

An Empirical Investigation of Internet Privacy:
Customer Behaviour, Companies' Privacy Policy Disclosures, and a Gap

by

Won Gyun No

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Management Sciences

Waterloo, Ontario, Canada, 2007

© Won Gyun No 2007

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Won Gyun No

Abstract

Privacy emerges as a critical issue in an e-commerce environment because of a fundamental tension among corporate, consumer, and government interests. By reviewing prior Internet-privacy research in the fields of information systems, business, and marketing published between 1995 and 2006, we consider the following research questions: 1) how an individual's privacy behaviour is affected by privacy policy disclosures and by the level of the individual's involvement regarding the sensitivity of personal information; 2) how companies' privacy policies vary with respect to regulatory approaches and cultural values; and 3) whether there is a gap between the privacy practices valued by individuals and those emphasized by companies. A three-stage study is conducted to answer these questions.

The first two stages, consisting of a Web-based survey and an online ordering experiment with 210 participants, found that individuals are more likely to read the privacy policy statements posted on Web sites and less likely to provide personal information, when they are under a high privacy involved situation as compared to being in a low privacy involved situation. However, the existence of a privacy seal did not affect individuals' behaviour, regardless of involvement conditions. This study also found a gap between self-reported privacy behaviour and actual privacy behaviour. When individuals were requested to provide personal information, their privacy policy statement reading behaviour was close to their self-report behaviour. However, their personal information providing behaviour was different from their self-reported behaviour.

The third stage, which entailed the study of 420 privacy policies spanning six countries and two industries, showed that privacy policies vary across countries, as well as with varying governmental involvement and cultural values in those countries. Finally, the analysis of all the three stages revealed a gap between individuals' importance ratings of companies' privacy practices and policies that companies emphasize in their privacy disclosures.

Acknowledgements

I would like to express my sincere appreciation for the continuous assistance and support which I received from both of my advisors, Dr. Efrim Boritz and Dr. R. P. Sundarraj. Throughout the years of my graduate training, Dr. Boritz and Dr. Sundarraj have shared with me their unique approach to working on research problems, an approach of critical thinking, careful examination, and the determination to get the essence of the problem. They were always encouraging when things looked impossible, and never seemed to falter in their faith in me. They helped me to succeed in spite of myself. I am endlessly indebted to Dr. Boritz and Dr. Sundarraj for their creative ideas and their invaluable guidance.

I would also like to thank my loving family and my parents. This work would not have been possible without their continuous support, both financial and emotional. They have been tremendously caring and understanding throughout all these years. It was a long haul, but it is finally done.

I would like to thank my examination committee members, Dr. Scott Jeffrey, Dr. Rod McNaughton, Dr. John Michela, and Dr. Steve G. Sutton, for their creative suggestions and all the time and effort invested into understanding this work.

I would be grateful for the vital contribution of 267 UW students who participated in my study as well as twelve graduate students who conducted the company Web site survey.

Finally, I would like to express my great appreciation to University of Waterloo Centre for Information System Assurance (UWCISA) for financial support during the years of my Ph.D. training.

Table of Contents

| | |
|--|------|
| ABSTRACT | iii |
| ACKNOWLEDGEMENTS | iv |
| TABLE OF CONTENTS | v |
| LIST OF TABLES | viii |
| LIST OF FIGURES | ix |
| INTRODUCTION | 1 |
| 1. PRIVACY IN E-COMMERCE | 5 |
| 1.1. HOW COMPANIES COLLECT PERSONAL INFORMATION | 5 |
| 1.2. INTERNET PRIVACY AND PRIVACY CONCERNS | 6 |
| 1.3. DEFINITION OF INTERNET PRIVACY IN E-COMMERCE | 8 |
| 2. LITERATURE REVIEW | 10 |
| 2.1. STUDIES INCLUDED IN THE REVIEW | 10 |
| 2.2. PRIVACY RESEARCH FRAMEWORK | 11 |
| 2.3. REVIEW AND RESEARCH OPPORTUNITIES | 13 |
| 2.3.1. Customer Perspective | 13 |
| 2.3.2. Company Perspective | 20 |
| 2.3.3. Government Perspective | 23 |
| 2.3.4. Customer–Company Interaction | 25 |
| 2.3.5. Customer – Government Interaction | 29 |
| 2.3.6. Company – Government Interaction | 31 |
| 2.3.7. Customer – Company – Government Interaction | 33 |
| 2.3.8. Other Factors | 34 |
| 2.4. THE PURPOSES OF THE STUDY | 37 |
| 3. INTERNET PRIVACY AND INDIVIDUAL PRIVACY BEHAVIOUR: PRIVACY BEHAVIOUR STUDY | 39 |
| 3.1. ELABORATION LIKELIHOOD MODEL (ELM) | 40 |
| 3.2. INVOLVEMENT AND PRIVACY BEHAVIOUR | 41 |
| 4. INTERNET PRIVACY AND COMPANIES’ PRIVACY PRACTICES: PRIVACY POLICY DISCLOSURE STUDY | 46 |
| 4.1. PRIVACY POLICY DISCLOSURES, INDUSTRY, AND COUNTRY | 46 |

| | | |
|--------|--|-----|
| 4.2. | PRIVACY POLICY DISCLOSURES AND REGULATORY APPROACHES | 48 |
| 4.3. | PRIVACY POLICY DISCLOSURES AND CULTURE | 51 |
| 5. | A GAP IN PERCEIVED IMPORTANCE OF COMPANIES' PRIVACY POLICIES: PRIVACY GAP STUDY | 57 |
| 6. | RESEARCH METHODOLOGY | 61 |
| 6.1. | AN OVERVIEW OF RESEARCH STAGES | 61 |
| 6.2. | PRIVACY BEHAVIOUR STUDY | 62 |
| 6.2.1. | Procedures | 62 |
| 6.2.2. | Design and Manipulation | 65 |
| 6.2.3. | Measurement | 69 |
| 6.2.4. | Participants | 72 |
| 6.3. | PRIVACY POLICY DISCLOSURE STUDY | 73 |
| 6.3.1. | Procedures | 73 |
| 6.3.2. | Survey Items | 75 |
| 6.3.3. | Measures | 77 |
| 6.4. | PRIVACY GAP STUDY | 79 |
| 7. | RESEARCH RESULTS | 81 |
| 7.1. | INTERNET PRIVACY STUDY | 81 |
| 7.1.1. | Manipulation Checks | 81 |
| 7.1.2. | Descriptive Statistics | 82 |
| 7.1.3. | Self-reported Privacy Behaviour | 85 |
| 7.1.4. | Actual Privacy Behaviour | 91 |
| 7.1.5. | Self-reported versus Actual Privacy Behaviour | 96 |
| 7.2. | PRIVACY POLICY DISCLOSURE STUDY | 97 |
| 7.2.1. | General Profile | 97 |
| 7.2.2. | Differences in Privacy Policy Disclosures across Industries and Countries | 101 |
| 7.2.3. | Analysis of Each OECD Principle | 102 |
| 7.2.4. | Government Involvement and Privacy Policy Disclosures | 107 |
| 7.2.5. | Cultural Values and Privacy Policy Disclosures | 109 |
| 7.3. | PRIVACY GAP STUDY | 110 |
| 7.3.1. | Important Companies' Privacy Policies that Individuals Want to Know | 110 |

| | |
|--|-----|
| 7.3.2. Frequently Addressed OECD Principles in Companies' Privacy Policy Disclosures | 113 |
| 7.3.3. Gap in Perceived Importance of OECD Principles | 115 |
| 8. DISCUSSION | 118 |
| 8.1. SUMMARY OF FINDINGS..... | 118 |
| 8.2. IMPLICATIONS | 122 |
| 8.3. LIMITATIONS AND FUTURE RESEARCH..... | 125 |
| 9. CONCLUSION..... | 128 |
| REFERENCES..... | 130 |
| APPENDIX I: AN ANNOTATED BIBLIOGRAPHY OF 74 KEY STUDIES..... | 138 |
| APPENDIX II: INTERNET PRIVACY USER SURVEY QUESTIONNAIRE..... | 154 |
| APPENDIX III: ONLINE EXPERIMENTAL SITE | 176 |
| APPENDIX IV: DEBRIEFING QUESTIONNAIRE..... | 184 |
| APPENDIX V: LIST OF 420 WEB SITES | 190 |
| APPENDIX VI: PRIVACY POLICY DISCLOSURE SURVEY | 202 |

List of Tables

| | |
|--|-----|
| Table 1: Experimental Design..... | 65 |
| Table 2: Privacy Behaviour Measurement Items..... | 70 |
| Table 3: Guideline and Detailed Comment of Use Limitation Principle..... | 76 |
| Table 4: Survey Questions for Use Limitation Principle..... | 76 |
| Table 5: Culture and Government Involvement Measures..... | 77 |
| Table 6: Eight Principles of OECD Guideline and Survey Questions..... | 78 |
| Table 7: Demographic Information of Participants..... | 82 |
| Table 8: Means and Standard Deviations for Self-reported Privacy Behaviour..... | 85 |
| Table 9: Analysis of Variance for Self-reported Privacy Behaviour..... | 86 |
| Table 10: Analysis of Variance for Self-reported Privacy Behaviour..... | 88 |
| Table 11: Chi-square Analysis of Actual Reading Behaviour..... | 92 |
| Table 12: Analysis of Variance for Time Spending to Read Privacy Policy Statement..... | 92 |
| Table 13: Chi-square Analysis of Actual Providing Behaviour..... | 93 |
| Table 14: Logistic Regression Predicting Actual Providing Behaviour..... | 94 |
| Table 15: Descriptive Statistics of Respondents' Behaviour With Respect to Privacy Seal..... | 95 |
| Table 16: Company Profile..... | 99 |
| Table 17: Participation in Privacy Seal Programs and Adoption of Technologies (P3P)..... | 100 |
| Table 18: OECD Principle Score between Non-sensitive and Sensitive Industry across Countries..... | 101 |
| Table 19: Analysis of Variance for OECD Principle as Function of Country and Industry..... | 102 |
| Table 20: Means and Standard Deviations for OECD Principles between Non-sensitive and Sensitive Industry across Countries..... | 104 |
| Table 21: Analysis of Variance for Eight OECD Principles as Function of Country and Industry.. | 106 |
| Table 22: Analysis of Variance for OECD Principle Score as Function of Governmental Involvement..... | 108 |
| Table 23: Means, Standard Deviations, and Intercorrelation for OECD Principle Score..... | 109 |
| Table 24: Individual's Perceived Importance of OECD Principles..... | 112 |
| Table 25: Proportion Score of OECD Principles..... | 114 |
| Table 26: Rank Order of OECD Principles..... | 116 |
| Table 27: Summary of Study Findings..... | 118 |

List of Figures

| | |
|--|----|
| Figure 1: A Privacy Research Framework | 12 |
| Figure 2: Level of Governmental Involvement in Corporate Privacy Management..... | 50 |
| Figure 3: Three Research Stages with Hypotheses | 61 |
| Figure 4: Involvement Manipulation Check | 64 |
| Figure 5: Detailed link between Internet privacy user survey and Online Ordering Experiment..... | 66 |
| Figure 6: Involvement Manipulation..... | 67 |
| Figure 7: Privacy Policy Disclosure Manipulation | 68 |
| Figure 8: Trustworthiness of Organizations and Privacy Concern Measure..... | 84 |

Introduction

Recent advances in computer and communication technology have influenced the way business is conducted. The Internet, especially the World Wide Web (Web), enables companies to reach potential customers through their Web sites. It also allows them to efficiently collect their customers' personal information. Many companies currently collect, store, and exchange personal information and use it to carry out their marketing strategies. As e-commerce environments become more sophisticated and interactive, the increased collection and use of customers' personal information allows companies to gain greater expertise in the evaluation of consumer behaviour.

However, the simplicity of information collection and use, coupled with the readily available personal information on the Internet also makes it easier and more tempting for companies to intrude on customers' personal information. Therefore, privacy is becoming one of the main concerns of customers while they are shopping over the Internet (Porter, 2000; Smith et al., 1996). Several public opinion polls reveal increasing levels of concern about privacy among Internet users (Business Week, 2000; Culnan, 1999; Culnan and Armstrong, 1999; FTC, 2000; Harris Interactive, 2003; Louis Harris and Associates and Westin, 1996; UNISIS, 2006; UPI, 2007; Zogby, 2007).

The growing privacy concerns of customers are resulting in companies paying increased attention to privacy (Culnan, 2000; Culnan and Armstrong, 1999; Shapiro and Baker, 2001). The main challenge to e-commerce companies is to balance the competitive advantages provided by the use of personal information with the privacy concerns that customers may raise with respect to the use of their personal information (Culnan and Armstrong, 1999). In other words, to survive in an extremely competitive e-commerce environment, corporations need to improve customer retention and build strong customer relationships through personalized services by using customers' personal information, but they must also be required to make a considerable effort to satisfy customers' privacy concerns.

Researchers have addressed the impact of privacy on consumers, companies, and society over the past decade and have identified a number of issues related to Internet privacy. For instance, one stream of previous research has examined companies' practices with respect to the privacy policy disclosures on their Web sites (e.g., Desai et al., 2003; Liu and Arnett, 2002; Milne and Culnan, 2002). Another stream has investigated the relationship between privacy concerns and customer behaviour (e.g., Earp and Baumer, 2003; George, 2004; Graeff and Harmon, 2002; Phelps et al., 2000). Still another stream has examined the relationship between factors affecting privacy concerns and customer behaviour (e.g., Ackerman et al., 1999; Earp and Baumer, 2003; Koyuncu and Lien, 2003; Phelps et al., 2001).

Although previous studies have made important contributions to our understanding of privacy issues, there is still much to learn about customers' actual behaviour and companies' current practices related to Internet privacy. Our current understanding of these interrelationships is somewhat limited and is based primarily on anecdotal evidence. It is particularly essential for researchers to understand how companies respond to their customers' privacy concerns and how the customers' response to the companies' actions influences online customer behaviour.

This study investigates several research questions that have not been addressed by previous literature. In particular, the main relationships among customer, company, and government are addressed. First, it examines the effect of privacy policy disclosures (i.e., privacy policy statement and privacy seal) and individuals' level of involvement with respect to the sensitivity of personal information on their privacy behaviour. In this regard, self-reported privacy behaviour and actual privacy behaviour are compared. Two privacy behaviours are investigated in this study: 1) the process of searching and evaluating information about companies' privacy policies and 2) making a decision whether to disclose personal information. Second, privacy policy disclosures are examined to see the differences in companies' privacy policies across countries and industries and to identify the effect of governmental involvement and cultural values on companies' privacy policy disclosures. Finally, this study investigates whether there is a gap

between companies' privacy practices that individuals value and what companies emphasize in their privacy policy statements.

The analysis of the Web-based survey and the online ordering experiment involving 210 participants indicated that the level of individuals' involvement regarding the sensitivity of personal information requested influences individuals' privacy policy statement reading behaviour as well as their personal information providing behaviour. However, the content of the privacy policy statement and the existence of a privacy seal did not influence individuals' privacy behaviour. The results of the analysis also revealed that when individuals were requested to provide personal information, their privacy policy statement reading behaviour was close to their self-report behaviour. However, their personal information providing behaviour was different from their self-reported behaviour. Furthermore, the findings from the analysis of 420 companies' privacy policy disclosures suggested the difference in companies' privacy policies across countries as well as the effect of governmental involvement and cultural values on companies' privacy policy disclosures. This study also found a gap between individuals' importance ratings of companies' privacy practices and privacy policies that companies emphasize in their privacy policy disclosures.

The results of this study are expected not only to contribute to our understanding of individuals' privacy behaviour and companies' privacy policy disclosures but also to broaden our knowledge of how companies perceive customers' privacy and how they protect their customers' privacy. Hence, they will provide a basis for identifying specific situations in which privacy policy disclosures are perceived as useful as well as strategies which can reduce their customers' privacy concerns by emphasizing matters which customers consider most important.

The study is organized as follows. Following this brief introduction, chapter 1 provides a brief discussion on privacy issues in e-commerce. In chapter 2, the study introduces a privacy research framework based on a review of over 80 Internet privacy studies in the fields of information systems, business, and marketing published between 1995 and 2006. The study also discusses gaps in our current understanding of Internet privacy which represent future research opportunities. In

chapter 3 through 5, a total of 19 hypotheses are developed, addressing such gaps with respect to individuals' privacy behaviour, companies' privacy disclosures, and a difference between what individuals value and what companies' privacy policies emphasize. Chapter 6 discusses the details of the research methods used, including a description of Web-based user survey, online ordering experiment, Web site survey, participants, and research instruments. The results of the study are presented in chapter 7. A brief summary of findings, the implications of the findings, and the limitations of the study are discussed in chapter 8. Finally, the thesis concludes with brief concluding remarks.

