological advancement it is more imperative than ever for companies to

[8] Source: Executive Summary, The Equifax Report on Consumers in the Information Age, 1990, is available from Equifax Inc., Atlanta, Georgia.

understand and reward customers for their relationship. According to Hagel and Singer (1999), there are two reasons for this. First, Internet consumers are beginning to get clever to the ruthless exploitation of personal data by corporations, which prompt an unwanted growth in junk mail and unsolicited advertising. Evidently, it has become increasingly simple now for savvy users to prevent businesses from collecting their personal data. Second, corporations need the personal information on customers and utilize it to their strategic advantage. Thus, Hagel and Singer (1999) prompt businesses to start compensating Internet users in exchange for their personal information.

Culnan and Milberg (1999) essentially share the same point of view. They argue that businesses must provide intangible benefits and privacy protection as an incentive for Internet users to relinquish their personal information (Culnan and Milberg, 1999). Culnan and Milberg (1999) further assert that this is an essential act in order to establish a long, trusting relationship with the Internet users and retain consumers' business and trust. Similar views are shared by Culnan and Milberg (1998) and Culnan and Armstrong (1997).

The above researches suggest that tangible as well as intangible incentives are required in order to nurture the relationship between Internet users and businesses. In addition to this, Culnan and Armstrong (1997) argue that procedural fairness also play a central role in establishing trust in the relationship. This can be accomplished by observing whether the organization's fair information practice matches or does not match the privacy policy posted on web sites. Subsequently, Internet users choose either to continue to participate

(practice matches policy) or halt their participation (practice does not match policy) (Culnan and Armstrong, 1997). Internet users have to take time and effort to read and understand web site privacy policies. However, the key problem here is consumers are ignorant about the issue of privacy. And privacy advocates constantly depict these consumers as careless and paranoid (Cranor, 2000; Dyson, 1998). This thesis will show the premise suggested is a valid one.

As discussed, experts in the field of information privacy have suggested that benefits would induce different levels of privacy concerns. However, this proposition is merely the experts' opinions and has not been empirically supported. The second part of this study tries to assess the willingness of Internet users to submit different types of personal information before and after benefits are revealed. However, the notion of whether fair information practice is in place was not divulged to the participants of the study. It is the contention of this thesis that Internet users could not possibly know if the organizations are adopting fair information practices. Realistically, Internet users will only realize this when ruthless activities of the organization to mine and distribute personal information are exposed. Therefore, this thesis seeks to understand whether or not Internet users are willing to relinquish their personal information given that the benefits to submit this personal information are revealed and the notion of whether or not organizations are adopting fair information practices is not told.

3.2 HYPOTHESES DEVELOPMENT

The preceding discussion apparently leads to the formulation research models depicted in Figure 1 and Figure 2. Figure 1 illustrates the first research question, which focuses on how six different types of personal information are affecting the level of information privacy concerns. Similarly, Figure 2 depicts the second research question, which focuses on how the level of information privacy concerns of six different types of personal information can be affected by attractiveness and perceived benefits of information disclosure.

First, this study hypothesizes that different types of personal information are not equally sensitive in the context of electronic commerce activities. In this study, six types of personal information are tested. Through thorough evaluation of numerous prominent web sites, the study opts to explore the relationship between these six types of personal information and information privacy concerns. These six types of information are financial information, medical information, personal history information, personal interest information, demographic information, and buying practices information. Further explanation and examples of these different types of personal information are shown in Table 5.

As noted earlier, it is expected that these different types of personal information will exhibit dissimilar sensitivity levels of privacy concern (Hoffman, et al, 1999, Hagel and Singer, 1999, Culnan and Milberg, 1999, Culnan and Armstrong, 1998). As Woodman and his colleagues (1982) put it, "Not all personal data are equally sensitive." In this

research, we posit that the six types of personal information will display unequal sensitivity levels of information privacy concerns. In other words, these six different types of personal information effect different sensitivity levels of privacy concerns. It might be expected that Internet users would value medical information more than their personal interest information. Therefore, this leads to:

Proposition 1: Sensitivity levels of personal information privacy concern will differ across the six types of personal information.

The above construct of information privacy concerns has four dimensions. These four underlying privacy dimensions addressing consumers' privacy concerns are unauthorized secondary use, improper access, collection, and errors[9]. In this study, we posit that different types of personal information do not affect these dimensions. Rationally, one may be bothered by the fact that a company is mining and distributing data illegitimately to an external party (unauthorized secondary use) regardless of the type of data involved. On the contrary, one may not be bothered by these dimensions at all. For example, these embedded dimensions may well be overlooked by Internet users and thought to be not important. In this case, Internet users may view information privacy issue from a single general overall perspective, without isolating their privacy concerns into different dimensions. Hence, the study conjectures that:

Proposition 2: Sensitivity levels of dimensions of information privacy concerns will not vary across different types of personal information.

[9] Refer to Table 4 for further explanation on these dimensions.

Secondly, we hypothesize that willingness to submit information would be higher when subjects exhibited lower level of information privacy concerns due to benefits revealed. Conversely, if the level of information privacy concerns remained unchanged or unaffected by the list of benefits, it would be the contention of this thesis that subjects would not be willing to relinquish personal information in exchange for benefits. The basic reasoning behind this presumption is that when subjects are influenced by attractiveness and perceived benefits of personal information's submission, they would be willing to lower their privacy concerns, therefore leading to eagerness to share their personal information. This theory is based on the numerous literatures that predict Internet users are keen on disclosing their personal information in general in exchange for tangible or intangible benefits (Kuchinskas, 2000; Hagel and Singer, 1999; Hoffman et al., 1999; Culnan and Milberg, 1999). Thus, the study postulates:

Proposition 3: Subjects will exhibit lower level of information privacy concerns across different types of personal information when they are told as to why submission of that information would be to their benefit.

3.3 SURVEY METHODOLOGY

Privacy Instrument

An information privacy instrument developed by Smith and his colleagues (1996) served as a framework to construct and plan the questionnaire used in this study[10]. The privacy instrument consists of fifteen questions that are initially intended to measure individuals' concerns about an organization's information privacy practices. The questions are categorized into four different subscales: Collection, Errors, Unauthorized Secondary

[10] Refer to Appendix I and Appendix II for the modified version of the questionnaire.

Use, and Improper Access[11] (Smith et al. 1996). Smith and his colleagues (1996) identified several central dimensions of individuals' information privacy concerns and through exhaustive surveys, they were convinced that these four dimensions are well representing the construct of individuals' information privacy concerns. These four dimensions were established through literature reviews and validated by comprehensive surveys. Also, the privacy instrument has been extensively validated and tested by Smith, et al. (1996) and Stewart, et al. (2001), indicating a high degree of reliability, generalizability, and validity.

However, the instrument was slightly adjusted to meet the primary objective of the study, which is to measure sensitivity level of different types of personal information. Specifically, the instrument was adapted in order to include different types of information. To meet the secondary objective of the study, which is to examine the willingness of the subjects to submit certain types of personal information, several questions were selected randomly from the questionnaire. Subjects would be asked to respond to these questions after being shown a list of benefits.

Pilot Studies

Before the final administration of the survey instrument, three pilot studies were conducted to validate the questionnaire. The surveys were administered to graduate students and volunteers at the University of British Columbia. There were several important findings worth mentioning here from the administration of the pilots.

[11] Refer to Table 4 for the subscales' explanation

In the first pilot study, subjects were less intrigued by the lists of benefits listed in the surveys. Post-survey interviews indicated that some of the benefits were of no interest to the subjects. This led the researchers to come up with a proposal to eliminate the problem. In addition to the list of benefits, subjects were asked to provide a list of reasons as to why the submission of such information to electronic commerce organizations on the web would be to their benefit. Then, the second pilot study was administered.

In the second pilot study, post-survey questions pointed out some flaws in some of the initially selected questions in the survey. For instance, subjects in pilot studies expressed similar concerns when they were presented with randomly selected questions from other dimensions before and after benefits were revealed, resulting in no effectiveness of benefits. One subject voiced her concern about a particular question in the pilot study, "I would feel the same way about unauthorized (secondary) access or use to personal information in a company no matter what benefits were offered." A further examination of the four dimensions revealed that only the "Collection" dimension was closely associated with the second objective of the survey, which is the measurement of subjects' willingness to submit personal information. The three other dimensions, namely unauthorized secondary use, improper access, and errors, were found to be related to the idea of handling and treatment of personal data. Quite the contrary, the "Collection" dimension was designated to measure the concerns of collecting and storing information by organizations. Subsequently, this designation of "Collection" dimension determines users' level of privacy concerns of organizations "collecting" and "storing" personal data,

which coincides with our objective of measuring subjects' willingness to share information. Plainly put it, we wished to measure subjects' information privacy perception of how personal information were collected before and after benefits were revealed, and not how the personal data were handled or scrutinized. Therefore, we contend that the "collection" dimension denoted the appropriate aspect to measure subjects' willingness to submit personal information than that of other dimensions

For the third pilot study, questions from the questionnaire under the "collection" dimension were chosen and the pilot subjects were asked to respond to these questions after being shown the benefits and asked to provide a list of reasons as to why the submission of such information to web sites would be to their benefit. Results indicated good acceptance of the questions selected from the "Collection" dimension and the benefits were perceived to be related to the survey context.

Therefore, questions under the "collection" dimension were chosen given that it better mirrored the intention of the subjects to relinquish or not to relinquish their personal information after benefits were revealed. The final modified survey instrument is shown in Appendix I and Appendix II. The survey instrument shown in Appendix I was used to validate propositions 1 and 2 whereas the survey instrument depicted in Appendix II was employed to validate proposition 3. The survey instrument was finally ready to be administered to experimental subjects.

Experimental Subject Population

This study utilized two different groups. The first group consisted of 83 students taking undergraduate commerce courses at the University of British Columbia. These students were given academic credit in their courses as an incentive to participate and participation was voluntary. Of the 83 students participating in the survey, 31% were males and 69% were females. Almost all of them were in their early 20s and come from diverse backgrounds such as accounting, health care, arts, economics, finance, and other disciplines as well. In addition, all participants had had at least a year of Internet experience, indicating their familiarity with computers and the World Wide Web. These students were randomly assigned to complete either Survey A or Survey B. A total of 42 students answered Survey A and 41 students completed Survey B.

The second batch of subjects was composed of faculty, staff, and doctoral students from the Faculty of Commerce at the University of British Columbia who volunteered to complete the survey. A total of 25 subjects in this group participated in this study. 16 subjects were males and 9 subjects were females. All of the subjects in this group used computer regularly and come from several disciplines such as information technology, marketing, finance, human resources, economics, and others. Of the 25 subjects participating in the survey, 12 subjects completed Survey A and 13 subjects finished Survey B. Implicit in this study is the belief that there are no differences in individuals in the two groups. The idea behind these two different groups is to enable the study to

correlate and contrast both groups' results. This is accomplished in order to maximize external validity and generalizability of the research.

Procedure

The questionnaire was administered to each subject. As mentioned, each subject was only required to answer either Survey A or Survey B, not both. The distribution of surveys was random in terms of selection of Survey A or Survey B. For the undergraduate students, the questionnaire was dispensed in a classroom. These students were asked to sit every other seat and not to discuss the experiment with other subjects. Most students completed the survey in about 25 minutes.

For the group of faculty, staff, and doctoral students, questionnaires were distributed to them via their mailbox. Again, the distribution of surveys was randomized and subjects were asked not to discuss about the survey with others. After this group had completed the questionnaire, the subjects returned the finished surveys to the researchers.

Experimental Methodology

As stated previously, proposition 1 tests whether or not sensitivity levels of personal information privacy concern would differ across the six types of personal information. In order to validate this proposition, a single factor repeated measures within group design (within subjects comparisons) was used. Specifically, subjects were randomly assigned to complete Survey A (Appendix I). In this first part of the study, the factor would be the types of information and the levels of the factor would be the six different types of

personal information. In addition, Survey A was randomized in the order of types of information exposure to strengthen the research design. For example, individual X would be exposed to questions pertinent to financial information first, followed by questions related to personal interest, medical, demographic, personal history, and buying practices information. Alternatively, Individual Y would be exposed to questions pertinent to medical information first, followed by questions associated with buying practices, personal history, personal interest, financial, and demographic information. All possible combinations of types of personal information were used and this was accomplished in order to reduce order effects. All responses collected here were used to confirm proposition 1 set forth in this thesis. Overall mean scores for each subject were calculated for each type of personal information and analyzed.

Secondly, proposition 2 described in this thesis examines the notion of levels of dimensions of information privacy concerns would not vary across different types of personal information. To test this proposition, two factors repeated measures within group design (within subjects comparisons) was used. Similar to previous design, the first factor would be the types of information with six levels (six types of personal information). The second factor, thereby, would be the dimensions of information privacy concerns with four levels (4 dimensions). All responses collected previously were used to analyze proposition 2. However, responses from the survey questions were divided into four dimensions as stated formerly. Specifically, mean scores for each of this dimension of each type of personal information were calculated for each subjects and analyzed.

In proposition 3, we state that subjects would exhibit lower level of information privacy concerns across different types of personal information when they were told as to why submission of that information to web sites would be to their benefits. This theory was examined using a single factor repeated measures between groups design (between groups comparison). The factor here would be the types of personal information and it involved 6 levels (six different types of personal information). Subjects were randomly assigned to complete Survey B. Similar to previous design, survey B was also randomized in the order of types of information exposure to reduce order effects. As explained earlier, the "Collection" dimension was used to measure subjects' willingness to submit personal information. Thus, Survey B only contained questions related to the "Collection" dimension after subjects were shown a list of benefits and asked to provide reasons as to why submission of personal information would be in their interest. Overall mean scores for each subject were calculated from Survey B. Therefore, relevant responses pertinent to questions under the "Collection" dimension were extracted from Survey A and were used in statistical analysis in conjunction with the results obtained from Survey B. Specifically, mean scores for the "Collection" dimension of each subject from Survey A were calculated. We would want to compare the results of relevant data collected from Survey A and Survey B. The chief reason for this comparison is to observe whether benefits induce differences. Recall that only Survey B contained benefits while Survey A lacked benefits.

An alternative within group design method to test proposition 3 was rejected based on several reasons. This alternative method would require each subject to complete both Survey A and Survey B. The desire to reduce "demand characteristics" of the participants to test proposition 3 is the chief rationale to eliminate the within group design method. The term "demand characteristics" in research field denotes the situation in which flaw experimental set-up design causes the participants of the study to speculate the hypotheses of the study and therefore confirm the experiment's hypotheses. In addition, the study would like to reduce the participants' fatigue and time in responding to the survey questions.

4. RESULTS

4.1 OVERALL RESULTS

Descriptive Statistics

There were no missing data and the sample size was 54 subjects for Survey A (see Appendix 1) and 54 subjects for Survey B (see Appendix II) in this experiment. Table 7 provides an overall result in which different types of personal information are ranked in decreasing order based on the mean scores[12]. Financial information ranks the highest with the mean score of 6.03 whereas Personal Interest information positions at the lowest with the mean score of 4.47 (See Table 8). Additionally, mean scores were also obtained for the four different dimensions discussed earlier. This was achieved by averaging the mean of questions pertinent to each dimension for each type of personal information. The number in the parentheses represents the ranking of these dimensions in the given type of personal information. For example, "Unauthorized Secondary Use" dimension is

[12] Based on the scale of 1 to 7.

ranked consistently the highest across the board for each type of personal information (See Table 7).

Perceived Differences of Sensitivity Levels on Different Types of Personal Information

For testing proposition 1, data was analyzed using a one-way repeated measures ANOVA. Table 8 summarizes the descriptive statistics. In this test, only one factor was involved and it had 6 levels (6 types of personal information). Table 9[13] illustrates the result of Mauchly's Test of Spherecity[14]. Mauchly's Test of Spherecity was used to determine whether the data satisfied one of the requirements for conducting a repeated-measures ANOVA. As shown in Table 9, the test produces a significant result indicating that the homogeneity of variance assumption had been violated. Therefore, the p-value for the test of within-subjects factor needs to be adjusted by using the Huynh-Feldt correction factor.

Table 10 denotes the Test of Within-Subjects Effects. The test proves that there is a highly significant difference between the six types of personal information in terms of the mean score overall concern levels ($F(3.89, 206.28)=49.90$, $p<0.0005$, with Huynh-Feldt correction). These results support proposition 1 that states levels of personal information privacy concern differ across different types of personal information.

However, the Test of Within-Subjects Effects only shows the significant main effect. Hence, a post-hoc test was conducted to test the difference between successive levels of

[13] SPSS Output.
[14] Huynh-Feldt adjusts the degrees of freedom downwards by an appropriate amount, which increases the p-value to correct the violation of assumptions.

the independent variables (different types of personal information). In this case, the Bonferroni test was performed and the results are reported in Table 11. A Bonferroni Test was conducted in which the test must be significant at the .05/n level (Cahusac and Langton, 2001). For this study, the n is 15 (based on the combinations of 6 types of information). Analysis revealed that Financial, Medical, and Personal History information were grouped together. These three types of information do not differ significantly and are ranked the most sensitive. Demographic information is ranked the second most sensitive by itself. The third group of Buying Practices and Personal Interest information is considered the least sensitive. This analyses on types of personal information shows how information privacy concerns on the Internet may differ.

Perceived Differences of Sensitive Levels on Dimensions of Different Types of Personal Information

Data associated with each dimensions of the information privacy concerns construct was analyzed using a two-way repeated measures ANOVA. Table 12 summarizes the descriptive statistic. In this test, an additional variable (DIMENSION) was added in addition to the "types" factor. The factor dimension has 4 levels (Unauthorized Secondary Use, Improper Access, Collection, and Errors). Similar to the one-way repeated measures ANOVA above, table 13 indicates the result of Mauchly's Test of Spherecity. Again, this test produces significant results indicating that the homogeneity of variance assumption had been violated. Therefore, the Huynh-Feldt correction factor would be used to correct the assumptions.

Table 14 depicts the results from the test for Within Subjects Effects. First, there is a highly significant F-ratio (the main effect) in which overall privacy concerns are significantly affected by different types of personal information (averaging over dimensions) ($F(3.89, 206.58)=49.47$, $p< .0005$, with Huynh-Feldt correction). This is similar to the results obtained through one-way repeated measures ANOVA. Therefore, the interesting part comes from the main effect results of the factor "Dimension." Likewise, the test shows a highly significant effect of dimension on overall information privacy concerns averaging over the six types of personal information. ($F(2.7,143.11)=39$, $p < .0005$, with Huynh-Feldt correction).

Finally, Table 14 also depicts that there is a significant interaction[15] between types of personal information and dimensions (the effects of dimensions depend on what types of information were tested). This can be possibly attributed to the "Collection" and "Errors" dimensions being ranked differently for the six types of information across the board. This result does not support proposition 2 in which the hierarchy of dimensions of information privacy concerns do vary across different types of personal information even though Table 7 shows that "Unauthorized Secondary Use" and "Improper Access" are ranked 1st and 2nd most sensitive respectively across the six different types of personal information.

A post-hoc contrast test on dimensions was conducted and the results are shown in Table 15. The interesting part comes from the first part of the table wherein successive contrast levels of the dimensions were performed averaging over six types of personal

[15] $F(12.67,519.29)=3.115$, $p < .0005$, with Huynh-Feldt correction

information. The test explains a pattern where "Unauthorized Secondary Use" and "Improper Access" dimensions are significantly different from each other ($F(1, 53)=24.31$, $p < .0005$). This applies to "Improper Access" and "Collection" ($F(1,53)=12.51$, $p= .001$) dimensions as well as "Collection" and "Errors" dimensions ($F(1,53)=6.21$, $p= .016$).

Since the SPSS software only tested 3 pairs combinations of these dimensions, a post hoc test was conducted to analyze all other combinations. The results are reported in Table 16. Overall, the four dimensions are significantly different from each other (averaging over types of information) based on the results. Based on Table 7, "Unauthorized Secondary Use" dimension were ranked the most sensitive, followed by "Improper Access," "Collection," and finally "Errors" dimension. Therefore, this can be interpreted in a way that these dimensions, to an extent, influence information privacy concerns on the Internet. In other words, subjects do care about these dimensions and may view information privacy concerns differently from the dimensions' context.

Perceived Benefits of Information Disclosure

In order to test proposition 3, the parametric unpaired T-Test was utilized. The mean scores of questions under the dimension "Collection" were calculated for each subject of Survey A (without benefits). Responses from participants of Survey B (with benefits) were averaged as well. Unpaired T-Test looks at these unpaired mean scores and determines the significant of these two groups. Table 17 contains the statistics results obtained from this test.

The underlying argument behind this hypothesis is that the study anticipated subjects would have lower privacy concerns when benefits were revealed in the experiment. A quick glance at Table 17 would convey the notion that the benefits did have an impact on subjects' responses. The mean scores of each type of personal information are lower, but not significantly, after the benefits were revealed. Proposition 3, wherein subjects will exhibit lower level of information privacy concerns across different types of personal information when they are told as to why submission of that information would be to their benefits, is only marginally supported by the results reported in Table 17. The null hypotheses are not rejected virtually across the board except for Personal Interest information. The study concludes that subjects have a lower privacy concerns for Personal Interest information when the benefits of submitting this information are told. Conversely, this does not hold true for other types of information. The lists of benefits do not have a significant effect on these remaining types of personal information. This result is appealing since one of the approaches that the survey took was to request participants to list benefits that they would like to receive in exchange of personal information.[16] Apparently, this did not have an impact on information privacy concerns in most cases.

4.2 COMPARISON OF RESULTS

Since our pool of subjects was consisted of two major demographic groups, it would be interesting to compare the results of both groups. Responses from subjects were separated into two groups, as mentioned previously, in order to extend the

[16] See Table 18.

generalizability of the research. Similar statistics tests were run again with results categorized into two groups; undergraduate students and faculty/staff/doctoral students. The latter group was deemed to be a more "mature" and experienced group as the subjects were older in terms of age. The undergraduate students group was composed of 83 subjects while the faculty/staff/doctoral students group was composed of 25 subjects.

Based on Table 19 and Table 20, we observe that the rankings of different types of personal information were very similar for both groups. Only a very small discrepancy evolved, in which the faculty, staff, and doctoral students group placed medical information more sensitive than financial information (See Table 20). This could have been caused by the small sample of faculty, staff, and doctoral students group. Otherwise, the overall ranking of different types of personal information results is strengthened by this group comparison.

An important finding discovered in this segregation is that the "mature" group had a higher concern toward the "Collection" dimension than that of the undergraduate students group. Table 19 and Table 20 summarize the responses to the survey questions. The mature group somewhat consistently ranked the "Collection" dimension as the second highest, behind Unauthorized Secondary Use. However, undergraduate students had a tendency to position the "Collection" dimension between third and fourth place. There is a possible explanation behind this pattern. It may be an indication that the mature and more experienced group had a tendency to be more worried about the data collection methods adopted by certain companies on the Internet. This well read and computer

savvy group[17] could be more concerned about technical issues such as cookie settings, identity tracking software, website "spoofing," and others before it comes to the issue of errors or improper access. This may hold less true for the undergraduate students as they were less experienced and educated when it comes to this matter. On the other end, the undergraduate students could be technically savvy too but they do not care about this "Collection" dimension.