1. Privacy in E-commerce

Generally, in e-commerce, a customer who wants to buy a product searches the Internet and finds a company which sells the product. Next, the customer places an order for the product through the company's Web site. During this ordering process, companies have many opportunities to collect and use customer information. By using customers' personal information, companies not only want to gain greater expertise in the evaluation of consumer behaviour but also achieve comparative advantage in the future (i.e., when multiple vendors provide the same products, a customer may select a vendor that he or she had good experience). Although personal information can be used to provide better services through customization, it also can create privacy issues in e-commerce due to inappropriate company practices such as information collection without consent, unauthorized information transfer, and misuse of personal information. This section is intended to address general privacy issues, such as reasons that companies collect personal information, and customers' privacy concerns in e-commerce. Also, the definition of Internet privacy used for this study is discussed.

1.1. How Companies Collect Personal Information

There are a number of ways through which companies can gather customers' personal information. The easiest way is during a registration or ordering process. For instance, companies usually request personal information such as name, address, phone number, and credit card number to complete billing information. Later, companies customize their products and services to match the customer's preferences by using the information provided. However, this approach does not allow the companies to collect information beyond demographics.

Companies often require attitudinal and behavioural information for more precise customization. Another approach is to capture customers' IP (Internet Protocol) addresses.¹ Using

¹ An IP address is an address assigned to a computer that is connected to the Internet. Using an IP address, one computer can request or send information to the other.

the customer's IP address, companies can track the specific Web pages the customer has viewed and the sequence of the Web pages the customer visited. Although information gathering using IP address allows companies to capture additional behavioural information, the primary limitation of an IP address is that it does not provide a means through which companies can link to specific customer information such as demographic data or preference data.

A third approach is to gather customers' personal information by the use of a 'Cookie.'² A cookie contains information that a Web server passes to the customer's Web browser to help the server identify the customer. The customer's preferences and behavioural information are tracked and stored in the cookie. Later, the company accesses the cookie to obtain valuable information about their customer's traits and preferences and uses the information for better customization. Through personalization, companies hope to improve customer retention, to build a good customer relationship, to achieve strong competitive advantage, and to increase revenue.

1.2. Internet Privacy and Privacy Concerns

There are three main reasons for e-commerce companies to collect personal information as compared to any traditional brick-and-mortar business. First, the relatively low barriers to entry make e-commerce both attractive and competitive. The competitive e-commerce environment is forcing companies to collect a vast amount of personal information for customizing their products and services, so that they can differentiate themselves through improved customer relationships and increase sales. Second, customers are requesting one-to-one communication and personalized services (Gurau *et al.*, 2003). Finally, advances in information technology have made it possible not only to capture personal information at the point of sale but also to track customers' behaviour including their keystrokes and mouse clicks. This form of tracking gives companies knowledge of

² A cookie is a file that is stored in a customer's computer.

customer behaviour such as the Web pages that customers have viewed and the activities performed on the Web pages.

Although this information gathering can aid marketing tactics in an e-commerce setting, it certainly raises numerous concerns about privacy. Unless it is adequately protected, customers' personal information can be used for purposes that could seriously harm their interests. For instance, companies can obtain personal information from customers by offering services such as free e-mail and customized news. Then, they sell, trade, or share that information among third-party companies without the consumers' expressed knowledge or consent. Customer privacy can also be seriously compromised by security breaches.

A number of approaches have been discussed over the past several years to deal with Internet privacy. The most common three approaches for dealing with concerns about Internet privacy are governmental regulation, industry self-regulation, and privacy-enhancing technologies. Many countries including the United Kingdom, Germany, and Canada have enacted privacy legislation governing the collection, use, and transfer of personal information as well as the transfer of such information to other countries that have not adopted similar privacy protection legislation. On the other hand, some countries, such as the United States, have taken a more liberal industry self-regulation approach. Under the industry self-regulation approach, each company is responsible for deciding on the degree of information that is collected and used and for developing its own privacy policy statement aligned with its industry guidelines. Government agencies only get involved in egregious breaches of privacy.³ The third approach relies on technologies such as the Platform for

³ For example, in 1999, DoubleClick, a leading provider of comprehensive Internet advertising solutions for marketers, announced that it was buying Abacus Direct, the largest direct marketing database in the United States, and was planning to merge Abacus's purchasing database with its customer online profiles. Privacy opponents worried about the corporate abuse of customer data by bring together Web surfing habits obtained from the banner ads DoubleClick serves and personally identifiable customer catalogue transactions recorded by Abacus. In February 2000, a complaint against DoubleClick was filed with the Federal Trade Commission (FTC) by the Electronic Privacy Information Center (EPIC). In July 2000 the FTC came to an agreement with the Network Advertisers Initiative (NAI), a group consisting of the largest online advertisers including DoubleClick, which allows for online profiling and any future merger of databases if it obtains "opt-out" consent.

Privacy Preferences (P3P) and Anonymizer (www.anonymizer.com) to protect customers' privacy. P3P is a standardized, machine readable protocol, which is used for implementing privacy practices. It was designed to block access to Web sites or automatically notify online users if a Web site's privacy policy is not in line with their pre-specified privacy preferences; the consumer is then left to decide whether he or she still wants to use the service. Anonymizer is Web site browsing software that enables individuals to browse Web pages with complete anonymity, so that their personal information is not available to the Web sites that they are browsing.

1.3. Definition of Internet Privacy in E-commerce

Many different disciplines have been interested in and have examined the topic of privacy. These research activities, however, use various definitions of privacy and thus create much difficulty in relating one study to another (see Burgoon (1982) for various definitions of privacy). According to Burgoon (1982), privacy encompasses various dimensions: physical privacy, psychological privacy, social privacy, and information privacy. Physical privacy is related to the concepts of personal space and territoriality. It implies the degree to which an individual is physically accessible to others. Psychological privacy is about the ability of an individual to control cognitive inputs and outputs to determine with whom and under which conditions he or she shares thoughts and reveals information about himself or herself. Social privacy indicates an individual's ability to engage in or to withdraw from social interaction. Informational privacy implies an individual's ability to determine what, when, and how his or her personal information will be released to another person or group.

Depending on the context and situation, one can view the privacy dimension differently and hence arrive at a different definition. For instance, one of the earliest, often quoted definitions is "the right to be let alone" (Warren and Brandeis, 1890). For Westin (1967, p. 7), privacy is "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." On the other hand, Altman (1975, p. 24) defines

privacy as “the selective control of access to the self.” For Bellotti (1997, p. 89), privacy is “a capability to determine what one wants to reveal and how accessible one wants to be.” In short, there is no agreement on what exactly privacy constitutes and for what reason.

This study defines and considers privacy from an e-commerce perspective. When it is associated with the customer activities that take places in e-commerce, the notion of privacy is usually related to personal information, and the invasion of privacy is commonly viewed as the unauthorized collection, use, and transfer of personal information as a direct result of e-commerce transactions (Milberg et al., 2000; Petty, 2000; Rezgui et al., 2003). The flow of computerized data and information is a prerequisite for business transactions, and it plays an important role in these transactions. Prior research shows that individuals are willing to disclose personal information in exchange for some economic and social benefits. That is, people disclose personal information after assessing the risks of disclosure: whether their personal information will subsequently be used fairly and they will not suffer negative consequences (Laufer and Wolfe, 1977; Stone and Stone, 1990). Therefore, privacy in e-commerce can be seen as an individual’s ability to control the collection, use, and transfer of his or her personal information. It is also reasonable to expect that information privacy is the primary privacy dimension in e-commerce. In line with this idea, this study excludes the physical, psychological, and social dimensions and focuses on information privacy. The following is the definition of Internet privacy used throughout the study.⁴

Internet privacy is the individuals’ ability to access and control their personal information with respect to collection, use, and transfer over the Internet.

⁴ Internet privacy and online privacy are used interchangeably in this paper.

2. Literature Review

Privacy emerges as a critical issue in an e-commerce environment because of a fundamental tension between corporate and consumer interests. Companies need to collect and use personal information to remain competitive while customers worry about the inappropriate collection and use of their personal information. Throughout the following subsections, the paper provides an overview of prior research on Internet privacy in the field of information systems, business, and marketing. Following a comprehensive review of the literature on privacy, a privacy research framework is introduced.

2.1. Studies included in the Review

The studies included in the review were selected based on several criteria. First, the review considers works from the year 1995 to the year of 2006.⁵ Second, the review is derived from the studies involving research in Internet privacy that examines privacy as a dependent or independent variable in their research model. Finally, the review includes qualitative research works which address Internet privacy such as privacy protection technologies and privacy regulation.

Because the privacy issues in an e-commerce environment depend on the context in which the information is revealed by customers and collected and used by companies, the review includes studies that investigate various dimensions of Internet privacy. However, several empirical studies that did not meet the above mentioned criteria are not included in the review. The review especially excludes studies that investigate the privacy of health information because the relationship between customers and companies in the health industry significantly differs from that of customers and e-commerce companies. For example, the personal information asked of patients in a hospital is more

⁵ Although an extensive search for prior studies has been carried out, this study is not claiming that this overview incorporates all possible research results available to date. The studies were collected through databases such as ProQuest and The ACM Digital Library as well as through several search engines such as Google Scholar.

sensitive information (e.g., medical records such as HIV/AIDS) than the information asked of customers in an online store. Furthermore, patients have limited opportunity to provide false information to the hospital while customers in an online retail store can easily fabricate their information (e.g., false email address and telephone number). As a result, a total of 88 studies are selected for the review. An annotated bibliography of 74 key studies that are included in this review is provided in the Appendix I.

2.2. Privacy Research Framework

A privacy research framework was developed to classify prior studies and to identify research opportunities that could be addressed in future research. The framework is organized around three main entities involved in Internet privacy: customers, companies, and governments.⁶

Customers are the main source of personal information. They may adopt privacy-enhancing actions (e.g., avoiding disclosure of personal information or providing false information) or privacy technologies (e.g., P3P software) or both to protect their privacy. Their privacy concerns influence companies' privacy practices as well as government regulation. Companies are the biggest consumers of personal information. They use personal information to deliver products, study customer profiles, and offer personalized services. In response to customers' increasing privacy concerns, companies may implement privacy protections such as privacy policy statements and privacy seals, and their privacy practices influence customers' privacy concerns and government regulations. Governments play two important but conflicting roles related to Internet privacy.

⁶ Three main entities were identified based on the analysis of 84 studies that addressed Internet privacy in e-commerce between 1995 and 2006. This study analyzed each study's research hypotheses. The results indicated that the hypotheses of 88 studies mainly examined three factors (i.e., customer, company, and government). That is, among 88 studies, 52 studies had hypotheses with respect to customer (e.g., how customers' privacy concerns influence their behaviour), 27 studies had hypotheses related to company (e.g., whether companies post privacy disclosures and the disclosures reflect fair information practices), and 14 studies had hypotheses regarding government (e.g., whether regulatory approaches influence companies' privacy practices.). Furthermore, several studies addressed all three entities as major stakeholders involved in Internet privacy (e.g., Culnan and Bies, 2003; Milberg et al., 2000; Milne, 2000).

Governments may seek to protect citizens' privacy but, at the same time, may need to use citizens' personal information to monitor and control individuals. To protect customer privacy, governments may promote privacy laws, oversee the implementation of these laws, educate the public about privacy issues, and encourage industry self-regulation. Such government activities affect customers' privacy concerns and companies' privacy practices.

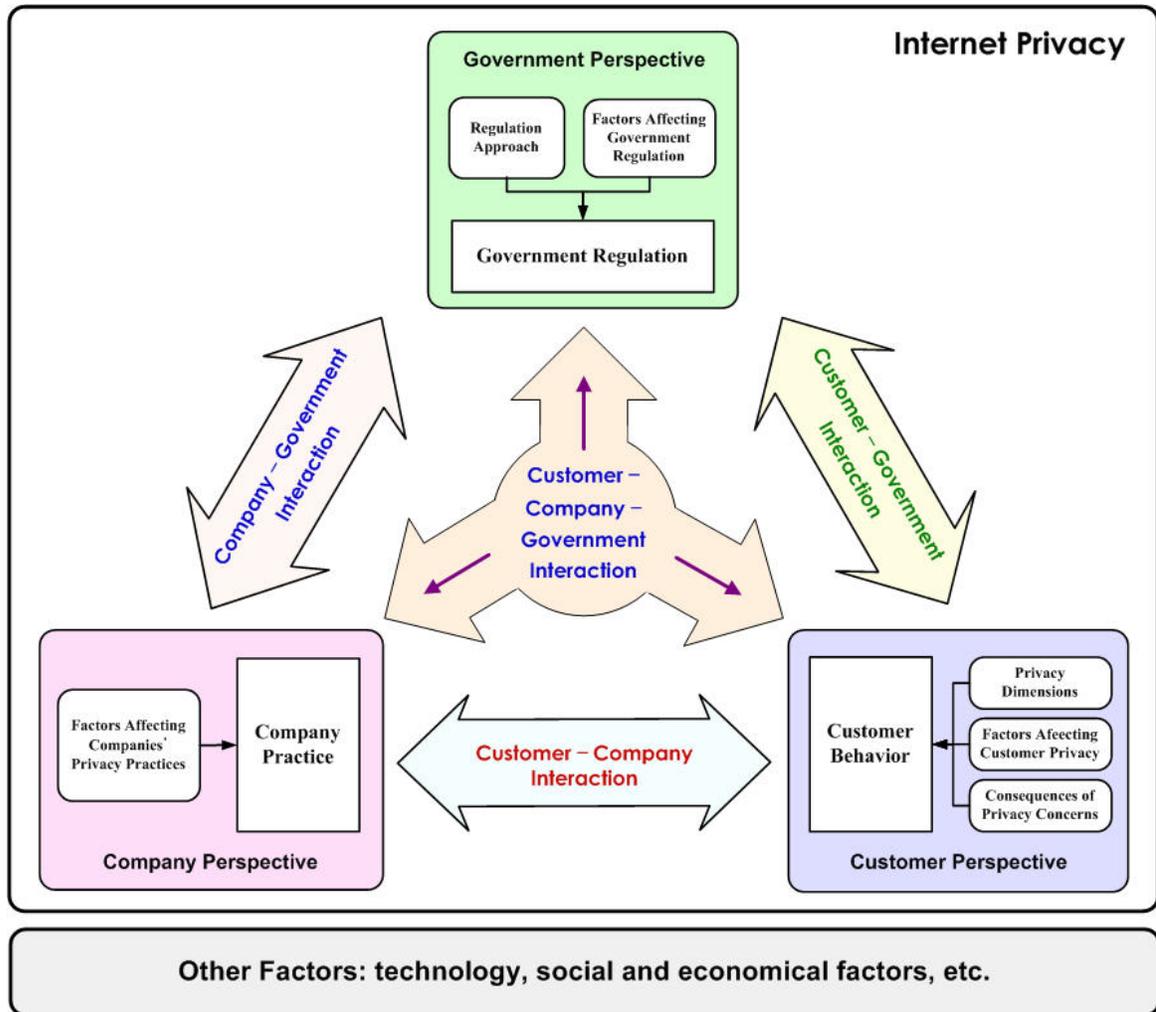


Figure 1: A Privacy Research Framework

The framework presented in Figure 1 shows all possible interactions between the three entities as well as the relationships between each entity and its influential factors.⁷ The framework suggests eight major research areas in Internet privacy: (1) privacy and customer perspective, (2) privacy and company perspective, (3) privacy and government perspective, (4) customer-company interaction, (5) customer-government interaction, (6) company-government interaction, (7) customer-company-government interaction, and (8) privacy and other factors. In the next section, this framework is used to discuss relevant literature and address directions for future research.⁸

2.3. Review and Research Opportunities

2.3.1. Customer Perspective

Public opinion polls have revealed a general desire among Internet users to protect their privacy (e.g., Business Week, 2000; Culnan, 1999; Harris Interactive, 2002, 2003). Prior studies have investigated three key privacy issues 1) what are the major dimensions of customers' privacy concerns, 2) what are the antecedent factors affecting such concerns, and 3) what are the consequences of customers' privacy concerns.

2.3.1.1. The Dimensions of Customers' Privacy Concerns

Prior literature has examined whether individuals' general attitudes about online privacy are constant or differ depending on the situation (e.g., Ackerman et al., 1999; Sheehan, 2002; Westin, 2003). Westin proposed a typology of individuals' concerns about privacy (Louis Harris and Associates and Westin, 1994, 1998; Westin, 2003). He argued that individuals can be categorized

⁷ The various interactions and relationships in the framework are identified from prior studies. While each study has its own unique focus, the studies can collectively provide an extensive perspective on Internet privacy. Admittedly, creating this extensive perspective may oversimplify prior studies and, more importantly, may subjectively classify a study as either an interaction or a relationship.

⁸ Only some of studies are discussed in this section due to the similarity among studies. For the sake of brevity, this study discusses only a few specific studies which are representative of the areas discussed in similar research.

into three groups: privacy fundamentalists, privacy unconcerned, and privacy pragmatists. The *privacy fundamentalists* are defined as being extremely concerned about the use of their personal information and are unwilling to provide their information. Individuals in the *privacy unconcerned* group do not take their privacy into consideration and are willing to provide their personal information. The *privacy pragmatists* are concerned about their privacy, but less than privacy fundamentalists. Sheehan (2002) examined whether online users privacy concerns fit well into Westin's typology. She measured individuals' privacy concerns using 15 statements (i.e., scenarios) that represent 5 different privacy influences that have been identified by prior literature (i.e., awareness, usage, sensitivity, familiarity, and compensation). The analysis of an email survey of 889 U.S. online users indicated that online users actually fell into four distinct categories: unconcerned Internet users, circumspect Internet users, wary Internet users, and alarmed Internet users.