Another important finding worth mentioning is that the two groups exhibited similar results when unpaired T tests were run for the second time to validate proposition 3. Subjects in both groups were only showing differences in the Personal Interest information category. For both groups, null hypotheses are not rejected, except for Personal Interest information, proving that there were no significant differences before and after benefits were revealed in most cases. To an extent, this supports and strengthens the overall results attained earlier. Table 21 and 22 summarize the results.

4.3 DISCUSSION OF RESULTS

Statistical analyses above provide support for proposition 1. Based on the results, this study suggests that the use of different types of information is a significant factor that needs to be considered carefully by companies wanting to extract data from its Internet users. Some types of information such as demographic information or personal interest information may be deemed to be relatively less sensitive while others such as medical or financial information may be judged to be an intrusion of personal privacy. The research

[17] This group is composed of faculty, staff and doctoral students. Majority of them had more than 5 years of Internet experience and were either doctoral students or professors.

confirms that financial, medical, and personal history information are categorized as more sensitive than that of demographic, buying practices, and personal interest information. On the second level, demographic information is proven to yield higher privacy concerns as compared to both buying practices and personal interest information. Buying practices and personal interest information are reckoned to generate similar information privacy concerns among users. There are several reasons as to why we think the differences exist across different types of personal information in terms of sensitivity levels. We theorize that the "identifier" factor plays an important role in this case. Most sensitive information such as financial, medical, and personal history information can be used to "identify" and trace the specific individual. On the other hand, less sensitive information, generated by the results of our study, such as buying practices and personal interest information are reckoned to be pretty generic. In addition, cultures can be a factor in determining sensitivity levels of personal information too. For example, one may not feel comfortable to discuss about medical or financial information of himself or herself in public. Alternatively, it is generally considered acceptable to discuss about one's personal interests or buying practices. Even though "identifier" and "culture" factors play an important role, these are not the only factors involved. There could be other complex factors influencing the sensitivity levels of different types of personal information too.

Another factor that needs to be taken into consideration as well is the dimensions of the information privacy concerns construct. We posited in Proposition 2 that privacy dimensions do not vary across different types of personal information. The results of the

statistical analyses do not provide sufficient evidence to support proposition 2. While "Unauthorized Secondary Use" dimension was somewhat consistently ranked the highest on subjects' list of privacy concerns, "Errors" dimension was consistently positioned at the lowest. The study theorizes that the sensitivity levels of both "Improper Access" and "Collection", to some degree, depend on maturity (age) as well as education of respective Internet users. Users who are computer literate may require organizations to tackle the issue of "Collection" dimension first before resolving the issue of "Improper Access" dimension.

Finally, results of this study provide sufficient evidence that the offering of benefits in exchange of personal information does not alleviate the problem of privacy concerns in most cases. Therefore, proposition 3 embedded in this thesis is only marginally supported by the statistical analyses. Benefits do not alleviate privacy concerns in five out of six types of personal information. This is a surprising finding because previous literature review had suggested that the issue of information privacy concerns could be improved by offering intangible and tangible benefits for Internet users. Nevertheless, the anecdotal opinions/theory gathered from the literature review were merely experts' opinions, and had not been empirically tested. Therefore, this study provides compelling empirical evidence that benefits do not induce lower privacy concerns. In general, subjects still viewed their personal information (except for personal interest) as a private entity that needs to be protected regardless of benefits or advantages that may come in the way.

5. DISCUSSIONS AND CONCLUSIONS

5.1 IMPLICATIONS FOR PUBLIC POLICY

The exploratory literature review of this study apparently suggests that laws and regulations are not sufficient to protect consumer privacy on the Internet. Evidently, government, who acts as an entity to establish these rules, always unearths loopholes in laws that established by themselves. For example, the U.S government once justified their action to post personal and financial information of public employees working with the government under the "sunshine law." Formerly, social security numbers and wages of teachers or policemen could be easily obtained from the government's web site. A prominent IT scholar once mentioned that the government is definitely not doing a great job so far to protect privacy (Rai, 2001). How do we expect government to protect its citizens' privacy on the Internet since the privacy laws set forth by the government itself are often vague and contradictory?

Also, our previous literature review shows that the issue of implementing regulations on the Internet boils down to the problem in which different countries have different standards in solving privacy problems. While the United States takes a very cautious and liberal platform, European countries, on the other hand, impose strict laws to tackle privacy online. Canada's choice of solution to the privacy problems lies between the two measures adopted by the United States and Europe. As a result, these three main continents often disagree with one another's choice of remedies to resolve privacy issues on the net (CNN, March 9, 2001). Based on this discussion, we recommend countries operate together and derive one lone comprehensive set of regulations that can be

adopted across nations. While our study alone is not sufficient to provide a thorough guideline to develop such sets of regulations, the empirical findings of this study can be used to understand how different types of personal information should be protected or guarded.

Information privacy on the Internet is not a clear-cut issue that can be tackled by some skimpy regulations. For example, should austere privacy laws of medical information be applied to personal interest information as well? The proper answer is no. A well thought out regulation should have different tenets on different types of information. It does not hold up to bundle them together and proclaim that one privacy law is adequate. One of this study's findings reckons that different types of information generate different levels of information privacy concerns amongst Internet users. This finding can provide a basic guideline for crafting public policy on the issue of privacy on the net. Some types of personal information such as medical, financial, and personal history information may need tougher legal protection while other types of information such as personal interest and buying practices may not need any official regulations at all. Recall the earlier discussion of the U.S. government publishing financial information of public employees. It may be acceptable to broadcast demographic information of the public employees, but it certainly raises eyebrows if financial information were made available on the net.

Secondly, we also observed that the four dimensions of the information privacy concerns construct were relatively important in determining sensitivity levels of users' privacy concerns. Again, tougher regulation may need to be placed on organizations on the issue

of unauthorized secondary use as it has consistently generated the highest level of concerns among our research subjects. Internet users need legal protection on this issue of unauthorized secondary use of personal data. Quite to the contrary, the issue of data errors in organizations' databases should not be taken seriously by the government. Data errors may serve as problems for the organizations itself, but they certainly do not possess threats to the general users population.

In addition to devise public policy to protect privacy on the net, government and federal agencies also run into difficulty when it comes to publishing information online. A recent article in The New York Times echoes the concerns and rage by New Yorkers when their voting information such as name, addresses, and party affiliations were made available on the Internet (Harmon, 2001). Albeit legal, the non-profit group took the information off the Internet. This example evidently shows of how government and federal agencies have little knowledge in regard to sensitivity levels of different types of personal information. But one of the outcomes derived from this study, the hierarchy of sensitivity levels of different types of personal information, can aid governments as well as federal agencies to recognize the sensitivity levels of different types of personal information in order to devise appropriate public policy to unravel privacy issues on the Internet.

To some extent, several experts surmise that legal regulations on the Internet could contribute to systems failure (Morrison and Firmstone, 2000). Morrison and Firmstone (2000) argue that 'policing' on the Internet ignores the central features of trust

mechanism, which primarily should be associated with internalization "of values and norms of what is appropriate behavior that assures system continuation." In spite of this, it is not the intention of this study to proclaim that privacy laws are worthless. Regulations indisputably work to a certain degree to protect consumer privacy. However, they are not sufficient and not consistently successful. One of the possible solutions to this issue is to promote on-going working relationships with both Internet users and digital businesses on the web. In such relationships, regulators try to determine the clear-cut objectives of both sides and evaluate appropriate laws or regulations that meet the needs. Needless to say, such approach may eliminate impervious laws.

5.2 IMPLICATIONS FOR BUSINESSES

The results in this study provide an understanding of one of the privacy dimensions from the Internet users' perspective. Start-up businesses aspiring to succeed in the digital business environment could use some of the results to guide their practice to elicit personal information from Internet users. First, it is crucial for these businesses to be aware of different sensitivity levels of different types of personal information and determine which types of information can be effectively extracted from Internet users and employed to the companies' utmost objectives.

We posit that when personal information can be traced to specific individuals, he or she may be reluctant to provide the information. In other words, personal information such as financial, medical, and personal history seem to "identify" individual whereas demographic, buying practices, and personal interest information are deemed to be less

intrusive. Companies need to take this logic into consideration when eliciting different types of personal information from Internet users. For instance, organizations should not ask for financial information unless it is an essential information to obtain in order to provide crucial services for Internet users.

Secondly, businesses have to address the dilemma of unauthorized secondary use and improper access or collection of personal information in the organizations as these issues ranked first and second most sensitive dimensions respectively on participants' list of privacy concerns[18]. Businesses do not only have to address this issue inside the organization, but they need to find approaches to convey these fair information practices to Internet users. Traditionally in brick and mortars financial institutions, banks communicate the information of their secure privacy practices to clients through pamphlets or brochures. In the digital environment, businesses customarily express the information through privacy policy posted online. However, results of this study show more than half of the participants only check the privacy policy on unreliable web sites to never check the policy at all.[19] Something is amiss and new and more effective ways to convey privacy practices information should be investigated.

In addition, this study finds that older and experienced[20] subjects' information privacy concerns are more gravitated toward the issue of "Collection." Conversely, the younger

[18] Demographic of sample determines which is more sensitive. As discussed earlier, a more mature and experienced group's concerns are more gravitated toward the "Collection" dimension than "Improper Access" dimension.
[19] See Table 6.
[20] Out of 25 subjects, 22 had more than 5 years experiences on the Internet and 3 had about 3-4 years experiences on the net.

subjects were more bothered by the issue of "Improper Access." Based on this premise, it is imperative for organizations to adopt different strategies to convince their targeted Internet users of their fair information practices. For example, a banking institution offering priority banking services online may want to convince their mature consumers that the bank is using legitimate and conspicuous methods to collect personal information.

Third, companies that collect information through the web are advised that benefits alone are not enough to attract Internet users to relinquish personal information. One of the paradoxes that digital businesses on the web may not realize is the fact that consumers tend to supply false information when requested. A 1998 National Survey on Consumer Preparedness and E-Commerce states that 35 percent of consumers in the age range of 18-29 year-old lie about their personal information on the Internet (Lotto, 2001). The inevitable discrepancies of information stored inside companies' integrated databases could spell inefficiency. This study theorizes that the combination of benefits and disclosure of fair information practices may alleviate the problem. Of course, as mentioned previously, a new technique to convey fair information practices needs to be considered.

Fourth, participants in the survey were asked to list benefits that they would like to receive in exchange for personal information. Table 18 summarizes the results obtained. The benefits are ordered in the order of significance for each type of personal information. It is interesting to note that the participants were keen on using their

personal information to build Internet community. This may dish up an opportunity to build a new model of start-up digital businesses although this approach has been employed by a number of successful business enterprises such as Amazon.com.

Finally, companies can learn how to resolve privacy issue by using a retrospective approach. Our discussion has displayed that privacy issues cannot be simplified. It cuts across many issues and there is a vital need to understand each of them thoroughly. However, the key to manage privacy problems is to establish trust on the Internet (Morrison and Firmstone, 2000). Morrison and Firmstone (2000) posit that trust facilitates to reduce uncertainty, risks, and complexity of individuals' decisions to exchange information and participate in electronic commerce activities. Unfortunately, Morrison and his colleague (2000) maintain that the Internet, as a system, presents various obstacles and challenges to the formation of trust. Perhaps, this remains as a challenge for digital businesses as business models and consumers continue to become complex in Internet environment.