Another set of studies investigated differences in privacy concerns across different cultures and countries. For instance, Milberg et al. (1995) examined whether nationality, information privacy regulatory approaches, and cultural values influence the level of information privacy concern. Their survey of approximately 900 members of the Information Systems Audit and Control Association (ISACA) in roughly 30 countries found that the overall level of privacy concern for personal information varies across countries; for instance, individuals from Thailand have the lowest level of privacy concern, and those from Canada have the highest privacy concern. Milberg, Smith, and Burke (2000) also examined the relation between cultural values and privacy concerns. Unlike Milberg et al. (1995), their results indicated that cultural values are associated with differences in levels of customers' privacy concerns as well as differences in regulatory approaches.⁹

Milne and Boza (1999) found that consumers' concerns about privacy varied by industry: banks, insurance, telephone, and credit card industries generated high privacy concerns; Internet

⁹ Milberg et al.(2000) conducted an analysis of privacy regulations of several countries. The results revealed a broad divergence of approaches to the governance of information privacy: self-help, voluntary control, data commissioner, registration, and licensing.

access, magazines, and catalogue companies generated moderate levels of privacy concerns; and airlines, bookstores, and video stores generated the lowest privacy concerns.

Dhillon and Moores (2001) examined major issues that could point to individuals' potential concerns with respect to Internet privacy. Based on the brainstorming results of two panels (11 experts and 16 IS executives), they identified the five most important Internet privacy concerns (e.g., companies should eliminate spam and not sell personal information). Dhillon and Moores also identified eighteen means to address these fundamental Internet privacy concerns (e.g., enact stronger laws to protect consumer privacy and make spam illegal).

2.3.1.2. Antecedents of Customers' Privacy Concerns

Two frequently-mentioned factors influencing customer's privacy concerns are the type of information (e.g., demographics versus financial data) and the use of information (e.g., secondary use and sharing information with third-parties).

Phelps, Nowak, and Ferrell (2000) examined the relationship between customers' privacy concerns and their behaviour as well as factors affecting their privacy concerns. Based on mail survey responses of 556 U.S. customers, they showed that the level of customers' privacy concerns is affected by the type of information requested, the way companies use personal information, and customers' desire for information control. From an online survey of 381 U.S. online users, Ackerman, Cranor, and Reagle (1999) found that there were significant differences in customers' comfort levels across various types of information. They also found different levels of acceptance of persistent identifiers (i.e., cookies) depending on the purpose. Lastly, they found several important factors related to customers' decisions about information disclosure including the sharing of information with other companies, the use of information in an identifiable way, the kind of information collected, and the purpose for which the information was collected. Chakraborty, Lala, and Warren (2002) identified eight factors which possibly affect the perceived effectiveness of B2B

Web sites: informativeness, organization, transaction-related interactivity, personalization, non-transaction-related interactivity, privacy/security, accessibility, and entertainment. Using a Web survey of 540 U.S. business customers of a large power tool company, they found privacy/security did not contribute to the perceived effectiveness of B2B Web sites while informativeness, organization, transaction-related interactivity, and personalization did.

Other researchers investigated the relationship between privacy concerns and other factors: for example, gender, (Dommeyer and Gross, 2003; Graeff and Harmon, 2002; O'Neil, 2001; Sheehan, 1999), age (Dommeyer and Gross, 2003; Earp and Baumer, 2003; Graeff and Harmon, 2002; Milne and Rohm, 2000; Sheehan, 2002), income level (Graeff and Harmon, 2002; O'Neil, 2001), and education (O'Neil, 2001; Phelps et al., 2000; Sheehan, 2002). Sheehan's (2002) analysis of an email survey of 889 U.S. online users indicated that online users' privacy concerns are influenced by their age and their level of education (e.g., well educated users tend to have higher level of privacy concern than less educated users). Sheehan (1999) found that women are more concerned than men about privacy, but men are more likely than women to change their behaviour to protect their privacy in the face of privacy concerns. O'Neil (2001) analysed an Internet survey of 1,223 U.S. online users done by Georgia Institute of Technology's Graphic, Visualization, and Usability Center (GVU) in 1998 and found that income level, gender, and race affected the level of concern about online privacy. That is, individuals with higher income levels are less concerned about their online privacy than those with lower income level, and women have more privacy concern than men. In addition, the level of privacy concern varies according to race, but different from prior studies¹⁰, other ethnic groups (i.e., Latinos, Indigenous or Aboriginal, Hispanics, and African Americans) are more concerned about their privacy than Whites. However, contrary to Sheehan (2002), education level did not affect the level of concern about online privacy.

¹⁰ For instance, the 1998 U.S. Department of Commerce study showed that Whites tend to have the highest levels of concern about online privacy, followed by Blacks, Asians and Pacific Islanders, and Hispanics (O'Neil, 2001).

2.3.1.3. Consequences of Customers' Privacy Concerns

Having examined the dimensions and antecedents of customers' concerns, the review now turns to the consequences of privacy concern (e.g., the effects of privacy concerns on customers' behaviour). Koyuncu and Lien (2003) found that privacy concern contributes negatively to consumer's online purchasing decision; i.e., individuals who are concerned more about their privacy tend to purchase less over the Internet. Sheehan and Hoy (1999) found that U.S. online users are less likely to register for a Web site when their privacy concerns are high. In addition, as privacy concern increased, online users were more likely to provide incomplete information, to notify Internet Service Providers (ISPs) about unsolicited email, to request their name removal from mailing lists, and to send negative messages to those sending unsolicited email.

Milne and Boza (1999) examined the relationship between privacy concern and trust by analyzing a mail survey of 1,508 U.S. respondents. They showed that consumers' perceptions of trust and level of concern about privacy vary by industry, and that trust is negatively related to privacy concerns. Milne and Boza also found that trust was affected by several factors: age, gender, knowledge of information practices, attitude toward relationship marketing, income, and computer usage.

Some studies have addressed the interrelationships between customer behaviour and factors such as customers' beliefs about privacy, attitude, and intention. Lwin and Williams (2003) developed a conceptual model to investigate a customer's behaviour in providing false information online. They used two theories: MDTP (Multidimensional Developmental Theory of Privacy: Laufer and Wolfe, 1977) and TPB (Theory of Planned Behaviour : Ajzen, 1985, 1987, 1991) with an additional factor of perceived moral obligation. They conducted an empirical study to test the TPB portion of the conceptual model using a mail survey of 341 U.S. online users. Their results indicated that attitudes, perceived behavioural control, and perceived moral obligation influence

customers' behaviour to provide false information while subjective norm (the perceived social pressure) does not. That is, the greater perceived behavioural control and perceived moral obligation, the more likely customers fabricate information.

Using the 1998 Web survey of 1,194 U.S. online users from the Graphics, Visualization and Usability (GVU) Center at the Georgia Institute of Technology, George (2002) also examined the relationship among beliefs about privacy and Internet trustworthiness, intention, and purchasing behaviour. He showed that beliefs about privacy and Internet trustworthiness help to determine attitudes towards the Internet, which in turn affects purchasing intentions. In a related study, George (2004) investigated whether privacy beliefs and trustworthiness of the Internet influence purchasing behaviour, as described in TPB. Based on a survey of 193 undergraduate students, he found that individuals' beliefs about the trustworthiness of the Internet have positive effect on their attitudes toward buying online, which in turn positively affects their purchasing behaviour. George also showed that customers' purchasing behaviour is affected by beliefs about self-efficacy (through perceived behavioural control). However, there is no relationship between customers' purchasing behaviour and beliefs about unauthorized use of personal information.

2.3.1.4. Research Opportunities in Customer Perspective

The research works surveyed so far suggest that consumers appear concerned about their privacy, and that such concerns may have negative effects on online transactions that could jeopardize the proliferation of e-commerce. While this literature contributes to our understanding about several privacy issues (dimensions, antecedents, and consequences), there are several additional research opportunities:

- The literature has not seen a comprehensive theory-based conceptual framework that identifies the factors that affect customers' privacy concerns and explains how customers' privacy concerns and their behaviour are influenced by these factors.

For companies and regulators such a framework could offer useful information about where they must concentrate in order to reduce customers' privacy concerns.

- While a number of dimensions of privacy concern have been identified, which ones are most important to customers? Which of the fair information principles proposed by government are most central to consumers? (Suggested by Caudill and Murphy, 2000).
- Factors that can potentially influence or moderate customers' privacy concerns include the trustworthiness of company (e.g., reputation and prior experience with the company) and customer motivation. Individuals are often willing to exchange their privacy for certain rewards (Caudill and Murphy, 2000; Shapiro and Baker, 2001). To what extent are customers are willing to provide their personal information for rewards such as discount coupons and free gifts, and do they perceive such tradeoffs as fair?
- How can we manage privacy risk and encourage trust to offset individuals' privacy concerns related to Internet use? What ways do individuals attempt to manage privacy risk? Does adjusting the settings on a Web browser diminish privacy risk and concern? Do installing security tools (e.g. firewalls) have a similar effect? (Suggested by Diney and Hart, 2006)
- Do individuals' privacy concerns actually cause individuals to engage in behaviour to protect their own online privacy? (Suggested by Sheehan and Hoy, 1999)
- There are some contradictions between studies. For instance, Sheehan (2002) showed that privacy concerns are sensitive to levels of education while the study done by O'Neil (2001) found no such difference. Such contradictions need to be resolved.

- Although several studies showed that consumers are concerned about online privacy, only a few have examined variations across different cultures. What makes individuals concerned about their privacy? Do the concerns exist because individuals in various cultures have different perceptions about their privacy?
- The previous literature of customers' behaviour is usually based on perception and not on actual behaviour. In other words, the actual behaviour was not measured in an e-commerce setting when customers actually conduct online transactions. Instead, individuals' intention was measured. It would be useful to have additional studies that examined customers' actual behaviour, rather than their intention.

2.3.2. Company Perspective

Customers' growing concerns about privacy have put pressure on e-commerce companies to develop customer-focused privacy practices (Culnan, 2000; Culnan and Armstrong, 1999; Shapiro and Baker, 2001). The studies in company perspective fall into two categories: those that describe companies' privacy practices and those that investigate the factors affecting those privacy practices.

2.3.2.1. Companies' Privacy Practices

Liu and Arnett (2002) analyzed 497 Web sites of the Fortune 500 and found that approximately 50 percent of these Web sites provide a privacy policy. They found no industry differences in the use of privacy policies to address customer's privacy concerns. Although most of them address opt-out, access/correction, and internal privacy protection, many Fortune 500 Web sites failed to cover all four privacy principles recommended by the US Federal Trade Commission (FTC) as representing "fair information practices": Notice/Awareness, Access/Participation, Choice/consent, and Security/Integrity.

Desai, Richards, and Desai (2003) examined Internet policies posted on 40 U.S. companies' Web sites from 1999 to 2001. They found that privacy-related policies were the most frequently posted policies on companies' Web sites. Milne and Culnan (2002) studied the changes and trends in voluntary privacy disclosures by analyzing four Web surveys conducted between 1998 and 2001 and found that the number of privacy disclosure statements increased over time, and also that the most popular sites had posted more privacy disclosures than their counterparts. Furthermore, they found a significant increase in disclosures about information collection, revealing information to third-parties, and choice.

Jamal et al. (2003) investigated e-commerce companies' privacy disclosures and the effectiveness of opt-out practices related to Notice/Awareness and Choice/Consent privacy principles. Upon analyzing 100 U.S. high traffic e-commerce Web sites, Jamal and his colleagues showed that the actual privacy practice of those sites closely complied with their stated privacy policies. Gurau, Ranchhod, and Gauzente (2003) also examined the privacy policies among three countries (France, UK, and US), and based on a Web site survey of French (93), UK (106), and US (92) Web sites they showed that there are differences among countries with respect to the form of data request and information provided in privacy disclosures. For example, the US sites provide more information about security of information than the French or British sites. While French sites collect data during transactions (transaction-based data request), the US sites are more focused on intrusive approaches such as data requests through pop-up windows.

2.3.2.2. Antecedents of Companies' Privacy Practices

Several studies have attempted to go beyond describing companies' privacy practices to identify the antecedents for those practices. For instance, Sarathy and Robertson (2003) introduced a model of factors influencing privacy strategy which incorporates the environmental context, ethical perspective, and firm-specific considerations. According to the model, a company's privacy strategy

is affected by its environmental context such as national history, culture, and existing and pending legislation. In addition, the company's privacy strategy is influenced by the ethical frame of the firm and top management as well as firm-specific factors such as the information intensity of the business, the age and experience of the firm, and the corporate culture. Further, cost-benefit analysis plays a role in the privacy strategy adopted by the company. That is, the company adopts different strategies depending on the analysis of economic benefits (e.g., meeting customer needs and relationship management) and cost of compliance (e.g., the cost of granting access to data). Although this model was not empirically tested, Sarathy and Robertson used it as a framework to help firms develop a strategy for addressing privacy concerns.

2.3.2.3. Research Opportunities in Company Perspective

Although several studies have examined privacy issues from a company perspective, such studies are somewhat limited, suggesting the need for additional research, such as:

- While prior studies have examined stated privacy policy disclosures, research on the actual privacy practices of e-commerce companies is needed. For example, to what extent do companies' data collection activities comply with their stated privacy policies? (Suggested by Liu and Arnett, 2002)
- Are the privacy policy statements currently disclosed by companies effective in dealing with consumer knowledge and control questions? (Suggested by Caudill and Murphy, 2000)
- How do companies' privacy practices affect short-term and long-term relationships with their customers?
- Do companies' privacy practices differ across countries? Do companies provide sufficient privacy protection as required by various governments? Are companies'

privacy practices influenced by regulatory approaches, cultural factors, and industry?

- What are the differences between Web sites that post privacy policies and sites that do not? Do the sites with privacy policies share common characteristics? What characteristics do the sites without policies share? Do the Web sites with the best privacy disclosures have anything in common? (Suggested by Culnan, 2000)

2.3.3. Government Perspective

This section reviews studies pertaining to government regulation of privacy, including regulation approaches and factors influencing regulation.

2.3.3.1. Regulation Approaches

Caudill and Murphy (2000) discussed online privacy conceptually and summarized regulations on privacy in the United States. Then, they proposed ethical standards that need to be addressed in corporate ethical policy and public policy. Smith (2001) investigated the differences in privacy approaches in the U.S. and Europe, identifying problems with the U.S. privacy approach such as the limitations of a voluntary approach to address privacy concerns and the secondary uses of personal information. Laudon (1996) examined individual privacy and the market for personal information and discussed several problems of current privacy protection based on “fair information practices” proposed by the U.S. Federal Trade Commission. For instance, according to Laudon, fair information practices leave individuals little or no control over the post-collection use of personal information (e.g., right for review and challenge). As one possible solution for such problems, he proposed a National Information Market (NIM) in which personal information could be bought and sold in a market, enabling individuals to receive fair compensation for the use of information about themselves.

2.3.3.2. Factors Influencing Government Regulation

Milberg et al. (1995) examined the interrelation among nationality, cultural values, and information privacy regulatory approaches. By analyzing survey responses from approximately 30 countries, they showed that the amount of government involvement (e.g., voluntary control, data commissioner, and regulation) is related to the cultural values identified by Hofstede (1980) – uncertainty avoidance, power distance, and individualism/collectivism. That is, countries with higher level of uncertainty avoidance or power distance tend to have higher levels of government involvement (e.g., regulation), but those with high individualism have less government involvement in regulating information privacy (e.g., voluntary control). Similarly, Milberg, Smith, and Burke (2000) conducted a survey of 595 internal auditors of the Information Systems Audit and Control Association (ISACA) from 19 different countries and examined the interrelationships among five factors: cultural values, individual privacy concerns, regulatory approaches, corporate privacy environment, and regulatory preferences. They developed a conceptual framework addressing the dynamic interrelationships among these factors in information privacy. Furthermore, based on the four measures of cultural values developed by Hofstede (1991), Milberg and his colleagues demonstrated that countries with higher level of power distance, masculinity/femininity, and individualism/collectivism each tend to have less government involvement, but countries with high uncertainty avoidance have higher levels of government involvement in the regulation of information privacy practices.

2.3.3.3. Research Opportunities in Government Perspective

Previous studies on Internet privacy from a government perspective leave a number of gaps:

- Currently, each country adopts different fair information principles to manage privacy issues (e.g., PIPEDA from Canada and FTC principles from U.S.). It is

useful to examine whether a set of universal core privacy principles exist across countries. Such research will contribute to understanding privacy regulation approaches in various countries as well as developing international privacy standards.

- What factors influence or moderate government approaches to regulating privacy practices? Potential factors to investigate include economic trends (e.g., the dot.com bubble), national security (e.g., the events of September 11 in the U.S.), and the transfer of personal information across borders (e.g., U.S. and EU safe harbour).

2.3.4. Customer–Company Interaction

Generally, in e-commerce, a customer searches one or more sites on the Internet, finds a suitable e-commerce site, and places an order. During this process, companies have many opportunities to collect and use personal information. This personal information can be used to provide better services through customization; however, it may also be misused. Each company decides upon the degree of information that it will collect and use; however, companies' privacy practices are influenced by customers' privacy concerns and behaviour, as well as influencing such concerns and behaviour through privacy policy statements posted on company Web sites and related privacy practices. Two types of customer-company interactions have been studied: (1) the interaction between a company's privacy practices and customer behaviour, and (2) the interaction between a company's characteristics and customer behaviour.

2.3.4.1. Company's Privacy Practice and Customer Behaviour

Whether or not customers provide their personal information can be influenced, in part, by the quality of companies' privacy practices (i.e., privacy policy disclosures). Palmer, Bailey, and Faraj (2000) examined how firms use trusted third parties (i.e., privacy seals) and privacy policy

statements to build trust on their Web sites. By analyzing a Web site survey of 102 publicly-traded U.S. companies, they showed that privacy policy statements and trusted third-party involvement can improve customers' trust.¹¹ That is, by posting a privacy policy statement on their Web sites, companies can reduce their customers' perceived privacy concerns about providing personal information.

Culnan and Armstrong (1999) studied the role of procedural fairness (i.e., information practices) in addressing privacy concerns based on telephone interviews of 1,000 U.S. customers, conducted by Harris Survey (1994), and found that people with greater privacy concerns are less willing to be profiled when they are not told that fair information practices are employed to manage their personal information. Similarly, Miyazaki and Fernandez (2000) found that online purchase intention is influenced by the prevalence of the company's privacy and security disclosures.

Miyazaki and Krishnamurthy (2002) found that a firm's participation in a seal program¹² favourably influences customers' perceptions of a Web site's privacy policy and the level of information disclosure. In contrast, Moores (2005) survey of 143 students found that few of them consider privacy seals as important in deciding to trust a Web site. Moores also found that although participants have a basic understanding about privacy seals and about the function of seals, quite a number of them did not know how a seal is obtained and failed to recognize genuine privacy seals. Similarly, Hui, Teo, and Lee (2006) examined the effect of privacy statements and privacy seals on individuals' behaviour. By conducting an exploratory field experiment in Singapore involving 109 students, they found that the existence of privacy statement encouraged individuals to provide their personal information, but that of a privacy seal did not. They also found that the positive effect of monetary incentive and the negative effect of the amount of information requested on individuals'

¹¹ Trusted third-parties are organizations that try to promote trust on the Web by awarding a logo (i.e., privacy seal) on a firm's web site to build consumer confidence regarding privacy by sending a signal to customers that companies' privacy practices comply with effective privacy practices.

¹² Seal programs are third-party enforcement programs that award an identifiable symbol to express that the Web site not only has implemented effective privacy practices, but is also abiding by those practices.

information disclosure. Lala et al. (2002) examined the impact of assurance seals (i.e., BBBOnline and WebTrust) and the information quality provided by such seals on consumers' Internet purchasing behaviour. Based on the experiment of 159 students, they showed that assurance seals have a positive effect on consumers' purchasing behaviour. They also found that the impact of assurance seals with the different level of information quality. Individuals had a strong preference for the high information quality seal (i.e., WebTrust) over the low information quality seal (i.e., BBBOnline).

Earp et al. (2005) studied whether there is a gap between the information provided in companies' privacy policy statements and the information that users want to know about Internet privacy. By analyzing privacy policy statements of 50 U.S. companies' Web sites and conducting a survey of 827 U.S. Internet users, they showed that the information addressed in companies' privacy policy statements does not fully provide the information that users want to know. That is, the three information items most frequently included in privacy statements are 1) security over data collection and transfer 2) how data is collected, and 3) consent about information collection. But users are most concerned about 1) transfer or sharing of their personal information, 2) information about what information is collected and how it is used, and 3) how organizations store and maintain their personal information.

2.3.4.2. Company Characteristics and Customer Behaviour

Several researchers have explored whether or not company characteristics such as the trustworthiness of their Web site affect customers' willingness to provide personal information as well as purchasing behaviour. Earp and Baumer (2003) studied consumers' behaviour and online privacy. By conducting an online survey of 415 U.S. respondents, they showed that the type of Web site (i.e., retail, financial, or medical/health) and brand status (e.g., well-known versus unknown Web sites) influence individuals' willingness to provide information.

Swaminathan, Lepkowska-White, and Rao (1999) also examined factors affecting online purchasing behaviour. Their analysis of 428 email responses indicated customers' online purchasing behaviour is influenced by three factors: the perceived reliability of a vendor, the convenience of placing an order and contacting the vendor, price competitiveness and access to information. They also showed that, on average, customers are not overly concerned about security or privacy, but customers who purchase frequently on the Internet are interested in new regulations protecting privacy on the Internet.

Ranganathan and Ganapathy (2002) examined key dimensions of business to customer (B2C) Web sites as perceived by online consumers. Based on an online survey of 214 U.S. online shoppers, they identified four key dimensions of B2C web sites: information content, design, security, and privacy. In addition, they found that privacy has a significant effect on customers' purchase intention.

2.3.4.3. Research Opportunities in Customer – Company Interaction

Research opportunities concerned with this interaction include:

- Do companies benefit by addressing customers' concerns about privacy? Companies posting well-developed privacy policies might affect customers' propensity to visit their Web sites often and to transact more. Therefore, companies are more likely to address privacy concerns if they gain benefits such as competitive advantage through building strong customer relationships.
- Do customers rely on privacy tools to protect their privacy? To reduce customers' privacy concerns, several privacy tools (e.g., P3P) have been developed to examine companies' privacy practices. However, it is not known how customers perceive such privacy tools and whether they are familiar with these tools.

- The studies on customers' behaviour usually used a survey methodology to measure self-reported privacy behaviour rather than actual behaviour. As seen in the literature (e.g., Horton et al., 2001; Szajna, 1996), however, individuals' stated action may differ from their actual behaviour. Therefore, it would be important to determine whether this gap exists in the Internet privacy domain.
- Do companies provide enough privacy protection to address customers' privacy concerns? Currently, many companies develop and disclose a privacy policy statement in their Web sites. It is expected that reading such privacy policy statements can reduce customers' perceived privacy risks associated with the disclosure of their personal information. However, it is not clear how customers perceive the privacy policy statement and whether the statement successfully addresses the customers' concerns.
- Customer perceptions of seal programs are uncertain due to conflicting findings by Miyazaki and Krishnamurthy (2002) and Moores (2005). It would be useful to have additional studies that explain what might be contributing to the different findings.
- While seals are meant to raise consumer confidence in a company's Web site, the fact is that they are not popular among companies, nor is it clear as to how customers perceive privacy seals. Interesting questions include: Why are privacy seals not popular? Are there specific situations in which seals are perceived as useful? Are there differences among companies participating in seal programs and those not participating in seal programs (i.e., differences in company size, industry, etc.)?

2.3.5. Customer – Government Interaction

Customers express their concerns about privacy through public opinion, and governments respond to customers' privacy concerns by way of regulations. However, only a few studies have examined this relationship.¹³

2.3.5.1. Customer's Privacy Concern and Government Approach

Sheehan and Hoy (2000) examined whether the underlying dimensions of customers' privacy concerns are addressed in FTC privacy principles. By conducting an e-mail survey of 889 U.S. online users, they showed that many underlying dimensions of customers' privacy concerns are addressed in the principles. However, they also found that two possible dimensions related to customers' privacy concerns are not addressed in FTC privacy principles: 1) online users' established relationships with online entities (i.e., familiarity with entity) and 2) the exchange of information for compensation.

2.3.5.2. Research Opportunities in Customer – Company Interaction

Few studies have examined the relationship between customers and governments. Promising future research opportunities include the following:

- Are the disclosures required by governments enough to ensure customers' privacy concerns? Although the studies conducted by Sheehan and Hoy (2000) and Earp et al. (2005) take up for the question of whether or not FTC principles adequately address the underlying dimensions of customers' privacy concerns and whether customers' privacy concerns are adequately addressed in companies' privacy policy statements, there are still other unanswered questions

¹³ Although most studies addressed in this section did not examine a particular causal relationship (e.g., how customer concerns influence government regulation approaches), they were classified into this section. Since such studies examined the relation between customer and government, they are somewhat akin to the interaction between customer and government.

such as whether customers' privacy concerns are adequately addressed in other FIP principles and whether companies' privacy policy statements include FIP principles that are most central to consumers.

- Is government regulation an effective approach to protect customers' privacy? Customers' concerns about privacy are influenced by several factors and keep changing, so as to keep up with social and technical changes. However, it usually takes a considerable amount of time for a new regulation to be effective. Therefore, it is useful to investigate whether government regulation itself can satisfy customers' privacy concerns.
- Do customer concerns influence government regulation approaches? How do such concerns affect governments' approaches?
- Various regulations have been enacted to protect individuals' privacy across countries: for example, Health Insurance Portability and Accountability Act (US), Personal Information Protection and Electronic Documents Act (Canada), and Data Protection Directive (EU). It would be interesting to see whether customers are aware of the legislation and what are the impact of government regulation on customers' privacy concerns and their behaviour.

2.3.6. Company – Government Interaction

While government regulation is affected by customers' privacy concerns, it could also be influenced by companies' practices and industry self-regulation.

2.3.6.1. Company's Privacy Practice and Government Approach

Milberg et al. (1995) found differences in privacy concerns associated with the level of government involvement in corporate privacy management. Milberg, Smith, and Burke (2000) found

that high levels of privacy concern are associated with greater preferences for strong laws over self-regulation and that regulatory approach is associated with both the corporate privacy management environment and regulator preferences. That is, countries with higher levels of governmental involvement tend to have a tighter corporate privacy environment (e.g., strong corporate privacy policies and practices and positive senior management attitudes) and greater regulator preferences (e.g., preference for government regulation over corporate self-management). Jamal et al. (2003) argued that governmental intervention through regulation is not necessary because the e-commerce industry develops industry standards or norms in the absence of government regulation.

Johnson-Page and Thatcher (2001) studied privacy policy discourses on Business to Customer (B2C) Web sites in nine countries (US, Canada, Germany, Hungary, UK, China, Singapore, Brazil, and Venezuela) across five industries (banking and financial services, Internet service providers, newspapers, online retailers, and telecommunications). The analysis of 149 B2C Web sites indicated that privacy policies are more commonly found in countries which establish a market economy with clear business regulations and in which customers not only have more access to the Web, but also have more experience in using it.

2.3.6.2. Research Opportunities in Company – Government Interaction

Making new regulations that balance companies' personal information needs and customers' concerns about privacy requires taking into account companies' information gathering activities and the context in which the information is used. Although some researchers have examined the relationship between company and government, there are several potential research opportunities:

- For most companies, government regulation will form the basis for developing privacy policy. Do companies provide enough privacy protections as required by government?

- To what extent do recently enacted and pending privacy regulations enhance Internet privacy? It is generally expected that existing and pending regulations influence companies' privacy practices. It would be beneficial to examine how companies respond to the new or pending regulations. It would also be interesting to study how these regulations enhance companies' privacy practices and reduce customers' privacy concerns.
- Are companies' privacy practices in one country different from those of other countries due to various regulation approaches? The differences in privacy regulations of each country may pose a significant regulatory challenge for companies looking to multiple markets around the world. It is interesting to see whether companies operating their business in less strict regulation countries have less comprehensive privacy practices than companies in strict regulation countries.

2.3.7. Customer – Company – Government Interaction

Internet privacy involves interactions among customers, companies and governments. Customers provide personal information, and companies collect and use the information for marketing purposes or customizing their services. Customer concerns about potential abuse of privacy lead to governmental involvement through laws or self-regulation, which in turn influences companies' privacy practices.¹⁴ Studies that have examined this relationship are rare. Culnan and Bies (2003) is one study that addressed relationships among customer, company, and government. In their research, Culnan and Bies discussed consumer privacy from a justice perspective and explained three types of justice factors related to consumer privacy (i.e., distributive justice, procedural justice,

¹⁴ Although it is plausible, it is not the sole relationship pattern that exists. For example, in Canada, the Personal Information Protection and Electronic Documents Act (2000) was passed with minimal public and business awareness of its impact. Although it only took full effect in 2004, considerable effort was actually required to try and educate (primarily) businesses and consumers about the law. This is not something one might expect based on the relational pattern presented in the paper. Therefore, the relationship pattern presented is one explanation of how the three factors interact.

and international justice). They argued that the violation of these factors may lead to consumers' privacy concerns. In addition, Culnan and Bies explained fair information practices in justice concerns and three implementation alternatives for implementing fair information practices: government regulation, self-regulation, and technological solutions. Research in this area is just beginning to emerge.

2.3.8. Other Factors

While most prior research has focused on privacy issues among customers, companies, and government, some attempts have been made to address privacy issues in terms of new technologies and social or economical perspectives.¹⁵ For example, Kenny and Korba (2002) argued that Digital Rights Management is a potential tool for the management of personal information. Cranor, Arjula, and Guduru (2002) examined the role of the Platform for Privacy Preferences (P3P) in customers' privacy behaviour. The AT&T Privacy Bird¹⁶ was used as a P3P user agent. Based on an analysis of an email survey of 331 AT&T Privacy Bird users, they showed that the use of the AT&T Privacy Bird guides users to read privacy policies more often and protects their privacy more proactively. Hochheiser (2002) examined the Platform for Privacy Preferences (P3P) in a U.S. policy context. In his research, Hochheiser provided an overview of P3P and described three proposed P3P privacy models (OECD, U.S. FTC, and Canadian fair information practices). He then discussed P3P from both historical and technical perspectives by focusing on political, legislative, and regulatory contexts in the U.S.

¹⁵ The studies addressed in this section are placed outside the model as other factors because they are mostly qualitative research works which address the impact of new privacy protection technologies and the economical aspects of privacy.

¹⁶ The AT&T Privacy Bird is software designed to help Internet users stay informed about the privacy policies of Web sites they visit. It reads privacy policies written in Platform for Privacy Preferences (P3P) and informs the Web site's policies by displaying a bird icon. That is, a green bird icon is appeared for Web sites that match users' privacy preference, but a red bird icon is shown for Web Sites that do not.

Other researchers address privacy issues in social or economical perspectives. For instance, the questions of how Internet privacy differs from traditional privacy and of whether customers' privacy will be diminished over time have been considered in the research. Ben-Ze'ev (2003) examined the concept of privacy. He argued that since individuals in cyberspace are relatively anonymous and have the ability to reveal matters that they choose to disclose, there are weaker conflicts between privacy and emotional closeness and between privacy and openness in cyberspace than in the real world. Therefore, individuals can achieve more privacy in cyberspace while they are attaining high levels of openness and closeness. Rust, Kannan, and Peng (2002) studied the erosion of privacy on the Internet. By using a simple economic model with assumptions that there is no government intervention, and privacy is left to free-market forces, they showed that over time, the amount of privacy will decline, and customers will bear more expenses to maintain their privacy.

In addition, several attempts have been made to address the importance of assurance services regarding information privacy and the role of the accounting profession in privacy assurance services (e.g., Greenstein and Hunton, 2003; Hunton et al., 2000; Kovar et al., 2000; Odom et al., 2002). For instance, Hunton et al. (2000) investigated the effect of e-commerce assurance on financial analysts' earnings forecast and stock price estimates. By analyzing a survey of 37 financial analysts and conducting an experiment of 87 analysts, they found that financial analysts issue more positive earnings forecasts and stock-price estimates when an e-commerce company acquired e-commerce assurance (i.e., WebTrust) and vendor- and outcome-based risks were high (i.e., the company is unknown and the perceived outcome risk from transactions is high). Greenstein and Hunton (2003) examined skills that potential clients view as necessary to perform privacy services and whether they perceive that CPA firms possess the skills that are necessary to perform privacy services. They also investigated whether potential clients are likely to hire a CPA firm to perform privacy services and whether a brochure produced by the American Institute of Certified Accountants (AICPA) changes potential clients' belief regarding CPA firms' qualifications. Based on the experiment of 82 corporate managers representing 27

companies, they identified four skill level categories that the management of audit client view as necessary: technical skills, legal skills, control/assurance skills, and strategic skills. Managers believe that CPA firms had high technical and control assurance skills, but low strategic and legal skills. They also found that many respondents consider that privacy services should be separated from the auditing engagement and have low willingness to engage a CPA firm to conduct privacy services. However, the brochure produced by AICPA increases managers' perception regarding the ability of CPA firms to perform privacy services. The brochure has the greatest impact on perceptions of technical skills, legal skills, and strategic skills.