5.3 IMPLICATIONS FOR INTERNET CONSUMERS

The bottom line for individuals is humans are essentially different. Nevertheless, this should not impede digital businesses on the Internet to provide excellent services for these consumers. And yet, we surmise that organizations cannot pursue this objective unaided. How might a company go about to provide crucial targeted services without a good grasp of what consumers want or do not want? In a sense, the orthodox approach of jumping in blindly into Internet business without understanding Internet users could be

a fruitless attempt. Internet users should be more aware that the more information companies know about the customer, the higher value can be provided by the institution (Moon, 2000).

Yet, many Internet users can be categorized as ignorant in regards to the issue of privacy on the Internet. The empirical results from our study, to an extent, support the premise above. One of the findings that can be generated from our study is from the demographic results that show more than half of the participants in this survey only check online privacy policy on unreliable web sites to never check privacy policy at all.[21] Surprisingly, our data also depicts most of them also perceive that laws or regulations is an effective method to deal with Internet privacy these days. In other words, Internet users want a third party (the government) to handle the convoluted issue for them. Up till now, the success of this practice remains a quandary.

We surmise that an on-going relationship between Internet users and businesses needs to be established. The thesis conjectures that successful relationship between Internet users and digital businesses shares several characteristics. First, Internet users ought to ensure a steady flow of germane information to businesses. Organizations need to identify what users need or do not need. Second, effective feedback should be provided to these users by digital businesses. This is done to ensure organizations' accountability and control of handling consumers' personal information without creating a stifling impression of unfair information practices. Bottom line again, consumers need to play a role too.

[21] Table 6

As research continues to be conducted to understand consumers' behavior, it is imperative for these Internet users to continue and foster a positive relationship with both business and government entities. Consumers should have an informed choice and the underlying idea here is a consistent and optimistic association with all parties involved as privacy on the Internet can only be improved if consumers play an active role.

5.4 FUTURE RESEARCH WORK

This thesis has laid down some settings for future research work in the area of information privacy in the context of electronic commerce. First, the study's findings show that six different types of personal information can be classified into groups and ordered based on its sensitivity levels. Future research work can entail another wide range of personal information constantly requested by businesses over the web. This may include information about education, politics, religious affiliations, and others.

Secondly, this study only tests the condition wherein subjects were asked whether or not lists of benefits affected their level of information privacy concerns. An alternative hypothesis would be to test whether lists of benefits AND disclosure of fair information practices would have an impact on privacy concerns. It would be interesting to observe if this combination could alleviate privacy concerns.

Third, it would be noteworthy to use this research method to test proposition 3 across nationalities or countries boundaries to see if it yields the same results. For example, it would be interesting to observe whether benefits alone can actually attract Internet users

in low privacy countries, such as Thailand or Indonesia, to share their personal information.

Finally, future study could be accomplished with a wider and diverse range of participants on the Internet. As would be explained in the next section, one of the limitations of the study is the diversity of the subjects in the experiments.

5.5 LIMITATIONS

There are several limitations of this study that need to be taken into consideration when evaluating the results. First, all participants of the study were undergraduate students, doctoral students, faculty, and staff at the University of British Columbia. Therefore, the results need to be assessed with care when applying it to the general Internet users population. In addition, the sample size of both homogeneous groups were rather small as compared to the population of Internet users. Although our survey population is not a good representative of the general Internet users population, we believe that our findings from the study, to an extent, are quite valid. Our pools of subjects could be classified into two groups; sophisticated and non-sophisticated in terms of using the Internet, which is fairly a considerable factor to categorize Internet users in general. In addition, the results from our study could be confidently applied effectively to younger generation of Internet users as most of our subjects in the experiment were in their early 20's (see Table 6). Nevertheless, it has to be pointed out that the results from this study should be evaluated with care since it may be difficult to differentiate the results between Internet users of

various demographic factors. This implies that there are many more demographic factors involved and the results of our study may not be representative of all Internet users.

Second, subjects in Group B who answered Survey B on the appendix were never told that their responses would be used to assess "willingness" to submit personal information in order to avoid "demand characteristics" as described formerly. It is possible that subjects would have invoked different responses if the objectives were revealed. However, as discussed, this is not desirable.

Third, similarly, subjects in Group A who answered Survey A on the appendix were never told that their responses would be used to classify and rank different types of personal information. However, the technique used in the study to present this treatment continuously (different types of personal information) could have instigated subjects to speculate about the hypothesis of the study. This may have contributed to the relationships of information privacy concerns and different types of personal information as revealed by the study's findings.

5.6 RESEARCH CONTRIBUTIONS

This research addresses two distinctive questions. First, it validates that different types of personal information evoke disparate information privacy concerns on the Internet. It furthers classifies these different types of information into groups and ranks these groups based on its sensitivity levels of privacy concerns. This helps to clarify which types of

information denoted to be sensitive than that of others from the consumers' point of views in the context of electronic commerce activities.

Second, this research also demonstrates that benefits alone are not sufficient to cease levels of privacy concerns among participants of the survey. The experimental findings indicate that the benefits will only have an effect on personal interest information, which consistently ranks the lowest in terms of privacy concerns amongst the six different types of personal information.

As discussed, the findings from this study can be utilized by government agencies as well as corporations to devise appropriate public and corporate policies respectively in order to deal with privacy issues. In addition, this study offers some degree of understanding of how our subjects viewed Internet privacy in general.

The research reported here can serve as a foundation for further research to explore several dimensions of privacy concerns from the Internet users' standpoints. Extensive research is still needed to understand consumers' behavior. Conventional ways to conduct businesses on the web would not succeed, as Internet requires digital businesses to be flexible, efficient, and robust. At the center, digital businesses that take initiatives to learn from outsiders, especially customers, can be assured of greater advantages. Again, the statement that needs to be reiterated is the three entities: government, Internet users, and digital businesses, ought to play a more active role in their quest to eradicate the problems of information privacy on the Internet. As today's information technology

continues to evolve, information sharing on the Internet is a critical idea that needs to be protected and treasured.

FIGURE 1: INFORMATION PRIVACY RESEARCH MODEL

(RESEARCH QUESTION 1)

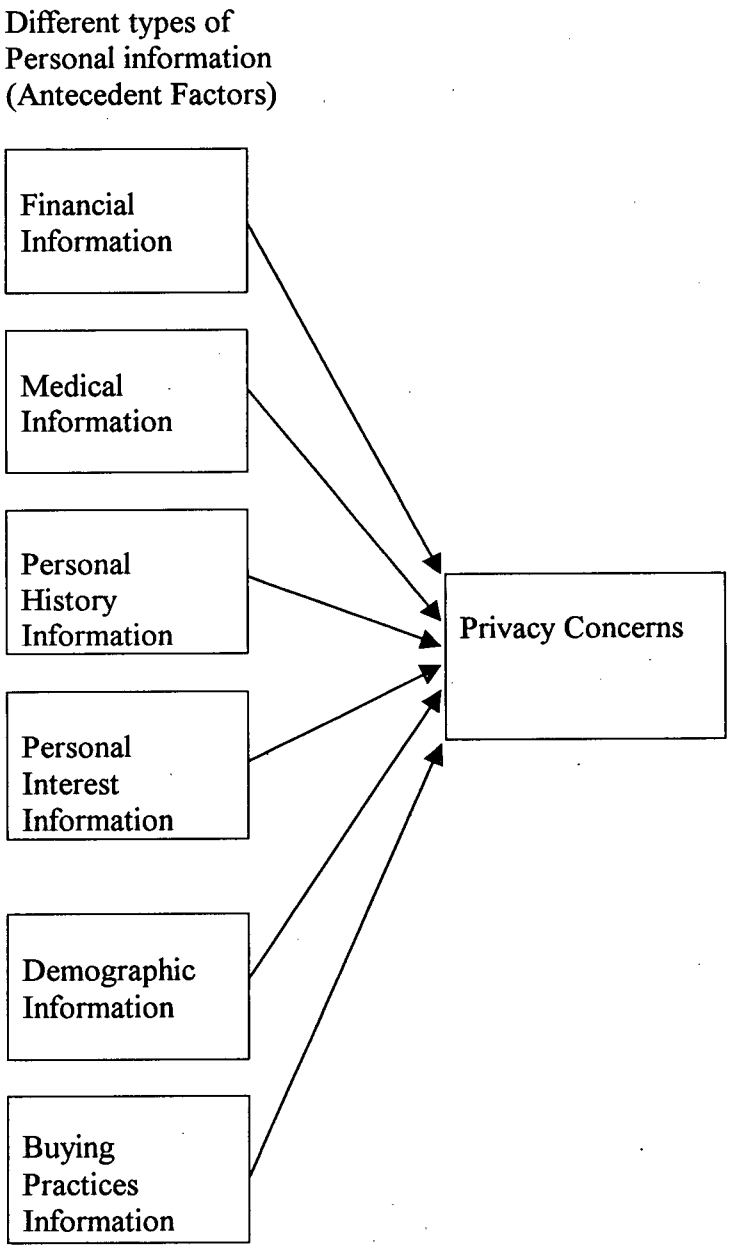


FIGURE 2: INFORMATION PRIVACY RESEARCH MODEL

(RESEARCH QUESTION 2)

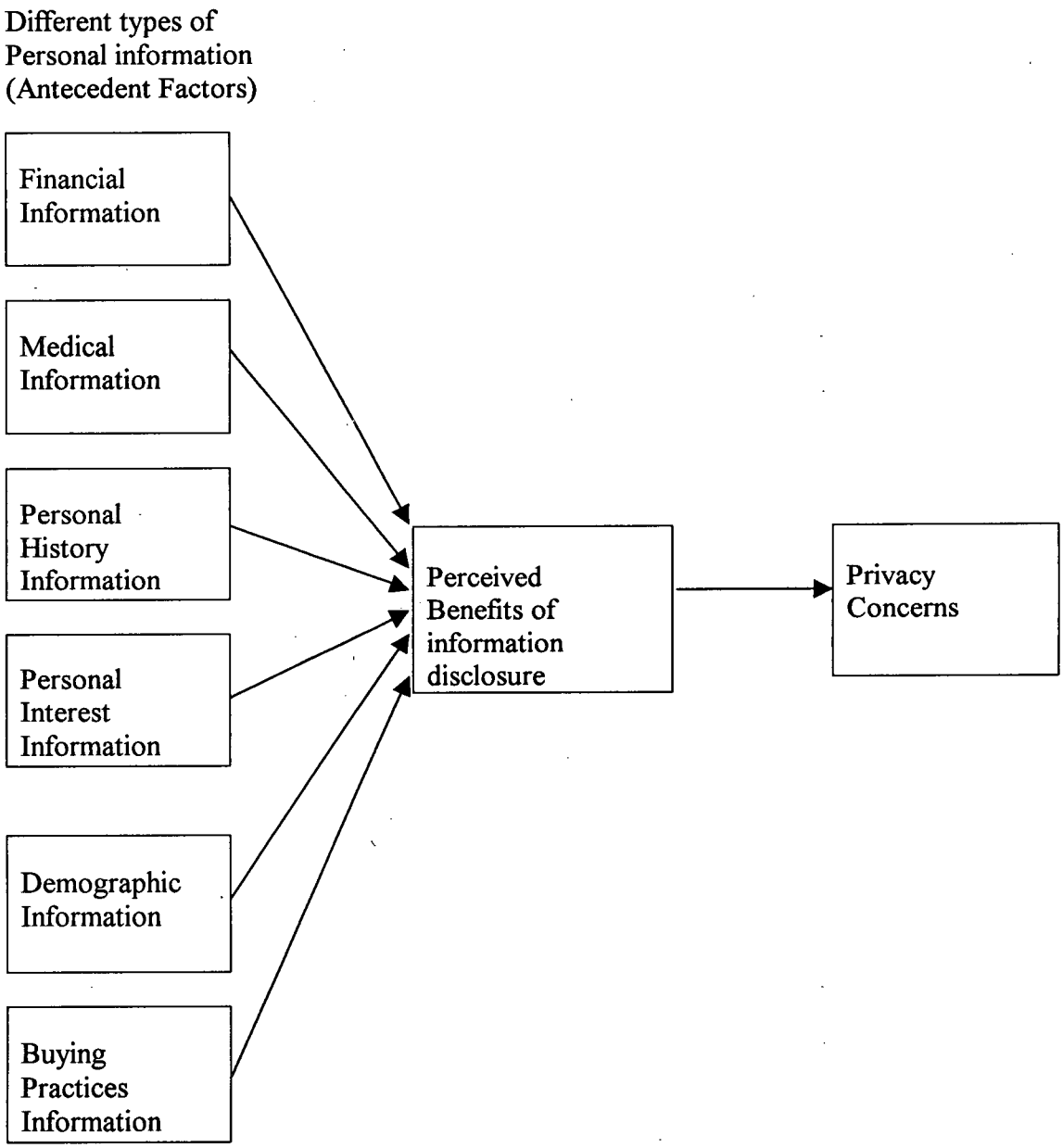


TABLE 1: FTC'S FOUR FAIR INFORMATION PRACTICE PRINCIPLES

Source: Federal Trade Commission **Privacy Online: A Report to Congress** June 1998

Principle	Explanation
Notice/Awareness	Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.
Choice/Consent	Choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information – *i.e.*, uses beyond those necessary to complete the contemplated transaction.
Access/ Participation	It refers to an individual's ability both to access data about him or herself – *i.e.*, to view the data in an entity's files – and to contest that data's accuracy and completeness.
Integrity/ Security	To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form

TABLE 2: A TAXONOMY OF CONSUMER PRIVACY CONCERNS

Source: Wang, H., Lee, M. and Wang, C. **Consumer Privacy Concerns about Internet Marketing** *Communications of the ACM* (41:3), March 1998, pp. 65.

	Improper acquisition			Improper use		Privacy invasion	
	Improper access	Improper collection	Improper monitoring	Improper analysis	Improper transfer	Unwanted solicitation	Improper storage
Direct mailing				P		E	
Preference tracking	E	E	E				
Unwanted eavesdrop	P	E	E				
No opting-out				E			P
Third-party distribution				E	E		P

E: Explicit P: Probable

TABLE 3: RELATIONSHIP BETWEEN PRIVACY ENHANCING TECHNOLOGIES AND PRIVACY CONCERNS

Source: Wang, H., Lee, M. and Wang, C. **Consumer Privacy Concerns about Internet Marketing** *Communications of the ACM* (41:3), March 1998, pp. 67.

	Awareness Principle		**Empowerment principle**				**Redress principle**
	Merchant profiling	**Trust framework**	**Access control**	**User pref. Profiling**	**Anonymity**	**Encryption**	**Content filtering**
Improper access		E	E	P			
Improper collection	P	P		P		E	
Improper monitoring	P	P		P	E	P	
Improper use	P	P					
Improper transfer	P	P		P			
Unwanted solicitation				P	P		E
Improper storage	P	P		P		E	

E: Effective P: Partially Effective

TABLE 4: EXPLANATION OF PRIVACY'S DIMENSIONS

Source: Smith, H. J., Milberg, S. J., Burke, S. J. **Information Privacy: Measuring Individuals' Concerns About Organization Practices** *MIS Quarterly* 20(2), June 1996, pp.172.

Dimension	Description of Concerns
Collection	Concern that extensive amounts of personally identifiable data are being collected and stored in databases
Unauthorized Secondary Use (Internal)	Concern that information is collected from individuals for one purpose but is used for another, secondary purpose (internally within a single organization) without authorization from the individuals.
Unauthorized Secondary Use (External)	Concern that information is collected for one purpose but is used for another, secondary purpose after disclosure to an external party (not the collecting organization).
Improper Access	Concern that data about individuals are readily available to people not properly authorized to view or work with this data.
Errors	Concern that protection against deliberate and accidental errors in personal data is inadequate.

Note: Unauthorized Secondary Use **(Internal)** and Unauthorized Secondary Use **(External)** are merged into a single dimension: Unauthorized Secondary Use.

TABLE 5: EXPLANATION OF DIFFERENT TYPES OF PERSONAL INFORMATION

Types of Information	Source (if any)	Explanation
Financial Information	Brown (2000)	This includes information about wages, mortgages, loan applications, and taxes.
Medical Information	Consultation Paper on Protection of Personal Health Information, Government of Saskatchewan (1997)	This includes information about states of one's health, treatments received, and hospital records.
Personal Interest Information		This includes information about hobbies, which web sites users like to go, music preferences, and others.
Buying Practices Information		This includes information about buying habits, how often users buy online or offline, what types of product/service users buy and others.
Personal History Information	Trempus (2000) Georgetown Internet Privacy Policy Survey (1999)	This includes information about name, postal address, and e-mail address
Demographic Information	Georgetown Internet Privacy Policy Survey (1999)	This includes information about gender, zip code, marital status and race.

Note: The list here is not extensive, but merely to present a few examples to denote the meaning of specific types of information.

TABLE 6: OVERALL DEMOGRAPHIC STATISTICS

Number of Subjects: 108 subjects

Variable	Selection	Percentage
Age	18 – 22 year old	67 %
	23 – 27 year old	5 %
	28 – 32 year old	12 %
	33 – 37 year old	4 %
	38 – 42 year old	1 %
	43 – 47 year old	2 %
	48 – 52 year old	3 %
	53 – 57 year old	2 %
	58 – 62 year old	4 %
Education	High School	5 %
	Vocational	1 %
	Diploma	3 %
	Some College	49 %
	College	17 %
	Graduate School	22 %
	Others	3 %
Gender	Male	39 %
	Female	61 %
Industry	Accounting	13 %
	Finance	19 %
	Information Technology	15 %
	Health Care	1 %
	Arts	3 %
	Marketing	20 %
	Sciences	1 %
	Operations Management	1 %
	Economics	3 %
	Human Resources	3 %
	Others	21 %
Internet Experience	1 – 2 years	4 %
	3 – 4 years	44 %
	More than 5 years	52 %
Privacy Policy	Check privacy policy every time	2 %
	Check privacy policy often	6 %
	Check privacy policy once in a while	37 %
	Check privacy policy only on unreliable web sites	28 %
	Never check privacy policy	27 %
Think that law/regulation is an effective method to deal with information privacy on the Internet?	Yes	53 %
	No	17 %
	Undecided	30 %

TABLE 7: OVERALL DESCRIPTIVE STATISTICS

Types of Information	Collection	Unauthorized Secondary Use	Errors	Improper Access	Average
Financial	5.99 (3)	6.52 (1)	5.39 (4)	6.26 (2)	6.03
Medical	5.56 (4)	6.52 (1)	5.64 (3)	6.18 (2)	5.97
Personal History	5.57 (3)	6.46 (1)	5.07 (4)	6.13 (2)	5.78
Demographic	4.61 (3)	5.51 (1)	4.55 (4)	5.21 (2)	4.95
Buying Practices	4.30 (3)	5.39 (1)	4.10 (4)	4.89 (2)	4.65
Personal Interest	4.33 (3)	5.22 (1)	3.73 (4)	4.71 (2)	4.47
Average	5.06 (3)	5.94 (1)	4.75 (4)	5.56 (2)	

Notes: The number in the parentheses represents the ranking of these dimensions in the given type of personal information

TABLE 8: DESCRIPTIVE STATISTICS OF ONE-WAY REPEATED MEASURES ANOVA

Types of Information	Mean	Std. Deviation	N
FINANCIAL	6.03	.6715	54
MEDICAL	5.97	.6666	54
PERSONAL HISTORY	5.78	.8348	54
DEMOGRAPHIC	4.95	1.0706	54
BUYING PRACTICES	4.65	1.0246	54
PERSONAL INTEREST	4.47	1.0443	54

TABLE 9: MAUCHLY'S TEST OF SPHERICITY OF ONE-WAY REPEATED MEASURES ANOVA

	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon[a]
Within Subjects Effect					Huynh-Feldt
TYPES	.377	49.873	14	.000	.778

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.

a May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

TABLE 10: TESTS OF WITHIN-SUBJECTS EFFECTS OF ONE-WAY REPEATED MEASURES ANOVA

Source		Type III Sum of Squares	df	Mean Square	F	Sig.
TYPES	Huynh-Feldt	131.507	3.892	33.788	49.904	.000
Error (TYPES)	Huynh-Feldt	139.665	206.282	.677		

TABLE 11: POST-HOC TEST OF ONE-WAY REPEATED MEASURES ANOVA

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	99.67% Confidence Interval of the Difference				
					Lower	Upper			
Pair 1	FINANCIAL - MEDICAL	5.315E-02	.7947	.1082	-.2797	.3860	.491	53	.625
Pair 2	FINANCIAL – HISTORY	.2111	.8297	.1129	-.1364	.5586	1.870	53	.067
Pair 3	FINANCIAL - DEMO	1.0778	1.0774	.1466	.6266	1.5291	7.351	53	.000
Pair 4	FINANCIAL – BUYING	1.3728	.9478	.1290	.9759	1.7698	10.644	53	.000
Pair 5	FINANCIAL – INTEREST	1.5518	1.0185	.1386	1.1253	1.9784	11.197	53	.000
Pair 6	MEDICAL – HISTORY	.1580	.7356	.1001	-.1501	.4661	1.578	53	.120
Pair 7	MEDICAL – DEMO	1.0247	1.1261	.1532	.5531	1.4963	6.687	53	.000
Pair 8	MEDICAL – BUYING	1.3197	1.1224	.1527	.8496	1.7897	8.640	53	.000
Pair 9	MEDICAL – INTEREST	1.4987	1.2135	.1651	.9905	2.0069	9.076	53	.000
Pair 10	HISTORY – DEMO	.8667	.9107	.1239	.4853	1.2481	6.994	53	.000
Pair 11	HISTORY – BUYING	1.1617	1.0523	.1432	.7210	1.6024	8.112	53	.000
Pair 12	HISTORY – INTEREST	1.3407	1.2016	.1635	.8374	1.8440	8.199	53	.000
Pair 13	DEMO – INTEREST	.4740	1.2934	.1760	-6.7693E-02	1.0157	2.693	53	.009
Pair 14	DEMO – BUYING	.2950	.9383	.1277	-9.7961E-02	.6880	2.310	53	.025
Pair 15	BUYING – INTEREST	.1790	.8424	.1146	-.1738	.5318	1.562	53	.124