There are also several research opportunities in this area:

- How do customers perceive new privacy protection technologies? Currently, a variety of technology tools are developed to help customers protect their privacy. For instance, several web browsers (e.g., Internet Explorer) allow users to set their privacy protection level. Thus, users, for instance, can block third-party cookies which use personally identifiable information without users' consent. However, it is not clear how customers perceive privacy protection technology tools and whether such tools can reduce customers' privacy concerns.
- What are the short-term and long-term consequences of loss of privacy to individuals and to society as a whole? (Suggested by Culnan and Bies, 2003)
- Do privacy protection technologies enhance Internet privacy? The basic assumption of privacy protection technologies is that just as information technology can erode privacy, it also can enhance privacy. However, there is no reliable evidence indicating that privacy protection technologies improve user privacy. Therefore, it would be interesting to investigate whether technologies are an effective approach to enhance Internet privacy.

2.4. The Purposes of the Study

This study investigates several research opportunities that have not been addressed by previous literature. In particular, this study is intended to address some important relationships among customer, company, and government. Three main research opportunities with respect to these relationships are explored throughout the study.

First, the study tries to explain how Internet privacy influences customers' behaviour (named as *Privacy Behaviour Study – Chapter 3*). In particular, the study examines the effect of companies' privacy policy disclosures and the level of involvement regarding the sensitivity of personal information on individuals' behaviour. This study also investigates whether there is a discrepancy between self-reported behaviour and actual behaviour. A Web-based survey and an online ordering experiment of 210 participants have been conducted to examine individuals' behaviour regarding Internet privacy. The results of this research are expected to contribute to our understanding of individuals' privacy behaviour and companies' privacy policy disclosures. Thus, it provides a basis for identifying strategies which can address customers' privacy concerns as well as specific situations in which privacy policy disclosures are perceived as useful.

Second, companies' privacy disclosures are examined to see the extent to which companies provide sufficient privacy protection as required by governments across countries (named as *Privacy Policy Disclosure Study – Chapter 4*). A total of 420 corporate Web sites have been examined and compared with the purpose of eliciting policy differences at country and industry levels. The results of this study will broaden our understanding of how companies perceive customers' privacy and how they protect their customers' privacy. The results will also highlight factors that influence companies' privacy disclosures and thus provide useful information for regulators.

Finally, this study investigates whether there is a gap between individuals' importance ratings of companies' privacy practices and privacy policies that companies emphasize in their privacy

policy disclosures (named as *Privacy Gap Study – Chapter 5*). In particular, after assess the fair information principles that are most central to consumers, the adherence to these principles by companies' privacy policy statements is examined. The results of this research are particularly important for regulators since the findings will be able to provide information as to whether individuals' privacy concerns are adequately addressed in companies' privacy policy disclosures. Furthermore, they will help companies to reduce their customers' privacy concerns by emphasizing matters which customers consider most important and thus be able to build strong trusting relationships with their customers.

3. Internet Privacy and Individual Privacy Behaviour: Privacy Behaviour Study

In this section, the effect of companies' privacy policy disclosures and the level of involvement on individuals' privacy behaviour are examined. Also, a discrepancy between self-reported privacy behaviour and actual privacy behaviour is investigated. Privacy behaviour is defined in this study as the process of searching and evaluating information about companies' privacy policies and making a decision about personal information disclosure.

Quite a number of studies have explored whether customers' behaviour is affected by customers' privacy concerns, companies' privacy policy disclosures, and company characteristics such as the trustworthiness of a company (e.g., Earp et al., 2005; Earp and Baumer, 2003; George, 2004; Kaplan and Nieschwietz, 2003; Koyuncu and Lien, 2003; Sheehan, 1999). For instance, Koyuncu and Lien (2003) showed education level, income level, and online experience have a positive effect on a consumer's online purchasing decision, but privacy concern contributes negatively to a consumer's online purchasing decision. Earp and Baumer (2003) found that the type of Web site (i.e., retail, financial, or medical/health) and brand status (e.g., well-known versus unknown Web sites) influence individuals' willingness to provide information. Also, Kaplan and Nieschwietz (2003) examined the effects of WebTrust and company type (i.e., known versus unknown) on purchase intentions. By conducting an Internet-based experiment of 216 participants, they showed that WebTrust influences individuals' purchasing intentions through the formation of assurance beliefs while company type influences the intentions through the formation of trust beliefs.

Based on prior literature and opinion polls indicating customers' high privacy concerns, the studies appear to assume that individuals are highly involved in privacy issues. That is, prior studies did not address the possible effects of an individual's involvement on his or her own attitude toward privacy. At the time of writing, no research could be found regarding how customer

involvement affects customers' attitudes and thus guides their behaviour with respect to Internet privacy.

3.1. Elaboration Likelihood Model (ELM)

According to Rothschild (1984), involvement is “an unobservable state of motivation, arousal or interest.” It is a motivational and goal-directed emotional state that determines the personal relevance of an object or situation. Customer involvement is recognized as an important factor influencing customers' information searching, information processing, and decision-making (Kapferer and Laurent, 1986). Therefore, it is reasonable to expect that the individuals' behaviour might be different depending on their involvement with privacy.

To examine the role of privacy involvement, this paper adapts the Elaboration Likelihood Model (ELM). ELM has been widely regarded as one of the most influential models of attitude and attitude change and has been applied in various research areas: marketing literature (e.g., Darley and Smith, 1993; Pham and Avnet, 2004), information systems literature (e.g., Coombs and Cutbirth, 1998; Mak et al., 1997), and health related literature (e.g., McCullough and Dodge, 2002). ELM is a dual-route information processing theory. It explains how variables (e.g., involvement, mood, and distraction) influence an individual's attitude toward objects and describes the persuasion processes that individuals undertake to form an attitude (Petty and Cacioppo, 1986; Petty and Wegener, 1999).

According to Petty and Cacioppo (1986), individuals' attitude changes are based on different degrees of elaboration (i.e., cognitive effort in information processing activity). When individuals find information interesting, important, and personally relevant without any distractions to prevent them from examining it in detail, they are likely to scrutinize available relevant information and arrive at an attitude that is well supported by reasons acquired from their effortful information processing activity (*Central Route*). However, when individuals are not sufficiently motivated or do not have the ability to scrutinize and evaluate information

provided, they examine available information less and less carefully (*Peripheral Route*). Individuals in the peripheral route emphasize positive or negative cues (e.g., the perceived credibility of information) rather than arguments in information (e.g., the context of the information).

3.2. Involvement and Privacy Behaviour

Many e-commerce sites now post privacy policies. The main purpose of privacy policies is to announce companies' information practices to customers. Such policies, usually stated in corporate privacy policy statements, refer to the set of implicit and explicit principles that determine whether and how personal information is collected, used, and transferred. Since involvement might have an impact on individuals' attitudes toward privacy and their behaviour, it is anticipated that there is a relationship between the level of privacy involvement and individuals' behaviour in terms of reading a privacy policy statement when they are requested to provide personal information on a Web site. Furthermore, ELM suggests that when individuals are sufficiently motivated and have the ability, they think more elaborately about available information. When they are not motivated or do not have the ability to process information, they take the easy way out by being influenced by unrelated factors such as the attractiveness or perceived credibility of the information.

In the e-commerce environment, therefore, it is expected that when individuals are under high privacy involved situations in which they are motivated to think about privacy, they will carefully examine all available privacy relevant information such as privacy policies and come to a judgment on the company's privacy practices based on the quality of the information they find. Therefore, the following hypothesis is introduced.

H1: Individuals in a high privacy involved situation are more willing to perform an information search regarding companies' privacy practices (i.e., read privacy policy statement) than those in a low privacy involved situation.

Since individuals in high privacy involved situations are motivated to think about privacy, they tend to be more concerned about their privacy than those in low privacy involved situations, and thus they are less willing to disclose their information when they are requested to provide personal information. Therefore, the following hypothesis is examined.

H2: Individuals in a high privacy involved situation are less willing to provide their personal information than those in a low privacy involved situation.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that a Web site not only has implemented effective privacy practices, but is also abiding by those practices. According to Palmer, Bailey, and Faraj (2000), trusted third-party involvement (i.e., privacy seal) can improve customers' trust. That is, by placing privacy seals on their Web sites, companies can reduce their customers' perceived privacy concerns about providing personal information.

It is possible that a privacy seal may work as a cue in ELM. However, according to ELM, individuals' behaviour with respect to reading a privacy policy statement may not be influenced by privacy seals (i.e., cue) even though privacy seals reduce privacy concerns and thus influence behaviour. Since individuals in high privacy involved situations are motivated to scrutinize all available privacy relevant information and come to a judgment on the company's privacy practices based on the quality of the information they find, they tend to read privacy policy

statements carefully regardless of privacy seals. Furthermore, individuals' behaviour about reading a privacy policy statement may not be affected by privacy seals (i.e., cue) in low privacy involved situations as well. ELM suggests that under low privacy involved situations, individuals are not motivated and thus tend to examine available privacy relevant information less and less carefully. Therefore, individuals are less willing to read privacy policy statements. In such circumstances, privacy seals may not influence individuals' behaviour because the existence of privacy seals does not prompt individuals to examine available privacy relevant information. Therefore, the following hypothesis is suggested.

H3: Individuals' behaviour with respect to reading a privacy policy statement is not influenced by a privacy seal in both high and low privacy involved situations.

However, an individual's decision about providing personal information is expected to be affected by privacy seals because it is influenced by positive or negative cues (e.g., the perceived credibility of information) rather than arguments about information. Therefore, it is anticipated that a privacy seal works as a cue as described in ELM. The next hypothesis for consideration is as follow.

H4: Individuals' behaviour related to providing personal information is more influenced by a privacy seal under a low privacy involved situation than under a high privacy involved situation.

Several works have argued that privacy policy disclosures help build trust and promote the disclosure of personal information, given that companies' privacy policies signal to customers about their fair information practices (e.g., Culnan and Armstrong, 1999; Milne and Boza, 1999). Although

companies' privacy policy disclosures can have a positive effect on the disclosure of personal information, individuals' information disclosure may vary depending on the quality of companies' privacy policies. Individuals have different privacy preferences for different kinds of personal information, and their preferences depend on the context in which this information is collected and used (Petty, 2000; Phelps et al., 2000; Sheehan and Hoy, 2000). For example, individuals may be less willing to disclose their financial information, such as credit card numbers, than their purchasing preferences, and their major concerns might be reasonable security safeguards against risks such as unauthorized access or disclosure of the information. Therefore, it is likely that people are less willing to provide their personal information if companies' privacy policy statements do not provide the important information that they want to know (e.g., security safeguards). However, this may have less influence on individuals' willingness to provide personal information if companies post privacy seals on their Web sites because as addressed in Palmer et al. (2000), trusted third-party involvement (i.e., privacy seals) enhance consumer confidence regarding privacy. Therefore, the next hypothesis is as follows.

H5: When the privacy policy statement of a company does not address the important privacy practices that individuals want to know, individuals are more willing to provide personal information to the Web site with a privacy seal compared to without a privacy seal.

Prior studies have tried to explain how customers' behaviour is influenced by Internet privacy (e.g., George, 2004; Koyuncu and Lien, 2003; Miyazaki and Fernandez, 2001). The studies of customers' behaviour, however, have usually used a survey methodology to measure self-reported behaviour, rather than actual behaviour. That is, the actual customers' behaviour was not measured in an e-commerce setting when customers actually conduct online transactions such as

ordering things or registering on a Web site for online services. A considerable amount of literature has suggested a difference between self-reported behaviour and actual behaviour. Berendt, Gunther, and Spiekermann (2005) examined whether there is a discrepancy between self-reported privacy concerns and actual self-disclosing behaviour. Based on the online experiment of 206 users, they showed a gap between self-reported privacy concerns and actual self-disclosing behaviour. Szajna (1996) found that in the domain of e-mail use self-reported behaviour is not an interchangeable measure for actual behaviour. In their study of intranet usage, Horton et al. (2001) also reached the conclusion that self-reported behaviour is an inappropriate substitute for actual behaviour. Given prior studies showing the gap between self-reported behaviour and actual behaviour, the following hypotheses are introduced.

H6: There is a difference between self-reported privacy behaviour and actual privacy behaviour with respect to reading a privacy policy statement.

H7: There is a difference between self-reported privacy behaviour and actual privacy behaviour with respect to providing personal information.

4. Internet Privacy and Companies' Privacy Practices: Privacy Policy Disclosure Study

The inappropriate use of personal information leads to customers' privacy concerns and reduces consumer trust in online transactions and may eventually jeopardize the proliferation of e-commerce (Hoffman et al., 1999b; Liu et al., 2004; Luo, 2002; Milne and Boza, 1999; Shankar et al., 2002). Studies have shown that a company's privacy protection influences customers' satisfaction with an online company (Branscum and Tanaka, 2000), their trust of a vendor (Milne and Boza, 1999), and online purchasing decisions (Caudill and Murphy, 2000). Just as having good privacy protection has a positive impact on a company, not having good privacy protection can increase the company's risk (e.g., lawsuit from customers and loss of customers). Another purpose of the study is to investigate companies' current practices of Internet privacy at the country level and industry level. In particular, this study discusses how companies' privacy policy disclosures can be influenced by regulatory approaches, cultural factors, and industry.

4.1. Privacy Policy Disclosures, Industry, and Country

Previous literature has examined companies' privacy policy disclosures on their Web sites (e.g., Desai et al., 2003; Jamal et al., 2003; Milne and Culnan, 2002; Miyazaki and Krishnamurthy, 2002; Sarathy and Robertson, 2003). Although the aforementioned studies are useful and enhance our understanding of companies' privacy policy disclosures, they usually examined U.S. companies. Furthermore, studies that explored a difference among countries did not examine the extent to which companies' policies stated in their privacy policy disclosures differ across countries and industries with respect to Fair Information Practices (FIP) principles.

In general, privacy policy statements are generated based on Fair Information Practices (FIP). FIP is a general term for a set of guidelines governing how information should be

collected, used, and protected. It represents procedures that not only provide individuals with control over the disclosure and subsequent use of their personal information but also govern the interpersonal treatment that customers receive (OECD, 1980). Furthermore, FIP includes principles developed as models for protecting the privacy of personal information and managing individuals' privacy risks.

A variety of governments and organizations have developed their own FIPs (FTC, 1999). They include FTC fair information practice in U.S., PIPEDA in Canada, EU Directive in EU, OECD guideline from OECD, and Generally Accepted Privacy Principles (GAPP) from AICPA/CICA. Although the aforementioned FIPs are similar, they differ in their specific requirements with respect to a number of key principles (AICPA/CICA, 2006). This study assesses the extent to which companies' privacy policies differ across countries with respect to FIP principles. Since the implementation of FIP varies due to the difference in FIP principles among countries, it is possible that some principles commonly addressed in the companies' privacy policy statements of one country may not be addressed in the statements of other countries. Therefore, the following hypothesis is suggested.

H8: FIP principles addressed in companies' privacy policy statements vary across countries.

Companies in a particular industry may perceive the importance of privacy risks such as legal risk (e.g., lawsuit from customers) and financial risk (e.g., loss of customers) differently as opposed to companies in other industries (Schoder and Yin, 2000). Several studies have argued that the privacy policies help build trust and promote the disclosure of personal information, given that companies' privacy policies signal to individuals about their fair information practices (Culnan and Armstrong, 1999; Milne and Boza, 1999). Since individuals have different privacy concerns and preferences depending on the type of information the company collects and uses (Ackerman et al.,

1999; Phelps et al., 2000), it is expected that the type of industry in which a company operates its business might influence the company's risk recognition and thus impact on its privacy policies. Therefore, companies that collect and use information which individuals consider sensitive might have more stringent privacy policies than other companies. That is, companies in information-sensitive industries develop more comprehensive privacy policies by stating related FIP principles in their privacy policy disclosures than those in less information-sensitive industries. Based on prior studies showing that medical and financial information is considered to be more sensitive than other types of information (Smith, 1994; Milberg et al., 2000), this study classifies financial and health industries as information-sensitive industries and other industries as less information-sensitive industries. This leads to the following hypothesis.

H9: Companies in information-sensitive industries (e.g., financial and health industries) incorporate more FIP principles in their privacy policy disclosures than do companies in less information-sensitive industries (e.g., manufacturing and retail industries).

4.2. Privacy Policy Disclosures and Regulatory Approaches

As an approach to deal with Internet privacy, each country adopts different regulatory approaches. For instance, the United Kingdom, Germany, and Canada have enacted privacy legislation that plays an important role in protecting privacy. On the other hand, the United States has taken a more liberal industry self-regulation approach. Since, for a number of companies, existing and pending legislations are likely to form the basis for developing their privacy policies (Sarathy and Robertson, 2003), companies' privacy policy disclosures can be influenced by the regulatory approach.

The research investigating the relation between companies' privacy policy disclosures and regulatory approach adds important information to the debate of self-regulation versus government

regulation. According to the opponents of government regulations, the problem with regulations is that they always lag behind technology development. On the other hand, the proponents of self-regulation argue that since customers are privacy conscious, market forces will lead companies to abide by industry privacy standards. Also, companies can establish a trust relationship with customers using privacy policy statements and privacy seals (Spiekermann *et al.*, 2001). However, self-regulation is often criticized as being self-defined (Rezgui *et al.*, 2003). That is, different companies can adopt different principles to handling their customers' information. Therefore, the role of governmental involvement (i.e., regulatory approach) in companies' privacy policy disclosures provides useful information for regulators so that they can consider which approach would be taken to manage privacy issues.