TABLE 12: DESCRIPTIVE STATISTICS OF TWO-WAY REPEATED MEASURES ANOVA

	Mean	Std. Deviation	N
FIN1	6.5324	.6516	54
FIN2	6.2655	.9005	54
FIN3	5.9861	.8854	54
FIN4	5.3796	1.1622	54
MED1	6.5324	.5747	54
MED2	6.1914	.7813	54
MED3	5.5556	1.0355	54
MED4	5.6667	1.1441	54
HIST1	6.4676	.8647	54
HIST2	6.0556	1.1723	54
HIST3	5.6620	1.0061	54
HIST4	5.0093	1.3787	54
DEMO1	5.5324	1.3711	54
DEMO2	5.2160	1.3631	54
DEMO3	4.6065	1.3207	54
DEMO4	4.5046	1.2547	54
BUY1	5.4213	1.3692	54
BUY2	4.8704	1.4089	54
BUY3	4.3194	1.1989	54
BUY4	4.0556	1.2292	54
INTER1	5.2546	1.3576	54
INTER2	4.6605	1.5289	54
INTER3	4.3380	1.1967	54
INTER4	3.6898	1.1471	54

Legend:

TYPES OF INFORMATION:

FIN – Financial Information
MED- Medical Information
HIST- Personal History Information
DEMO – Demographic Information
BUY – Buying Practices Information
INTER – Personal Interest Information

DIMENSIONS (NUMBERS PROCEEDING THE TYPES)

1 – Unauthorized Secondary Use
2 – Improper Access
3 – Collection
4 – Errors

TABLE 13: MAUCHLY'S TEST OF SPHERICITY OF TWO-WAY REPEATED MEASURES ANOVA

	Mauchly's W	Approx. Chi-Square	df	Sig.	Epsilon[a]
Within Subjects Effect					**Huynh-Feldt**
TYPES	.383	49.099	14	.000	.780
DIMENSION	.707	17.904	5	.003	.900
TYPES * DIMENSION	.023	179.441	119	.000	.883

Tests the null hypothesis that the error covariance matrix of the orthonormalized transformed dependent variables is proportional to an identity matrix.
a May be used to adjust the degrees of freedom for the averaged tests of significance. Corrected tests are displayed in the Tests of Within-Subjects Effects table.

TABLE 14: TEST OF WITHIN-SUBJECTS EFFECTS OF TWO-WAY REPEATED MEASURES ANOVA

Source		Type III Sum of Squares	df	Mean Square	F	Sig.
TYPES	**Huynh-Feldt**	527.451	3.898	135.323	49.474	.000
Error (TYPES)	**Huynh-Feldt**	565.046	206.579	2.735		
DIMENSION	**Huynh-Feldt**	284.073	2.700	105.203	39.001	.000
Error (DIMENSION)	**Huynh-Feldt**	386.039	143.112	2.697		
TYPES * DIMENSION	**Huynh-Feldt**	19.576	13.242	1.478	3.663	.000
Error(TYPES* DIMENSION	**Huynh-Feldt**	283.222	701.802	.404		

TABLE 15: TESTS OF WITHIN SUBJECTS CONTRASTS OF TWO-WAY REPEATED MEASURES ANOVA

Source	DIMENSION	Type III Sum of Squares	df	Mean Square	F	Sig.
DIMENSION	Level 1 vs. Level 2	9.235	1	9.235	24.305	.000
	Level 2 vs. Level 3	11.692	1	11.692	12.508	.001
	Level 3 vs. Level 4	7.012	1	7.012	6.213	.016
Error (DIMENSION)	Level 1 vs. Level 2	20.139	53	.380		
	Level 2 vs. Level 3	49.540	53	.935		
	Level 3 vs. Level 4	59.813	53	1.129		

Legend:

Level 1 – Unauthorized Secondary Use
Level 2 – Improper Access
Level 3 – Collection
Level 4 – Errors

TABLE 16: POST HOC ANALYSIS OF TWO WAY REPEATED MEASURES ANOVA

Source		Type III Sum of Squares	df	Mean Square	F	Sig.
Unauthorized Secondary Use Vs Collection	Huynh-Feldt	125.127	1.000	125.127	57.813	.000
Error (Unauthorized Secondary Use Vs Collection)	Huynh-Feldt	114.711	53.000	2.164		
Unauthorized Secondary Use Vs. Errors	Huynh-Feldt	248.769	1.000	248.769	95.757	.000
Error (Unauthorized Secondary Use Vs. Errors)	Huynh-Feldt	137.689	53.000	2.598		
Improper Access Vs. Errors	Huynh-Feldt	110.434	1.000	110.434	44.611	.000
Error (Improper Access Vs. Errors)	Huynh-Feldt	131.199	53.000	2.475		

TABLE 17: OVERALL UNPAIRED T-TEST RESULTS

TYPES OF INFORMATION	Mean before benefits were revealed	Mean after benefits were revealed	Test Result	Significant Level
Financial	5.99	5.80	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.168
Medical	5.56	5.39	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.255
Personal History	5.67	5.35	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.070
Demographic	4.61	4.21	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.074
Buying Practices	4.30	4.12	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.243
Personal Interest	4.33	3.52	Ho is rejected; Insufficient evidence to support that the mean scores are the same.	0.003

Note:

- Tested at an alpha level of significance of 0.05
- Mean scores for each type of personal information were calculated by averaging the responses from the "Collection" dimension of the surveys.

TABLE 18: LIST OF BENEFITS

Note: The benefits are ordered in decreasing order of significance for each type of personal information

TYPES OF INFORMATION	Frequency Count
FINANCIAL INFORMATION	
- Information about tax submission	8
- Stock market information	5
- Better services and interest rates (credit cards application, mortgages, etc.)	5
- More accurate information about financial planning, recommendations and others	5
- Monetary award	3
- Security	2
- Information about student loan.	1
PERSONAL HISTORY INFORMATION	
- More freebies and discounts	8
- Recruiting/Job Fairs information	5
- Building community online	4
- Monetary award	3
- Air miles collection	1
BUYING PRACTICES INFO	
- To get information about latest product (based on previous buying history)	8
- Directory for buying merchandises	7
- Discounts/Coupons	5
- Relevant free goods	4
- Ability to save time (online shopping)	3
- Monetary award	2

Note: Continue on the next page.

LIST OF BENEFITS II

TYPES OF INFORMATION	Frequency Count
DEMOGRAPHIC INFO	
- More discounts/coupons	6
- Ability to build/join community online	5
- Free Goods/Disk Space	3
- Job Fairs/Recruiting information	2
- Monetary award	2
PERSONAL INTEREST INFO	
- Meeting people with the same interests (community online)	8
- Relevant promotional emails	8
- Providing extra knowledge about interests	3
- Related discount/coupons	2
- Monetary award	2
MEDICAL INFORMATION	
- Relevant medical information based on historical background (family, gender)	11
- Discounts on products (insurance)	6
- Power to divulge medical information to any medical practitioner when needed	4
- Record of previous prescriptions (so that can be purchased again)	4
- New drugs information	3
- Monetary award	2
- Obtaining health record through phone	1

TABLE 19: UNDERGRADUATE STUDENTS' RESULTS

UNDERGRADUATE STUDENTS' RESULTS

Types of Information	Collection	Unauthorized Secondary Use	Errors	Improper Access	Average
Financial	5.85 (3)	6.54 (1)	5.55 (4)	6.32 (2)	6.05
Medical	5.39 (4)	6.48 (1)	5.79 (3)	6.29 (2)	5.97
Personal History	5.57 (3)	6.56 (1)	5.24 (4)	6.37 (2)	5.90
Demographic	4.47 (4)	5.61 (1)	4.72 (3)	5.36 (2)	5.02
Buying Practices	4.17 (4)	5.49 (1)	4.25 (3)	5.06 (2)	4.72
Personal Interest	4.17 (3)	5.38 (1)	3.95 (4)	4.96 (2)	4.59
Average	4.93 (3)	6.01 (1)	4.92 (4)	5.73 (2)	

Note: The number in the parentheses represents the ranking of these dimensions in the given type of personal information

TABLE 20: FACULTY/STAFF/DOCTORAL STUDENTS' RESULTS

FACULTY/STAFF/DOCTORAL STUDENT' RESULTS

Types of Information	Collection	Unauthorized Secondary Use	Errors	Improper Access	Average
Financial	6.48 (2)	6.50 (1)	4.79 (4)	6.08 (3)	5.96
Medical	6.13 (2)	6.71 (1)	5.23 (4)	5.83 (3)	5.98
Personal History	6.00 (2)	6.15 (1)	4.21 (4)	4.97 (3)	5.36
Demographic	5.08 (2)	5.25 (1)	3.75 (4)	4.72 (3)	4.70
Buying Practices	4.85 (2)	5.19 (1)	3.38 (4)	4.19(3)	4.42
Personal Interest	4.92 (1)	4.83 (2)	2.79 (4)	3.61 (3)	4.07
Average	5.58 (2)	5.77 (1)	4.03 (4)	4.90 (3)	

Note: The number in the parentheses represents the ranking of these dimensions in the given type of personal information

TABLE 21: UNPAIRED T-TEST RESULTS (UNDERGRADUATE STUDENTS)

TYPES OF INFORMATION	Mean before benefits were revealed	Mean after benefits were revealed	Test Result	Significant Level
Financial	5.85	5.72	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.300
Medical	5.39	5.15	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.215
Personal History	5.57	5.28	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.139
Demographic	4.47	4.12	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.146
Buying Practices	4.17	4.12	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.436
Personal Interest	4.17	3.58	Ho is rejected; Insufficient evidence to support that the mean scores are the same.	0.027

Note:
-Tested at an alpha level of significance of 0.05
-Mean scores for each type of personal information were calculated by averaging the responses from the "Collection" dimension of the surveys.

TABLE 22: UNPAIRED T-TEST RESULTS (FACULTY/STAFF/DOCTORAL STUDENTS)

TYPES OF INFORMATION	Mean before benefits were revealed	Mean after benefits were revealed	Test Result	Significant Level
Financial	6.48	5.98	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.095
Medical	6.13	6.17	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.432
Personal History	6.00	5.71	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.157
Demographic	5.08	4.65	Ho is not rejected; Insufficient evidence to support that the mean scores differ.	0.132
Buying Practices	4.85	4.10	Ho not rejected; Insufficient evidence to support that the mean scores differ.	0.071
Personal Interest	4.92	3.13	Ho is rejected; Insufficient evidence to support that the mean scores are the same.	0.006

Note:
-Tested at an alpha level of significance of 0.05
-Mean scores for each type of personal information were calculated by averaging the responses from the "Collection" dimension of the surveys.

REFERENCES

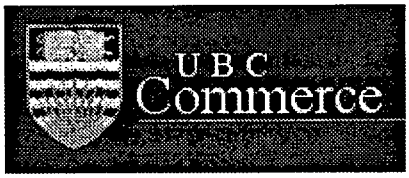
1. Ackerman, M. S. & Cranor, L. (1999) Privacy Critics: UI Components to Safeguard Users' Privacy, Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI'99) (pp. 258-259).
2. Bier, W. C. (1980) Privacy: A Vanishing Value? New York: Fordham University Press.
3. Brown, L. R. Banking and Financial Information on the Internet: Personal Privacy vs. New Technology Online. Internet. 30 March. 2000. Available: http://www.law.stetson.edu/courses/rbrown.htm.
4. Cahusac, P.M.B. & Langton, S.R.H. (2001) Multiple Comparison Procedures Online. Internet 1 March 2001. Available: http://www.stir.ac.uk/Departments/HumanSciences/Psychology/4614/HANDOUTS/Lectures/mc_anova.pdf.
5. Cohen, A. (9 July 2001). Internet Insecurity. Time pp. 22-29.
6. CNNfn. FTC sues Toysmart.com. Online. Internet. 10 July. 2000. Available: http://cnnfn.com/2000/07/10/technology/toysmart/.
7. CNN. U.S. Lawmakers examine pros, cons of privacy law. Online. Internet. 2 March. 2001. Available: http://www.cnn.com/2001/TECH/internet/03/02/privacy.reut/index.html
8. CNN. U.S. Lawmakers criticize strong EU privacy laws Online. Internet, 9 March. 2001. Available: http://www.cnn.com/2001/TECH/industry/03/09/privacy.reut/index.html
9. Cooper, D.R. & Schindler, P.S. Business Research Methods (6^{th} edition) Irwin/McGraw-Hill Series.
10. Cranor, L. F. (June/July 1998). Internet Privacy: A Public Concern. netWorker: The Craft of Network Computing (2:3). pp. 13-18.
11. Cranor, L. F. (February 1999). Internet Privacy. Communications of the ACM (42:2). pp. 29-31.
12. Culnan, M. J. (September 1993) How did they get my name?: An exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly . pp. 341-361.
13. Culnan, M. J. & Armstrong, P.K. (1997) Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation Organization Science, forthcoming
14. Culnan, M. J. & Milberg, S. (1999) Consumer Privacy Information Privacy: Looking Forward, Looking Back, Georgetown University Press. Forthcoming.
15. Culnan, M.J. & Milberg, S. (1998) The Second Exchange: Managing Customer Information in Marketing Relationships. Forthcoming publishing.
16. Dyson, E. (23 April 1998). Privacy Protection: Time to think and act locally and globally. Release 1.0.
17. Federal Trade Commission (July 1999). Self-Regulation and Privacy Online: A Report to Congress. Available: http://www.ftc.giv/privacy/.
18. Federal Trade Commission FTC Recommends Congressional Action to Protect Consumer Privacy Online. Online. Internet. 22 May. 2000. Available: http://www.ftc.gov/opa/2000/05/privacy2k.htm.

19. Gavison, R. (January 1980) Privacy and the Limits of Law The Yale Law Journal (89:3). pp. 421-471
20. Government of Saskatchewan. Consultation Paper on Protection of Personal Health Information Online. Internet. 27 October. 1997. Available: http:// www.gov.sk.ca/health/phiq/types.htm
21. Green, H., France, M., Stepanek, M. & Borrus, A. Our Four-Point Plan. Business Week Online. Internet. 20 March. 2000. Available: http://www.businessweek.com/2000/00_12/b3673006.htm.
22. Georgetown Internet Privacy Policy Survey 1999. Online. Internet. 11 August. 2000. Available: http://www.gsb.georgetown.edu/faculty/culnanm/gippshome.html.
23. GVU's Tenth WWW User Surveys. Online. Internet. October. 1998. Available: http://www.gvu.gatech.edu/user_surveys/survey-1998-10/
24. Hagel, J. & Singer, M. (January 1999) Net Worth: Shaping Markets When Customers Make The Rules. Harvard Business School Press.
25. Harmon, A. Group Deletes Private Information About Voters from the Internet. The New York Times 25 August, 2001.
26. Hoffman, D. L., Novk, T. P. & Peralta, M. (April 1999). Building Consumer Trust Online. Communications of the ACM (42:4). pp. 80-85.
27. Industry Canada's e-commerce web site. Personal Information Protection and Electronic Documents Act Online. Internet. Available: http://e-com.ic.gc.ca.
28. Kleinbard, D. Web has its eye on you. Online. Internet. March 6. 2000. Available: http://cnnfn.com/2000/03/06/technology/privacy_main/.
29. Kuchinskas, Susan. (12 September 2000). One-to-(N)one? Business 2.0 (5:17). pp. 141-148.
30. Laudon, K. C. (September 1996). Markets and Privacy. Communications of the ACM (39:9). pp. 92-104.
31. Loch, K. D., Carr, H. H. & Warkentin, M. E. (June 1992) Threats to Information Systems: Today's Reality, Yesterday's Understanding. MIS Quarterly. (16:2). pp. 173-186.
32. Lotto, R. De. (16 April 2001). Demographic Variation in Privacy Concerns. Gartner Advisory – Research and Advisory Services.
33. Louis Harris and Associates, Inc. (1990). The Equifax Report on Consumers in the Information Age. Equifax, Inc., Atlanta, GA.
34. Louis Harris and Associates, Inc. (1992). Harris Equifax Consumer Privacy Survey 1992. Equifax, Inc., Atlanta, GA.
35. Louis Harris and Associates, Inc. & Westin, A. (March 1998). BW/Harris Poll: Online Insecurity. Business Week. Available: http://www.businessweek.com/1998/11/b3569107.htm
36. Mabley, K. (2000) Privacy Vs. Personalization. Online. Internet. 2000. Available: http://www.cyberdialogue.com
37. Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E.A. (December 1995). Values, Personal Information Privacy Concerns, and Regulatory Approaches. Communications of the ACM (38:12). pp. 65-74.

38. Moon, Youngme. (March 2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers. Journal of Consumer Research (Vol 26) pp 323 – 339.
39. Morrison, D. E., Firmstone, J. (2000). The social function of trust and implications for e-commerce. International Journal of Advertising (19:5) pp. 599 – 623.
40. Profunda Software APS. Internet Statistic. Online. Internet. 31 July. 2000. Available: http://www.profunda.dk/resources/internet/internet_stats.html
41. Rai, Arun, Professor of eCommerce Institute, Georgia State University, Interview conducted on 11 May. 2001
42. Rosenberg, R. S. (12-13 June 1998). Privacy Protection on the Internet: The Marketplace Versus the State Wiring the World: The Impact of Information Technology on Society, IEEE Society on Social Implications of Technology, Indiana University South Bend. (pp. 138-147).
43. Rosenberg, R. S. (16 May 2000). Appearance Before the Senate Subcommittee on Communications Freedom of Information and Privacy Association of British Columbia.
44. Smith, H. J. (December 1993). Privacy Policies and Practices: Inside the Organizational Maze. Communications of the ACM (36:12). pp. 105-122.
45. Smith, H. J., Milberg, S. J., & Burke, S. J. (June 1996). Information Privacy: Measuring Individuals' Concerns About Organization Practices. MIS Quarterly 20(2). pp.167-196.
46. Stewart, K.A., Segars A.H., Grover, V., Fiedler, Kirk. (2001). A Model of Consumers' Perceptions of the Invasion of Information Privacy. Paper submitted to MIS Quarterly.
47. Stone, E. F. & Stone, D. L. (1990). Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms. Research in Personnel and Human Resources Management (8). K. M. Rowland and G. R. Ferris (eds.). JAI Press, Greenwich, CT. pp.349-411.
48. Straub, D. W., Jr. & Collins, R. W. (June 2000). Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy MIS Quarterly (14:2). pp.142-156.
49. Trempus, R. T. Online. Internet. 2000. Available: http://www.pbi.org/pbiaudio/internetupdate/trempus.htm.
50. Wang, H., Lee, M. & Wang, C. (March 1998). Consumer Privacy Concerns about Internet Marketing. Communications of the ACM (41:3). pp. 63-70.
51. Warren, S. D. & Brandeis, L. D. (March 1890). The Right to Privacy Harvard Law Review (4:5). pp. 193-220.
52. Westin, A. (1967). Privacy and Freedom. Atheneum, New York.
53. Westin, A. and Publisher. (1997). Privacy and American Business. "Whatever works" The American Public Attitudes Toward Regulation and Self-Regulation on Consumer Privacy Issues. Available: http://www.ntia.doc.gov/reports/privacy/selfreg1.htm
54. Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., & Fromkin, H. (September 1982). A Survey of Employee Perceptions of

Information Privacy in Organizations. Academy of Management Journal (25:3). pp. 647-663.

APPENDIX 1



The University of British Columbia

A study of Information Privacy Concerns in the context of Electronic Commerce

Study Objective:

This study is intended to understand the information privacy concerns from the consumers' perspective in an electronic commerce setting.

Your participation in this study will be greatly appreciated.

The success of this survey will depend on your participation. We would be grateful if you would take about 15 - 20 minutes to complete the survey. In this survey, you will be shown a series of questions related to several specific types of personal information. Please pay attention to the **types of personal information** being asked in each question.

Confidentiality is guaranteed.

Your response will be held in strictest confidence and data about individuals will not be divulged. Only consolidated data will be published. It is assumed that consent has been given to use the data collected once the questionnaire is completed.

Participation in this study is entirely voluntary. You may withdraw from the study at any time at your own discretion.

This research is part of the requirements for Andrew Kong's graduate degree.

Dr. Izak Benbasat
Division of Management of Information Systems
Faculty of Commerce and Business Administration
The University of British Columbia
Vancouver, B.C. Canada V6T 1Z2
izak@interchange.ubc.ca

Andrew Kong
Division of Management of Information Systems
Faculty of Commerce and Business Administration
The University of British Columbia
Vancouver, B.C. Canada V6T 1Z2
sykong@interchange.ubc.ca

Below are some statements about the collection, storage, and use of ***medical information*** in the context of *electronic commerce or the World Wide Web*.

Medical information includes (not limited to) information about states of one's health, treatments received, hospital records, etc.

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **medical** information.
1 2 3 4 5 6 7

B. All the **medical** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **medical** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **medical** information.
1 2 3 4 5 6 7

E. When companies ask me for **medical** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **medical** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **medical** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **medical** information.
1 2 3 4 5 6 7

I. Computer databases that contain **medical** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **medical** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **medical** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **medical** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **medical** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **medical** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **medical** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***financial information*** in the context of electronic commerce or the World Wide Web.

Financial information includes (not limited to) information about wages, family income, mortgages, loan applications, taxes, and others.

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **financial** information.
1 2 3 4 5 6 7

B. All the **financial** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **financial** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **financial** information.
1 2 3 4 5 6 7

E. When companies ask me for **financial** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **financial** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **financial** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **financial** information.
1 2 3 4 5 6 7

I. Computer databases that contain **financial** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **financial** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **financial** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **financial** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **financial** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **financial** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **financial** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***personal interest information*** in the context of electronic commerce or the World Wide Web:

Personal interest information (not limited to) includes attitudes toward the Internet, hobbies, special interests, ads/promotions responded, information about hobbies, which web sites users like to go, music preferences, and others

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **personal interest** information.
1 2 3 4 5 6 7

B. All the **personal interest** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **personal interest** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **personal interest** information.
1 2 3 4 5 6 7

E. When companies ask me for **personal interest** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **personal interest** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **personal interest** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **personal interest** information.
1 2 3 4 5 6 7

I. Computer databases that contain **personal interest** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **personal interest** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **personal interest** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **personal interest** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **personal interest** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **personal interest** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **personal interest** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***personal history information*** in the context of *electronic commerce or the World Wide Web*.

Personal history information includes (not limited to) name, age, birth date, education level, mailing address, and e-mail address.

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **personal history** information.
1 2 3 4 5 6 7

B. All the **personal history** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **personal history** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **personal history** information.
1 2 3 4 5 6 7

E. When companies ask me for **personal history** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **personal history** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **personal history** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **personal history** information.
1 2 3 4 5 6 7

I. Computer databases that contain **personal history** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **personal history** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **personal history** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **personal history** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **personal history** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **personal history** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **personal history** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***buying practices information*** in the context of *electronic commerce or the World Wide Web*.

Buying practices information includes (not limited to) information about buying habits, how often users buy online or offline, what types of thing users buy and others.

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **buying practices** information.
1 2 3 4 5 6 7

B. All the **buying practices** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **buying practices** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **buying practices** information.
1 2 3 4 5 6 7

E. When companies ask me for **buying practices** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **buying practices** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **buying practices** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **buying practices** information.
1 2 3 4 5 6 7

I. Computer databases that contain **buying practices** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **buying practices** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **buying practices** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **buying practices** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **buying practices** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **buying practices** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **buying practices** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of **demographic information** in the context of *electronic commerce or the World Wide Web*.