Research on the impact of regulation on company privacy disclosures is just beginning to emerge. Most studies discuss the differences in approaches to privacy regulation among countries, especially between the U.S. and the EU (e.g., Hinde, 2003; Nijhawan, 2003; Smith, 2001). It is difficult to find empirical research that examines how companies' privacy policy disclosures are influenced by regulatory approach. One such study is by Milberg *et al.* (1995) who examined the relationships among nationality, cultural values, information privacy regulatory approaches, and the nature and level of information privacy concerns. They showed that the differences in privacy concerns are associated with different regulatory structures, and the amount of government involvement in information privacy regulation is affected by cultural values in the various countries. More recently, Milberg, Smith, and Burke (2000) found that the regulatory approach is associated with both corporate privacy environment and regulatory preferences. Thus, in countries with high levels of government involvement, corporate privacy management occurs in higher levels in organizations, and a preference for strong laws in regulating privacy is high.

Although the aforementioned studies are useful, they focus on corporate information privacy in general, but not on Internet privacy. In other words, they do not examine companies' privacy

practices with respect to collecting and using customers' personal information. This study examines the role of regulatory approach in companies' privacy disclosures stated in privacy policy statements.

An analysis of the privacy regulations of several countries reveals a broad divergence of approaches to the governance of information privacy (Milberg *et al.*, 1995; Milberg *et al.*, 2000; Smith, 1994). Figure 2 shows the regulatory approach model.¹⁷

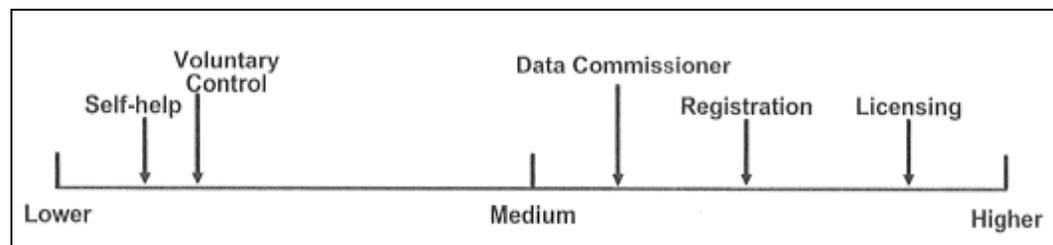


Figure 2: Level of Governmental Involvement in Corporate Privacy Management

The above model indicates that in countries at the left end of the continuum (*low governmental involvement*), the government has a limited role in protecting personal information. Therefore, individuals are responsible for their own privacy problems and must find remedies for problems on their own. In countries at the right end of the continuum (*high governmental involvement*), the personal data of individuals are quite well protected through governmental involvements that entail licensing and supervision. Thus, companies in these countries that want to collect and use personal information need to be licensed and are overseen by regulatory agencies (Milberg *et al.*, 1995; Milberg *et al.*, 2000; Smith, 1994).

Corporate privacy management involves several important areas such as privacy protection levels, privacy policies, and the management of these policies (Smith, 1994). Prior research has shown that organizations with tighter privacy management (e.g., more adequate privacy policies and actual practices) show fewer privacy related problems compared with organizations with less tight privacy management (Milberg *et al.*, 2000). However, managers have been reactive in addressing

¹⁷ Adapted from Smith (1994) and Milberg et al. (1995; 2000).

information privacy concerns even though companies are more concerned about information privacy with the increased levels of governmental involvement in corporate privacy management (Smith, 1993, 1994). Companies have shown a tendency not to establish privacy policies until confronted by governmental regulations, and thereafter they react with formalized policies that increase their attention to privacy.

Given that companies' privacy policy statements contain information about corporate privacy policies and are generated based on FIP, it is expected that FIP principles addressed in privacy policy statements vary according to the regulatory approach that a country adopts. Based on the regulatory models, this study proposes the following hypothesis.

H10: Companies that operate their business in high governmental involvement countries incorporate more FIP principles in their privacy policy disclosures than do companies in low governmental involvement countries.

4.3. Privacy Policy Disclosures and Culture

Culture is defined as “a collective programming of the mind that distinguishes a group or category of people from another” (Hofstede, 1991). Culture provides individuals with a sense of identity and an understanding of acceptable behaviour within a group. Groups of people in the same culture share unique cultural values because of their shared history, economy, geography, religion, and demographics. These cultural values represent implicit and explicit ideas shared in a group about what events, characteristics, and conducts are good, right, and desirable (Williams, 1968, 1970). Therefore, individuals' perceptions and their interpretation of the objects or situations are influenced by their cultural values. According to Adler (1991), culture influences individuals' expectations, values, beliefs, attitudes, and ultimately their behaviour in everyday life. It also influences behavioural norms in society and affects social interactions by establishing the nature of

relationships among individuals and between individuals and organizations (Aycan *et al.*, 2000; Schwartz, 1992).

Cultural differences among countries may lead to differences in privacy perceptions. For example, Europe and U.S. differ substantially on how they approach the protection of individual privacy with respect to legislation, society, and culture (Smith, 2001). European countries emphasize governmental regulation to protect consumer data privacy via a centralized privacy agency. On the other hand, the U.S. uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation instead of having federal level privacy regulation. Furthermore, most European countries consider privacy as a fundamental human right, but in the U.S., privacy is usually considered as a matter for contractual negotiation, and customers need to protect their own privacy (Smith, 2001). Thus, such cultural differences may cause not only differences in customers' privacy concerns but also differences in companies' privacy practices between Europe and U.S.

Some studies have examined the role of cultural values on privacy. For instance, Milberg *et al.* (1995) found that the level of personal information privacy concerns varied across countries, but cultural values do not influence the level of personal information privacy concerns. However, unlike Milberg *et al.* (1995), Milberg, Smith, and Burke (2000) found that cultural values are associated with differences in levels of consumer information privacy concerns. While such studies focused on the relationship between cultural values and individuals' privacy concerns, there has been no attempt to examine whether cultural differences influence company privacy policy disclosures. This study, therefore, seeks to fill the gap by addressing this topic.

Hofstede's (1980, 2001) cultural typology offers a theoretical framework for cultural comparisons across countries. Since it provides accessible independent variables to explain why behaviours vary among national culture, Hofstede's cultural typology has been extensively used in variety of studies across many disciplines and has been proven to be stable (Andrew and Habte, 2003; Milberg *et al.*, 1995; Milberg *et al.*, 2000; O Connor, 1995; Quaddus and Tung, 2002).

Hofstede investigated culture by surveying over 100,000 employees of IBM in more than 70 countries. His research focused on fundamental differences as part of national culture in the way in which people in various countries perceive and interpret their worlds. Based on the survey results, Hofstede characterized culture with five dimensions: power distance, uncertainty avoidance, individualism/collectivism, masculinity/femininity, long-term/short-term orientation.

Power distance refers to the degree to which individuals in a society expect and accept differences in power, wealth, and social status (Hofstede, 1991, 2001). High power distance cultures usually have centralized, top-down control, and thus individuals in high power distance cultures tend to accept a hierarchical order usually without any further justification. On the other hand, low power distance societies emphasize equality and empowerment. Consequently, people in low power distance societies strive for power equalization and demand justification for power inequalities.

It is reasonable to make an inference that power distance has obvious consequences for the way individuals build their organizations and societies. Thus, it can influence companies' information disclosures with respect to their privacy practice. That is, compared with high power distance cultures, companies in low power distance cultures tend to disclose more privacy policies to address customers' needs, recognizing that companies' privacy policies signal to customers about their fair information practices, and thus they help build trust and reduce information asymmetry.¹⁸ Therefore, the implementation of FIP principles in privacy policy statements varies between low power distance countries and high power instance countries. This leads to the following hypothesis.

H11: Companies in low power distance countries incorporate more FIP principles in their privacy policy disclosures than do companies in high power countries.

¹⁸ Information asymmetry, often called asymmetrical information, indicates a condition in which one party to a transaction has more or better information than the other party. With respect to Internet privacy, it is the companies that know more about the collection and use of personal information than customers. This causes inequality between companies and customers since customers do not have full access to the information they need for their decision making processes.

Uncertainty avoidance is about the extent to which an individual in a society feels threatened by ambiguous, uncertain situations and tries to avoid them. It indicates the preference of a society for strict laws and regulations over ambiguity and risk. According to Hofstede (2001, p. 161), high uncertainty avoidance societies have a low tolerance for uncertainty and ambiguity of any deviations from group or organizational norms and thus tend to develop many rules to control social behaviours whereas low uncertainty avoidance societies need few rules to control social behaviours. Therefore, such differences, especially the preference for formal rules, can influence companies' privacy policies and thus cause the difference in their privacy policy disclosures between two cultures. In line with this idea, the following hypothesis is introduced.

H12: Companies in high uncertainty avoidance countries incorporate more FIP principles in their privacy policy disclosures than do companies in low uncertainty avoidance countries.

Individualism/collectivism indicates the extent which individuals emphasize self interests as opposed to those of the group. Therefore, individuals from collectivist cultures tend to have an emotional dependence on others and are more inclined to give up their individual needs when there is a conflict between their needs and the group's needs (Triandis, 1989). A key element of Internet privacy is about individuals having control over their personal information. Because individuals from collectivist cultures are more likely to accept organizational practices that will intrude on one's private life and thus have a greater tendency to sacrifice their privacy, it would be expected that people from collectivist cultures are less concerned about privacy than those from individualist cultures. Furthermore, such differences in individuals' privacy concerns and their expectations can put increasing pressure on companies to ensure the appropriate use and management of their

customers' personal information and, in turn, affect companies' privacy policies. Accordingly, the following hypothesis is examined.

H13: Companies in individualist cultures incorporate more FIP principles in their privacy policy disclosures than do companies in collectivist cultures.

Masculinity/femininity indicates the expected gender roles in a society. Masculine societies tend to have very distinct expectations in gender roles and value ambition, assertiveness, competitiveness, and the accumulation of wealth and material possessions. On the other hand, feminine societies prefer equality between male and female and place more value on relationship and quality of life such as helping others and sympathy for the unfortunate. According to the Vitell et al. (1993), individuals in masculine cultures are less likely to perceive ethical problems and less inclined to adhere to strict standards than individuals in feminine cultures. Therefore, it is expected that companies in masculine cultures are less concerned about their customers' privacy and thus have less rigorous privacy policies. The related hypothesis is as follows.

H14: Companies in feminine cultures incorporate more FIP principles in their privacy policy disclosures than do companies in masculine cultures.

Long-term/short-term orientation indicates whether societies' values are oriented towards the future or towards the past and present. In long-term oriented societies, thrift, perseverance, and future directed action are valued more. On the other hand, short-term orientation societies place more value on tradition, stability, and fulfilling social obligations. Since companies in short-term orientation cultures have more tendencies to fulfil social obligations, they tend to be concerned about privacy issues and thus implement more stringent privacy policies. Therefore, this study proposes the following hypotheses.

H15: Companies in short-term oriented cultures incorporate more FIP principles in their privacy policy disclosures than do companies in long-term oriented cultures.

5. A Gap in Perceived Importance of Companies' Privacy Policies: Privacy Gap Study

In the previous two chapters, several research questions from customer and company perspectives on Internet privacy were addressed. In chapter 3, the study, based on ELM, develops seven hypotheses that examine the effect of individuals' involvement with respect to the sensitivity of personal information and privacy policy disclosures on their privacy behaviour. In chapter 4, the study raises eight hypotheses about companies' privacy policy disclosures at the country, culture, and industry levels. Answers to the hypotheses in chapter 3 will explain whether certain factors (i.e., individuals' involvement and privacy policy disclosures) affect individuals' privacy behaviour with respect to reading privacy policy disclosures and providing personal information as well as the difference between self-reported privacy behaviour and actual privacy behaviour. On the other hand, answers to the hypotheses in chapter 4 will show how companies perceive individuals' privacy and how they protect individuals' privacy through their privacy policy disclosures. In this chapter, these two perspectives are linked.

As discussed earlier, Fair Information Practices (FIP) is a general term for a set of standards governing how information should be collected, used, and protected. Many companies have developed their privacy policies based on FIP principles and have provided statements about their privacy policies on their Web sites. What is not clear, however, is the manner by which individuals perceive companies' privacy policies and whether companies' privacy policy disclosures address privacy policies that Individuals want to know. Knowing the gap between individuals' perceived importance of companies' privacy policies and what companies emphasize in their privacy policy disclosures will help in the assessment of whether current company privacy policy disclosures adequately address individuals' privacy concerns.

A number of studies have shown that customers are more inclined to trust a Web site if it provides a privacy policy disclosure (Culnan and Armstrong, 1999; Earp and Baumer, 2003;

Miyazaki and Fernandez, 2000; Palmer et al., 2000). However, only a few studies examined whether customers' privacy concerns are adequately addressed in companies' privacy policy disclosures. For instance, based on findings from prior literature, Sheehan and Hoy (2000) came up with five influences that might reflect the underlying dimensions of customers' privacy concerns and examined whether FTC fair information practice principles reflect these five influences. They found that the FTC fair information practice principles reflect three influences on customers' privacy concerns (i.e., awareness of information collection, information usage, and information sensitivity), but not two influences (i.e., the exchange of information for appropriate compensation and the relationships between entities and online users). Earp et al. (2005) studied a gap between the information provided in companies' privacy policy statements and the information that users want to know about Internet privacy. They found that the information addressed in Web site privacy policy statements does not fully provide the information that users want to know.

Although the studies conducted by Sheehan and Hoy (2000) and Earp et al. (2005) take up for the question of whether FTC principles adequately address the underlying dimensions of customers' privacy concerns and whether customers' privacy concerns are adequately addressed in companies' privacy policy statements, there are still other unanswered questions such as 1) whether customers' privacy concerns are adequately addressed in other FIP principles (e.g., OECD principles); and 2) whether companies' privacy policy statements include FIP principles that are most central to consumers. This study primarily differs from the study conducted by Sheehan and Hoy (2000) that tries to explain whether FTC's core principles reflect the underlying dimensions of customers' privacy concerns. The objective of Sheehan and Hoy is the opposite of what this study intends: it tries to explain whether customers' concerns are addressed in companies' privacy policy statements using FIP principles. This study also differs from Earp et al. (2005). While Earp and his colleagues investigated the gap between what users value and what companies' privacy policies emphasize based on FTC principles, the gap based on OECD

principles is examined. Furthermore, this study explores whether customers and companies perceive each OECD principle differently due to the nature of personal information (e.g., sensitive versus non-sensitive information).

Individuals do not have the same privacy concerns about all personal information pertaining to them. Individuals have different privacy preferences for different kinds of personal information, and their preferences depend on the context in which this information is collected and used (Petty, 2000; Phelps et al., 2000; Sheehan and Hoy, 2000). For example, individuals may be less willing to disclose their financial information such as credit card number, and their major concerns might be reasonable security safeguards against risks such as unauthorized access or disclosure of the information. On the other hand, others may be more willing to disclose their purchasing preferences, and their major concerns might be the purpose of collecting personal information. Therefore, it is possible that individuals perceive certain privacy policies as more important when they are asked sensitive personal information compared to less sensitive personal information. Given that companies' privacy policies are developed based on FIP principles, the following hypothesis is suggested.

H16: Individuals' perceived importance of FIP principles differs depending on the type of information requested.

It is also possible that individuals perceive FIP principles as having a different importance when they are requested to provide their personal information in financial or health Web sites (i.e., information-sensitive industries) when compared to manufacturing or retail Web sites (i.e., less information-sensitive industries). Accordingly, this study proposes the following hypothesis.

H17: Individuals' perceived importance of FIP principles differs depending on the type of Web site.

Prior studies reveal that companies' privacy policies stated in privacy policy statements help build trust and promote the disclosure of personal information by signalling customers about their fair information practices (Culnan and Armstrong, 1999; Milne and Boza, 1999). Since companies in information-sensitive industries collect and use personal information that leads individuals' concerns about their privacy, their privacy policy disclosures may differ from companies in less information-sensitive industries. For instance, online banking sites may put more emphasis on security issues in their privacy policy disclosures than do online shopping sites because customers are often requested to provide their sensitive information such as credit card number and SIN (Social Insurance Number). Therefore, the related hypothesis is as follows.

H18: Companies in information-sensitive industries perceive FIP principles as having a different importance when compared to less information-sensitive industries.

Furthermore, it is anticipated that companies may develop their privacy policy statements to address customers' concerns, recognizing the fact that a good privacy protection has a positive impact on them, but a poor privacy protection can increase their risks (e.g., lawsuit from customers and loss of customers). Accordingly, the following final hypothesis is suggested.

H19: Companies incorporate more FIP principles that individuals perceived as important principles in their privacy policy disclosures than FIP principles that individuals perceived as less important.

6. Research Methodology

The study conducted a Web-based user survey, online purchasing experiment, and a Web site survey and performed analyses using regression, analysis of variance, and non-parametric tests to investigate the research hypotheses.

6.1. An Overview of Research Stages

This study was done in three stages, the first two involving individuals' behaviour and the third concerning companies' privacy policies. Figure 3 illustrates these stages with the related hypotheses.

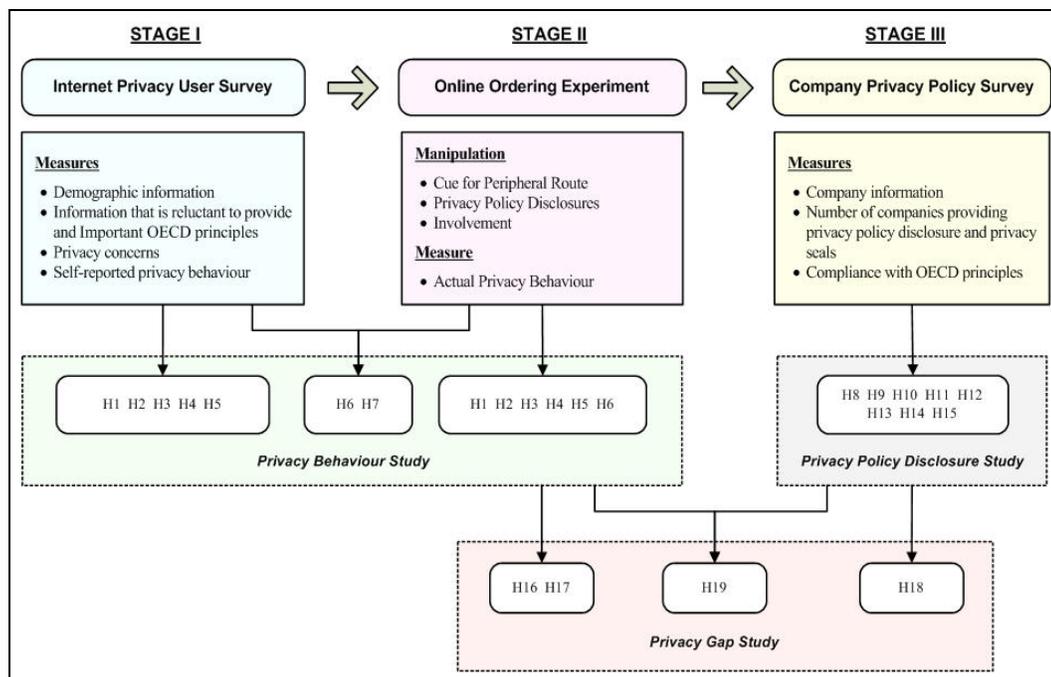


Figure 3: Three Research Stages with Hypotheses

In the privacy behaviour study, five hypotheses (H1, H2, H3, H4, and H5) were introduced to investigate whether involvement influences individuals' self-reported privacy behaviour. To examine these hypotheses, stage I (named as *Internet privacy user survey*) was designed to capture individuals'

self-reported privacy behaviour, including demographic information, privacy concerns, information that individuals feel reluctant to provide, and importance ratings of FIP principles. The customer's actual privacy behaviour was measured in stage II (named as *online ordering experiment*), and the same five hypotheses were investigated for the effect of involvement on individuals' actual privacy behaviour. Then, by comparing actual privacy behaviour with self-reported privacy behaviour, two hypotheses (H6 and H7) were investigated.

In the privacy policy disclosure study, eight additional hypotheses (H8, H9, H10, H11, H12, H13, H14, and H15) were investigated to address companies' privacy policies stated in their privacy policy statements. In stage III (named as *company privacy policy survey*), 420 companies' Web sites were surveyed to capture the content of privacy policy disclosures as well as the compliance of the disclosures with OECD principles.

Finally, in the privacy gap study, the measures from both stage I and III were used to explore four research hypothesis (H16, H17, H18, and H19), pertaining to a gap between individuals' importance ratings of OECD principles and the frequently addressed OECD principles in companies' privacy policy statements.

6.2. Privacy Behaviour Study

The privacy behaviour study was conducted to examine how an individual's privacy behaviour is affected by privacy policy disclosures and by the level of the individual's involvement regarding the sensitivity of personal information. In particular, two privacy behaviours were investigated in this study: 1) information search regarding companies' privacy practices and 2) decision to provide personal information. This study also examined a gap between self-reported privacy behaviour and actual privacy behaviour with respect to two privacy behaviours.

6.2.1. Procedures

Research participants were first provided general information about the study and randomly assigned to experimental groups. Then, they were asked to complete the Internet privacy questionnaire (named as *Internet privacy user survey*). A questionnaire was developed to probe participants' concerns regarding various aspects of Internet privacy. The questionnaire consisted of four sections. The first section was designed to gather the demographic information. The second section was developed as part of the manipulation for an online ordering experiment. In this section, participants were asked to identify the type of information that they feel reluctant to provide as well as important companies' privacy policies which they want to know. The third section measured individuals' privacy concerns. The final section was designed to measure self-reported privacy behaviour. A pretest and a pilot test were conducted, and as a result, a total of 50 questions were finally developed. Except for demographic questions such as age, gender, and ethnicity, most questions were measured using a seven-point scale. Appendix II contains the Internet privacy user survey questionnaire. A Web-based survey was employed because it provides the ability to skip questions based on previous answers and allows greater design flexibility and data control. The survey was hosted on a university server, and in the anticipation of potential server problems, a mirrored site was also put up at another university server.

After the participants completed the Internet privacy user survey, they were informed that a gift was being provided as a token of appreciation for participation and were directed to an online ordering site. The second stage (named as *online ordering experiment*) was designed to gather information on actual privacy behaviour while participants were performing an online ordering task. The task required participants to order a free gift from an experimental site and provide personal information to complete their order. The content of the site was a gift site that people can use to order goods such as gift tickets, books, and music CDs.¹⁹ The free gift was actually sent to the

¹⁹ Participants were made aware that the site is not part of the Internet privacy user survey site and also informed that the responsibility for using Gift4U rests with them. Both Web site design and the ordering process of the site were developed based on the real online ordering process of a well-known e-commerce site

address that each participant provided during the ordering process. Appendix III contains the online experimental site and also illustrates each step involved in the online ordering task.

Finally, after participants completed the online ordering task, they were asked to complete a debriefing questionnaire (named as *debriefing*). Appendix IV shows the debriefing questionnaire. The debriefing questionnaire was developed to check experimental manipulations and to validate participants’ understanding of the task. In particular, for the involvement manipulation check, the Personal Involvement Inventory (PII), developed by Zaichkowsky (1985), was adapted to measure participants’ involvement with their experimental condition using a seven-point scale. Only five questions from the PII were employed in this study because the remaining 15 questions did not match with the context of the study. The five items used for the involvement manipulation check are shown in Figure 4.

DEBRIEFING 5 / 5 PAGE

Please Indicate your level of **AGREEMENT**.

NOTE: Make each item a separate and independent judgment. Work at fairly high speed through this questionnaire. Do not worry or puzzle over individual items. It is your first impressions, the immediate feelings about the items, that we want. On the other hand, please do not be careless, because we want your true impressions.

While I was providing personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*) at Gift4U, to me privacy was

1 2 3 4 5 6 7

| | | | | | | | | |
|-----------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| Important ◀ | <input type="radio"/> | ▶ Unimportant |
| Relevant ◀ | <input type="radio"/> | ▶ Irrelevant |
| Means nothing ◀ | <input type="radio"/> | ▶ Means a lot to me |
| Involving ◀ | <input type="radio"/> | ▶ Uninvolving |
| Not needed ◀ | <input type="radio"/> | ▶ Needed |

Previous Next

* The question was automatically generated based on each participant’s experimental condition.

Figure 4: Involvement Manipulation Check

(i.e., Amazon.com). Furthermore, an actual URL (i.e., www.Gift4U.ca) was used for the site. That is, the experimental site was designed to create a realistic situation in order to elicit actual behaviour.

6.2.2. Design and Manipulation

A 2×3 between-subject experiment was designed with *INVOLVEMENT* and *PRIVACY POLICY DISCLOSURE* being manipulated. For each self-reported behaviour and actual privacy behaviour, two privacy behaviours were measured and used as dependent variables. Table 1 summarizes the experimental design.

Table 1: Experimental Design

| | | PRIVACY POLICY DISCLOSURE | | |
|-------------|------------------|---|--|--|
| | | <i>Privacy Seal & Privacy Policy Statement (SEAL)</i> | <i>Privacy Policy Statement (POLICY)</i> | <i>No Privacy Policy Disclosure (NONE)</i> |
| INVOLVEMENT | <i>High (HI)</i> | HI_SEAL | HI_POLICY | HI_NONE |
| | <i>Low (LI)</i> | LI_SEAL | LI_POLICY | LI_NONE |

* The name of each experimental group (i.e., HI_SEAL, HI_POLICY, HI_NONE, LI_SEAL, LI_POLICY, and LI_NONE) will be used through the thesis.

6.2.2.1. Involvement Manipulation

Studies showed that the type of information requested has an effect on customers' privacy concerns (e.g., Ackerman et al., 1999; Earp and Baumer, 2003) and purchase intentions (e.g., Malhotra et al., 2004; Phelps et al., 2000). Since individuals' privacy concerns and decisions about information disclosure are influenced by the type of personal information requested, involvement was manipulated based on the sensitivity of personal information. The involvement manipulation was implemented through the Internet privacy user survey (Stage I) and the online ordering experiment (Stage II). Figure 5 shows the link between the two stages.

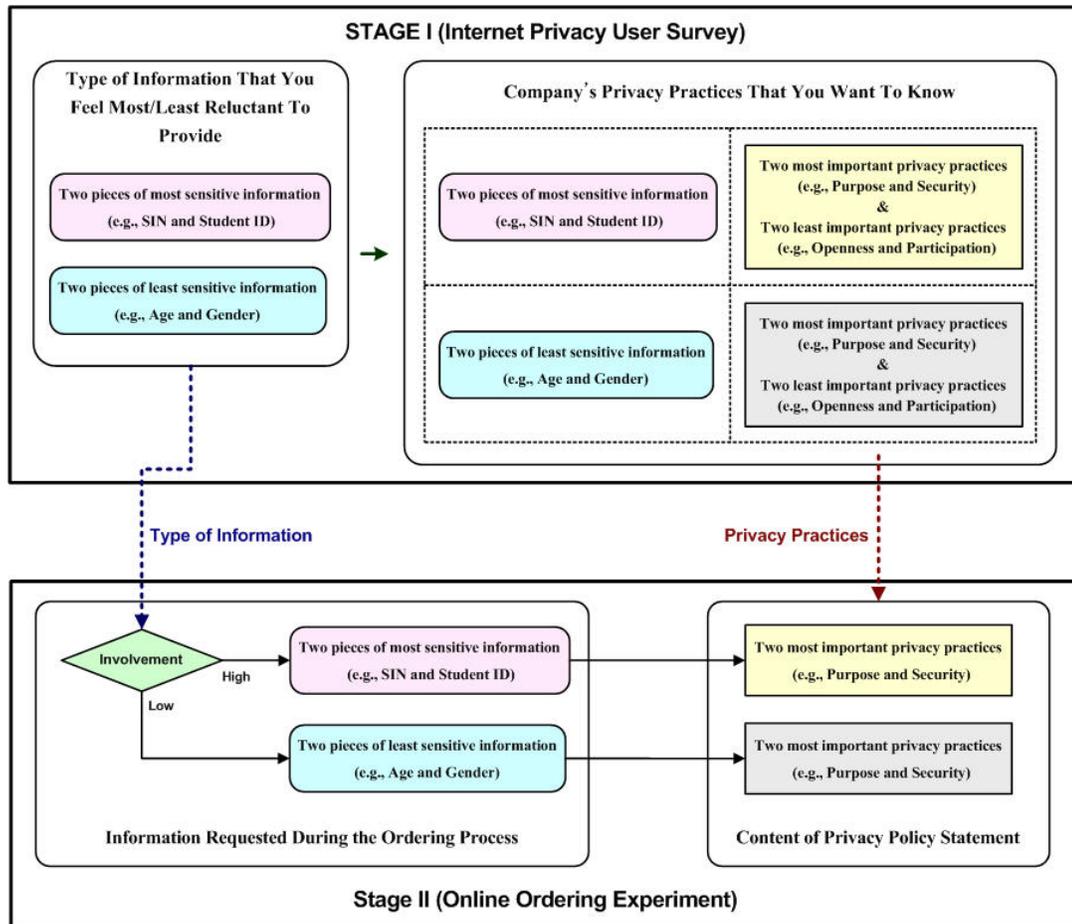
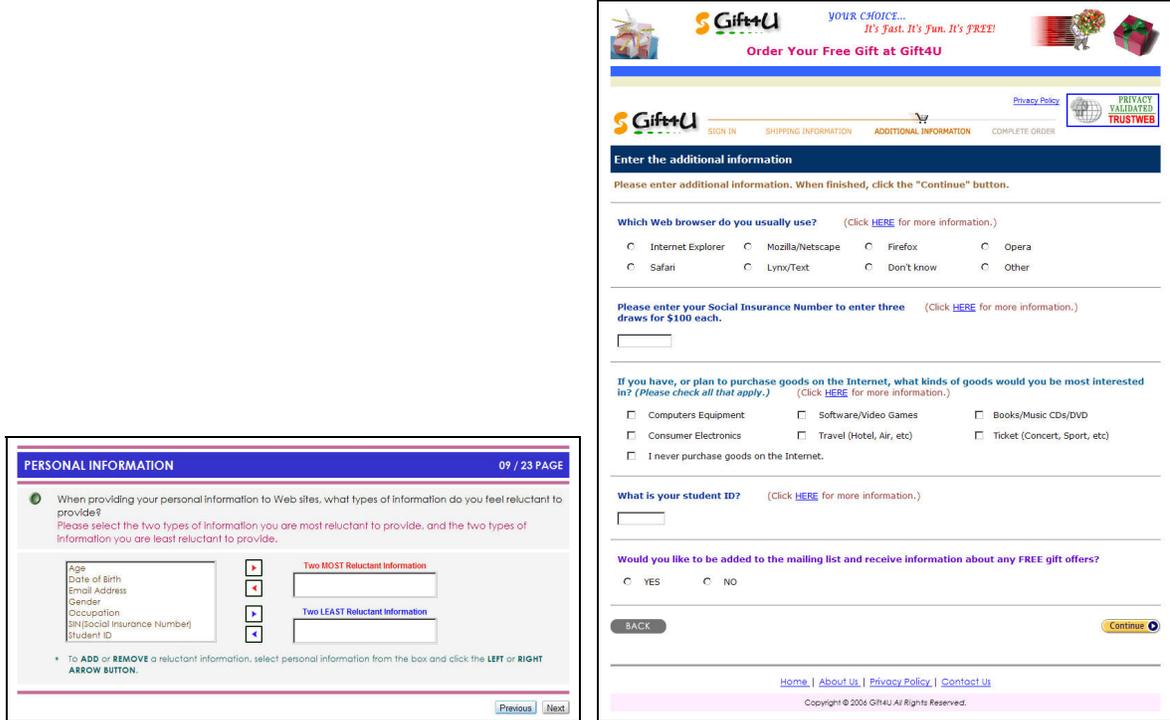


Figure 5: Detailed link between Internet privacy user survey and Online Ordering Experiment

Assume that in stage I, a participant answered that *Student ID* and *SIN* are two pieces of personal information that he or she feels the most reluctant to provide, but *Age* and *Gender* are two pieces of information that he or she feels the least reluctant to provide (see Figure 6.a). In stage II, such information was used to manipulate involvement conditions (the dotted arrow labelled type of information in Figure 5). That is, if the participant were in the high involvement group, he or she was requested to provide *Student ID* and *SIN* during the ordering process (see Figure 6.b). On the other hand, if the participant were in the low involvement group, his or her *Age* and *Gender* were asked. Thus, the high involvement condition was expected to lead participants to consider their information privacy while making an information disclosure decision. With the low involvement condition, on the other hand, participants were expected to give less consideration to their information privacy.



a) Type of Information that One Feels Reluctant to Provide

b) Additional Information Page

Figure 6: Involvement Manipulation

6.2.2.2. Privacy Policy Disclosure Manipulation

The privacy policy disclosure was introduced to examine whether participants’ privacy behaviour is influenced by the type of privacy policy disclosure. The privacy policy disclosure was manipulated by presenting a privacy policy statement and a privacy seal. The content of the privacy policy statement was designed to lead participants to consider their information privacy.