Demographic information includes (not limited to) information about gender, zip code, marital status, and race.

From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Notes:
Strongly Disagree *Strongly Agree*
1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **demographic** information.
1 2 3 4 5 6 7

B. All the **demographic** information in computer database should be double-checked for accuracy-no matter how much this costs.
1 2 3 4 5 6 7

C. Companies should not use **demographic** information for any purpose unless it has been authorized by the individuals who provided the information.
1 2 3 4 5 6 7

D. Companies should devote more time and effort to preventing unauthorized access to **demographic** information.
1 2 3 4 5 6 7

E. When companies ask me for **demographic** information, I sometimes think twice before providing it.
1 2 3 4 5 6 7

F. Companies should take more steps to make sure that the **demographic** information in their files is accurate.
1 2 3 4 5 6 7

G. When people give **demographic** information to a company for some reason, the company should never use the information for any other reason.
1 2 3 4 5 6 7

H. Companies should have better procedures to correct errors in **demographic** information.
1 2 3 4 5 6 7

I. Computer databases that contain **demographic** information should be protected from unauthorized access-no matter how much this costs.
1 2 3 4 5 6 7

J. It bothers me to give **demographic** information to so many companies.
1 2 3 4 5 6 7

K. Companies should never sell the **demographic** information in their computer databases to other companies.

1 2 3 4 5 6 7

L. Companies should devote more time and effort to verifying the accuracy of the **demographic** information in their databases.

1 2 3 4 5 6 7

M. Companies should never share **demographic** information with other companies unless it has been authorized by the individuals who provided the information.

1 2 3 4 5 6 7

N. Companies should take more steps to make sure that unauthorized people cannot access **demographic** information in their companies.

1 2 3 4 5 6 7

O. I'm concerned that companies are collecting too much **demographic** information about me.

1 2 3 4 5 6 7

Please select the appropriate answer to the questions asked:

1) Your age:

Below 18 years old ☐

18 - 22 years old ☐

23 - 27 years old ☐

28 - 32 years old ☐

33 - 37 years old ☐

38 - 42 years old ☐

43- 47 years old ☐

48 - 52 years old ☐

53 - 57 years old ☐

58 - 62 years old ☐

Above 62 years old ☐

2) Your education level:

High School ☐

Vocational/ Technical School ☐

Diploma ☐

Some college ☐

College Degree ☐

Graduate School ☐

Others ☐

3) Gender:

Male ☐

Female ☐

4) Primary Industry:

Accounting	☐	Finance	☐
Information Technology	☐	Health Care	☐
Arts	☐	Marketing	☐
Sciences	☐	Operation Research	☐
Human Resources	☐	Economics	☐
Others	☐	Engineering	☐

5) How long you have been using the Internet? (Emails, Webs, Telnet, etc.)

Less than 6 months	☐
6 - 12 months	☐
1 - 2 years	☐
3 - 4 years	☐
More than 5 years	☐

6) How often do you check out or read the privacy policy posted on the web sites you visit?

Read the privacy policy every time.	☐
Read the privacy policy often,	☐
Read the privacy policy once in a while.	☐
Read the privacy policy only on unreliable/never visited web sites	☐
Never read the privacy policy posted on web sites	☐

7) Do you think that regulation or law is the most appropriate method to deal with information privacy concern/issue on the Internet?

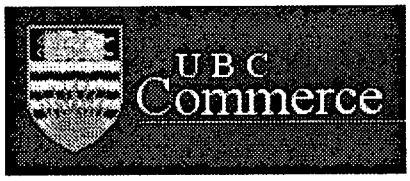
Yes ☐

No ☐

Undecided ☐

Thank you for participating in our research!

APPENDIX II



The University of British Columbia

A study of Information Privacy Concerns in the context of Electronic Commerce

Study Objective:

This study is intended to understand the information privacy concerns from the consumers' perspective in an electronic commerce setting.

Your participation in this study will be greatly appreciated.

The success of this survey will depend on your participation. We would be grateful if you would take about 15 - 20 minutes to complete the survey. In this survey, you will be shown a series of questions related to several specific types of personal information. Please pay attention to the **types of personal information** being asked in each question.

Confidentiality is guaranteed.

Your response will be held in strictest confidence and data about individuals will not be divulged. Only consolidated data will be published. It is assumed that consent has been given to use the data collected once the questionnaire is completed.

Participation in this study is entirely voluntary. You may withdraw from the study at any time at your own discretion.

This research is part of the requirements for Andrew Kong's graduate degree.

Dr. Izak Benbasat
Division of Management of Information Systems
Faculty of Commerce and Business Administration
The University of British Columbia
Vancouver, B.C. Canada V6T 1Z2
izak@interchange.ubc.ca

Andrew Kong
Division of Management of Information Systems
Faculty of Commerce and Business Administration
The University of British Columbia
Vancouver, B.C. Canada V6T 1Z2
sykong@interchange.ubc.ca

Below are some statements about the collection, storage, and use of ***medical information*** in the context of *electronic commerce or the World Wide Web*.

Notes: **Medical information** includes (not limited to) information about states of one's health, treatments received, hospital records, etc.

These are benefits of submitting **medical** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **medical** information:

- Relevant information and personal e-mails directly related to your health record
- Discounts or sales notices on drugs or prescriptions.
- Up to date information of treatments about particular health issues that you are interested in.
- Information about various life insurance plans offered by companies concerning your health condition.
- Information about your physician's practice history.
- Personal health care report/profile accessible online only by yourself.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **medical** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **medical** information.

1 2 3 4 5 6 7

B When companies ask me for **medical** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **medical** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **medical** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***financial information*** in the context of *electronic commerce or the World Wide Web*.

Notes: **Financial information** includes (not limited to) information about wages, family income, mortgages, loan applications, taxes, and others.

These are benefits of submitting **financial** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **financial** information:

- Relevant market information about mortgages or loan applications.
- Personal e-mails concerning financial advice or recommendations.
- Faster processing of credit card or loan applications.
- Information about brokerage firms research that might be of interest to you.
- Personal financial management services.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **financial** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **financial** information.

1 2 3 4 5 6 7

B. When companies ask me for **financial** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **financial** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **financial** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***personal interest information*** in the context of electronic commerce or the World Wide Web.

Notes: **Personal interest information** includes (not limited to) attitudes toward the Internet, hobbies, special interests, ads/promotions responded, information about hobbies, which web sites users like to go, music preferences, and others

These are benefits of submitting **personal interest** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **personal interest** information:

- Customized web sites according to your personal interest.
- Personal e-mails concerning recommendation of sites, products, or services that suit your personal interest or arrangement of clubs/communities related to one's personal interests.
- Up to date information about discount or sales information related to your own personal interest.
- Opportunity to download computer software or listen/download music related to your own preferences.
- Free coupons related to your personal interest such as special music events, conference, and others.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **personal interest** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **personal interest** information.

1 2 3 4 5 6 7

B. When companies ask me for **personal interest** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **personal interest** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **personal interest** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***personal history information*** in the context of *electronic commerce or the World Wide Web*.

Notes: **Personal history information** includes (not limited to) name, age, birth date, education level, mailing address, and e-mail address.

These are benefits of submitting **personal history** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **personal history** information:

- Customized interfaces of the web sites you visit.
- Personal e-mails concerning discounts, sales, and information that might interest you.
- Free e-mails accounts or free personal web sites from the companies.
- Submitting personal history information enables you to join online communities or online clubs.
- Information about job market or education opportunities available near your residential area.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **personal history** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **personal history** information.

1 2 3 4 5 6 7

B. When companies ask me for **personal history** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **personal history** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **personal history** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of ***buying practices information*** in the context of *electronic commerce or the World Wide Web*.

Notes: **Buying practices information** includes (not limited to) information about buying habits, how often users buy online or offline, what types of thing users buy and others.

These are benefits of submitting **buying practices** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **buying practices** information:

- Relevant e-mails about sales/discounts on the merchandise you are interested in.
- Detailed information about products that are related to your history of buying practices.
- Customized interfaces and Internet agents that can help track your favorite or relevant merchandise or goods.
- Recommendations or discounts from the web site.
- Digital coupons that you can download and print to be used for products related to your buying practices history.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **buying practices** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **buying practices** information.

1 2 3 4 5 6 7

B. When companies ask me for **buying practices** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **buying practices** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **buying practices** information about me.

1 2 3 4 5 6 7

Below are some statements about the collection, storage, and use of **demographic information** in the context of *electronic commerce or the World Wide Web*.

Notes: **Demographic information** includes (not limited to) information about gender, zip code, marital status, and race

These are benefits of submitting **demographic** information in the context of electronic commerce.

You may receive the following examples of benefits of submitting **demographic** information:

- Customized web sites according to your locations or even gender. For example, you will receive relevant information pertinent to the area you live such as news, weather report, and others.
- E-mails in regard to the information relevant to your own demographic information. This could be contemporary local news, women or men's health information, tips on marriage/being single, and others.
- Free e-mail accounts from the web sites.
- Extensive information services such as horoscope, entertainment news, or information about particular concerts within your residential area.

In addition to the above benefits, please write down up to 3 other benefits or information that you would like to receive for submitting **demographic** information:

-

-

-

Assuming that you will receive all the benefits and information shown and written above, please indicate the extent to which you, as an individual, agree or disagree with each statement by selecting the appropriate number.

Strongly Disagree *Strongly Agree*

1 2 3 4 5 6 7

A. It usually bothers me when companies ask for **demographic** information.

1 2 3 4 5 6 7

B. When companies ask me for **demographic** information, I sometimes think twice before providing it.

1 2 3 4 5 6 7

C. It bothers me to give **demographic** information to so many companies.

1 2 3 4 5 6 7

D. I'm concerned that companies are collecting too much **demographic** information about me.

1 2 3 4 5 6 7

Please select the appropriate answer to the questions asked:

1) Your age:

- Below 18 years old ☐
- 18 - 22 years old ☐
- 23 - 27 years old ☐
- 28 - 32 years old ☐
- 33 - 37 years old ☐
- 38 - 42 years old ☐
- 43- 47 years old ☐
- 48 - 52 years old ☐
- 53 - 57 years old ☐
- 58 - 62 years old ☐
- Above 62 years old ☐

2) Your education level:

- High School ☐
- Vocational/ Technical School ☐
- Diploma ☐
- Some college ☐
- College Degree ☐
- Graduate School ☐
- Others ☐

3) Gender:

Male ☐

Female ☐

4) Primary Industry:

Accounting	☐	Finance	☐
Information Technology	☐	Health Care	☐
Arts	☐	Marketing	☐
Sciences	☐	Operation Research	☐
Human Resources	☐	Economics	☐
Others	☐	Engineering	☐

5) How long you have been using the Internet? (Emails, Webs, Telnet, etc.)

Less than 6 months ☐

6 - 12 months ☐

1 - 2 years ☐

3 - 4 years ☐

More than 5 years ☐

6) How often do you check out or read the privacy policy posted on the web sites you visit?

Read the privacy policy every time.	☐
Read the privacy policy often,	☐
Read the privacy policy once in a while.	☐
Read the privacy policy only on unreliable/never visited web sites	☐
Never read the privacy policy posted on web sites	☐

7) Do you think that regulation or law is the most appropriate method to deal with information privacy concern/issue on the Internet?

Yes	☐
No	☐
Undecided	☐

Thank you for participating in our research!