One question was developed for this purpose. Depending on their experimental condition, respondents were requested to identify the two most important and two least important company’s privacy practices that they want to know from the list of privacy policies developed based on OECD principles (see Figure 7.a).²⁰ The response of each participant was used to create a privacy policy statement (the dotted arrow labelled privacy practices in Figure 5). For example, assume that a participant

²⁰ This study used the OECD principles because FIP principles developed by many countries were mostly based on the OECD principles (AICPA/CICA, 2004; Ashley et al., 2002b).

in the high involvement condition answered that he or she believed that the company should address the purpose of collecting personal information as well as security information in its privacy policy disclosure. In the experiment, such information was used to generate a privacy policy statement. That is, the purpose of collecting personal information and security information are not presented in the company's privacy policy statement (see Figure 7.b). On the other hand, participants in the non privacy policy disclosure condition were not presented the privacy policy statement.

a) Most Important and Least Important Privacy Practices

b) Privacy Policy Statement

c) Privacy Seal

Figure 7: Privacy Policy Disclosure Manipulation

In addition, the cue addressed in H3 and H4 was operationalized based on the existence of a privacy seal on the experimental site. Privacy seals are developed to build consumer confidence regarding privacy by sending a signal to customers that companies' privacy practices comply with effective privacy practices (Miyazaki and Krishnamurthy, 2002; Moores, 2005; Palmer et al., 2000). Although several Internet seal programs exist in various forms, the majority of companies involved in such programs currently participate in one of three dominant programs: TRUSTe, BBBOnline, and WebTrust (Moores and Dhillon, 2003; Palmer et al., 2000). BBBOnline, TRUSTe, and WebTrust have, respectively, 707, 2,598, and 25 participants in their privacy seal of approval programs as of October 2006 (BBBOnline, 2006; TRUSTe, 2006; WebTrust, 2006).

Although a firm's participation in a seal program may favourably influence customers' perceptions of its privacy practices and the level of information disclosure, Moores (2005) found that few people consider privacy seals as important in deciding to trust a Web site. Moores also found that quite a number of participants did not know how a seal is obtained and failed to recognize genuine privacy seals even though they have a basic understanding about privacy seals and about the function of seals. Since all individuals may not be familiar with a specific privacy seal, it is possible that the awareness of the privacy seal may influence the online ordering experiment. Hence, a contrived seal was used in this study, similar to the TRUSTe seal (see Figure 7.c). As a result, the privacy policy disclosure condition consisted of three levels: *Privacy Seal & Privacy Policy Statement (SEAL)*, *Privacy Policy Statement (POLICY)*, and *No Privacy Policy Disclosure (NONE)*.

6.2.3. Measurement

Privacy behaviour was measured in two ways: *Self-reported Privacy Behaviour* and *Actual Privacy Behaviour*. When individuals are requested to provide personal information and are concerned about their privacy, they are assumed to examine the privacy policy statement and the privacy seal posted on a Web site and make a decision about providing their personal information. Thus, this study defines

privacy behaviour as 1) the process of searching and evaluating information about companies' privacy policies and 2) making a decision about personal information disclosure. Table 2 shows the privacy behaviour measures.

Table 2: Privacy Behaviour Measurement Items

| Self-reported Privacy Behaviour | |
|---------------------------------|---|
| ITEM 1 | <ul style="list-style-type: none"> I would read the privacy policy statement of the Web site when it requests [<i>two pieces of personal information</i>]. |
| ITEM 2 | <ul style="list-style-type: none"> During the past 6 months, did you read the privacy policy statement of the Web site when it requested [<i>two pieces of personal information</i>]? |
| ITEM 3 | <ul style="list-style-type: none"> How likely would you be to complete this form when [<i>two pieces of personal information</i>] are requested? If the Web site had a privacy policy statement, how likely would you be to complete this form when [<i>two pieces of personal information</i>] are requested? If the Web site had a privacy policy statement and a privacy seal how likely would you be to complete this form when [<i>two pieces of personal information</i>] are requested? |
| ITEM 4 | <ul style="list-style-type: none"> I would provide my [<i>two pieces of personal information</i>] when the Web site's privacy policy does NOT address [<i>two important company privacy practices</i>] as defined above. |
| ITEM 5 | <ul style="list-style-type: none"> During the past 6 months, did you provide your [<i>two pieces of personal information</i>] when the Web site's privacy policy does NOT address [<i>two important company privacy practices</i>] as defined above? |
| Actual Privacy Behaviour | |
| ITEM 6 | <ul style="list-style-type: none"> Does the participant click the privacy policy statement of Gift4U? |
| ITEM 7 | <ul style="list-style-type: none"> How long does the participant open the privacy policy statement of Gift4U? |
| ITEM 8 | <ul style="list-style-type: none"> Does the participant provide his or her true personal information? |
| ITEM 9 | <ul style="list-style-type: none"> Does the participant click the TRUSTWEB page of Gift4U? |
| ITEM 10 | <ul style="list-style-type: none"> How long does the participant open the TRUSTWEB page of Gift4U? |
| * | Scale: Item 1 – 5 (a seven-point scale) Item 6, 8, and 9 (Yes / No) Item 7 and 10 (Number of seconds) |
| ** | [<i>Two pieces of personal information</i>]: Participants in the high involvement group were requested to provide two pieces of sensitive personal information while those in the low involvement group were asked to provide two pieces of least sensitive personal information (see Figure 5 and Appendix II – Internet Privacy Users Survey Page 9). |
| *** | [<i>Two important company privacy practices</i>]: Two most important company's privacy practices that participants want to know when they asked to provide two pieces of personal information (see Figure 5 and Appendix II – Internet Privacy Users Survey Page 10). |

6.2.3.1. Self-reported Privacy Behaviour

Self-reported privacy behaviour was measured by asking a series of questions about how individuals act in a given situation. Assume that a participant was in HI_POLICY group. Also, he or she answered that *student ID* and *SIN* were the two most sensitive personal information items and that the company should address the *purpose* of collecting personal information as well as *security* information in its privacy policy disclosure. A scenario was automatically generated using his or her answers, and then the respondent was asked questions (ITEM 3) designed to measure whether he or she would provide his or her personal information in the given scenario (see Figure 7.a).

Furthermore, four additional questions were employed to elicit individuals' behaviour in a given condition (see Appendix II – Internet privacy user survey page 17). ITEM 1 was designed to capture whether respondents were willing to read a privacy policy statement, and ITEM 2 was developed to assess their past behaviour with respect to reading a privacy policy statement in a given involvement condition. ITEM 4 and ITEM 5 were used to examine whether individuals provide their personal information when the privacy policy statement does not address privacy policies that they have indicated are important to them. ITEM 4 was designed to measure individuals' willingness to provide personal information, and ITEM 5 was designed for their past behaviour related to providing personal information.

6.2.3.2. *Actual Privacy Behaviour*

Actual privacy behaviour was measured based on participants' behaviours in a given experimental condition (see Appendix III). This study defines actual privacy behaviour as a series of behaviours that individuals perform while they make a decision about personal information disclosure. Five actions were examined to measure privacy behaviour (i.e., ITEM 6 – ITEM 10 in Table 2): 1) whether the participant clicked to open the privacy policy statement; 2) the amount of time spent in the Web page containing the privacy policy statement; 3) whether the participant clicked to open the privacy seal; 4) the amount of time spent in the Web page describing the privacy seal; and 5) whether the

participant provided his or her personal information.²¹ These five actions were automatically captured and stored into the database while participants were performing the ordering task.

6.2.4. Participants

A total of 210 students participated in the study. According to Bellman et al. (1999), student subjects provide a reasonable surrogate for online consumers because online consumers tend to be more educated and younger than the general population. Therefore, this study considers student subjects as an appropriate sample even though it is suggested to take precaution when interpreting results obtained from samples of students since unpredicted differences could appear in the initially established theoretical relations (Peterson, 2001). The sampling frame consisted of 559 students at two large universities. The participants were recruited from four undergraduate and two graduate courses where the researcher was allowed to ask for participation. The researcher visited each classroom and briefly introduced the purposes and procedures of the study along with a recruitment letter. Over a month, 267 students visited the survey site.²² Among them, 11 did not provide any information, 23 did not finish the Internet privacy user survey (Stage I), 8 did not complete the online ordering experiment (Stage II), and 6 did not finish the debriefing. In addition, 9 participants were excluded because they did not pass the manipulation

²¹ ITEM 8 deserves attention because individuals might fabricate their personal information when they are concerned about privacy. That is, when respondents are requested to provide sensitive information, they are more willing to fabricate their personal information compared to when they are asked to provide less sensitive information. In the experiment, participants were asked five mandatory questions (see Figure 6.b). Three questions were filler questions: *name of Web browser they usually use*, *type of products they plan to purchase in the near future*, and *whether they want to be added to the mailing list*. These questions are generally used in online shopping sites and used to deter the focus of respondents on their privacy. Therefore, the three filler questions were not scored. Two other questions were about two pieces of information that they had identified during the Internet privacy user survey. However, when they are requested to provide sensitive information such as SIN, it is possible that some participants fabricated their information due to their privacy concerns. Therefore, this study examined whether they fabricated information. For SIN and student ID, a JavaScript was developed to check whether they were valid. For other information (i.e., age, date of birth, email address, gender, and occupation), participants' answers in stage I were compared with what they provided in stage II. As a result, the actual behaviour measure reflects whether participants provided their 'true' information.

²² Participants in the study were asked to indicate their consent as well as to provide their name, student ID, and email address. Such information was used to avoid an individual participating in the study more than once.

check.²³ Accordingly, the final sample consisted of 210 valid responses and the response rate was 38 percent. On average, it took 43 minutes for participants to complete all three stages: 29 minutes for stage I, 9 minutes for stage II, and 5 minutes for debriefing.

6.3. Privacy Policy Disclosure Study

To examine companies' privacy policy disclosures across countries and industries, 420 companies' Web sites were examined to assess the content of privacy policy statements. The study adopted procedures similar to those implemented in FTC (2000). A total of twelve trained graduate students (hereafter, surfers) were hired to conduct the Web site survey. Two surfers were assigned per country. The assigned surfers were able to fluently communicate in English as well as in the language of the assigned country (in the case of China, Japan, and Germany). Questions were independently answered by the surfers, and then differences in the responses, if any, were reconciled, as was the procedure with FTC (2000). The data collection was done using a Web-based survey because it not only provides the ability to skip questions based on previous answers but also can reduce coding errors. The survey was hosted on a university server, and in the anticipation of potential server problems, a mirrored site was also put up at another university server.

6.3.1. Procedures

The Web site survey was conducted in three phases. In the first phase, all surfers received considerable training and practice in examining companies' privacy policy disclosures (i.e., privacy policy statements). Each surfer participated in a three-hour training session. The training session was intended to explain the entire survey procedures, skills required to visit and review Web sites, and the use of Web-based survey. In the second phase (named as *Web site survey*), a list of companies' Web sites of

²³ Privacy policy disclosure was one of the experimental manipulations. Nine participants did not properly indicate their experimental condition in the debriefing stage. For instance, 5 respondents who were in the privacy seal condition stated that they did not recognize the privacy seal.

each country was provided to a pair of assigned surfers. The sites were drawn from Mergent Online (formerly Moody's Online). Mergent Online is an online resource for global business and financial information including a fully searchable database of over 35,000 companies worldwide (Mergent Online, 2006). The total list of companies extracted from this database was: Canada (2,785), China (1,347), Japan (2,208), Germany (1,043), U.K. (2,241), and U.S. (9,812). For each country, the top 50 largest companies from information-sensitive industries and another top 50 from less information-sensitive industries were selected. As with literatures in the past, this study defined "large" by the number of employees and information-sensitive industries to include finance, insurance and real-estate (SIC major group 60 to 65 and 67), and health-care (SIC major group 80).

Surfers conducted the survey in two rooms. Only surfers and proctors were allowed to use the rooms and computers. Also, each surfer was given an ID and password to access the survey Web site, so that the study could control the access to the survey Web site and capture extra information such as time taken for the survey and the time required to reconcile answers. Each surfer in the pair independently accessed each Web site to search for its privacy policy disclosures and to print privacy policy disclosures. After each pair completed the Web site survey, they reconciled their answers for each site and compared the privacy policy disclosures.

To examine whether the companies' privacy policies address FIP principles, for each country, a set of 70 sites with privacy policy disclosures (35 for information-sensitive industries and 35 for less information-sensitive industries) was established.²⁴ Thus, if a pair of surfers for the assigned country failed to obtain enough sites with privacy policy disclosures, a list of additional companies' Web sites was provided until each pair reached the target size of 70 sites. In the final stage (i.e., *company privacy policy survey*), a list of 70 companies obtained from the Web site survey was provided to both surfers of the assigned country with companies' privacy policy disclosures. Appendix V shows the list of 420 Web sites. Each surfer then independently completed a privacy policy survey questionnaire. Once both surfers

²⁴ The number, 70 Web sites, was arbitrarily select to ensure enough statistical power for the study.

of the assigned country completed the survey, they reconciled their answers for each survey question. If they failed to reach an agreement, a third surfer was assigned and resolved the differences. The Web site survey, on average, took 47 minutes for each company: approximately 6 minutes for the Web site survey and 41 minutes for the company privacy policy survey.

6.3.2. Survey Items

A total of 50 questions were developed to capture whether companies' privacy policies stated in privacy policy statements address FIP. Since each country adopts different FIP, companies develop their privacy policy statements based on their country's FIP. To compare companies' privacy policies across six countries, OECD guidelines were used because most FIP developed by these countries were based on OECD guidelines (AICPA/CICA, 2004; Ashley et al., 2002b). All sixteen questions developed in FTC (2000) were adapted for this study. The remaining questions were created to address OECD guidelines that were not covered by FTC (2000).

First, the researcher carefully examined the guidelines and detailed comments of OECD guideline principles (henceforth, OECD principles) in 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (1980). Then, major requirements of each OECD principle were identified. Based on these requirements, survey items for each OECD principle were developed. For example, Table 3 describes the guideline and detailed comment regarding *Use Limitation* principle. By analyzing the guideline and detailed comment, two major requirements with respect to *Use Limitation* principle were identified. Next, three questions based on requirements were created. Table 4 showed two major requirements and three survey questions for *Use Limitation* principle.

Table 3: Guideline and Detailed Comment of Use Limitation Principle

| | |
|-------------------------|---|
| Guideline | Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law. |
| Detailed Comment | This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative – see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning. |

Table 4: Survey Questions for Use Limitation Principle

| Main Points | Questions |
|---|---|
| <ul style="list-style-type: none"> • Do not disclose and make personal data available or otherwise used for purposes other than those specified except: <ul style="list-style-type: none"> ▪ with the consent of the data subject; or ▪ by the authority of law • Disclose or make available personal data only for specified purposes unless the data subjects give their consent or it required by the authority of law. | <p>Q10. Does the Privacy Policy state anything about whether the domain does NOT use or disclose the collected personal information for a new (i.e., not previously specified) purpose without customers' consent?</p> <p>Q12. Does the Privacy Policy state anything about whether personal information is used ONLY for the purpose for which the information was obtained or compiled?</p> <p>Q21. Does the Privacy Policy state that if the domain gathers and combines personal information from more than one source, it ensures that the original purposes of collections have NOT changed?</p> |

Additionally, the careful examination of OECD guidelines and detailed comments of OECD principles was followed by qualitative research in an effort to further elicit major requirements of each OECD principle that might have been missed in the previous step (Straub et al., 2004). This qualitative research was conducted through reviews with a panel of experts to assure the study had adequately tapped into each OECD principle.²⁵ Furthermore, 7 graduate students conducted a pilot test to identify any ambiguous questions and assess the length of time

²⁵ The panel consisted of two privacy experts (one lawyer and one professor) and two survey experts (one professor in sociology and one professor in statistics).

needed to complete the questionnaire. Following the pilot test, some minor changes were made to the questionnaire to improve questionnaire flow and respondent comprehension. Feedback from these processes resulted in 50 survey items. The survey items are provided in Appendix VI.

6.3.3. Measures

Six countries were coded as a categorical variable (COUNTRY): U.S. (0), Canada (1), U.K. (2), Germany (3), Japan (4), and China (5). Industry was coded as ‘0’ (less information-sensitive industries) and ‘1’ (information-sensitive industries). In addition, three measures were required to evaluate eight hypotheses in the privacy policy disclosure study (see Figure 3). These measures were a government involvement measure, a measure of culture, and the number of OECD principles addressed in a company’s privacy policy disclosure. For the government involvement, based on the country classifications identified by Milberg, Smith, and Burke (2000), this study classified six countries according to the regulatory approach model in Figure 2. Similarly, the five cultural dimension scores developed by Hofstede (1991, 2001) were adopted as the measure of culture for each country. Table 5 shows these measures.

Table 5: Culture and Government Involvement Measures

| Country | Culture* | | | | | Government Involvement** |
|---------|----------------------|-----------------------------|---------------------|-------------------|-----------------------------|--------------------------|
| | Power Distance (PDI) | Uncertainty Avoidance (UAI) | Individualism (IDV) | Masculinity (MAS) | Long-Term Orientation (LTO) | |
| U.S. | 40 | 46 | 91 | 62 | 29 | 2 |
| Canada | 39 | 48 | 80 | 52 | 23 | 3 |
| U.K. | 35 | 35 | 89 | 66 | 25 | 4 |
| Germany | 35 | 65 | 67 | 66 | 31 | 3 |
| Japan | 54 | 92 | 46 | 95 | 80 | 2 |
| China | 80 | 30 | 20 | 66 | 118 | 0 |

* Hofstede (1991, 2001) or www.geert-hofstede.com

** Governmental Involvement (Milberg et al., 2000, p. 44)

Finally, the number of OECD principles addressed in a company’s privacy policy statement was measured based on the privacy policy disclosure survey results. The eight principles of OECD guideline include *Accountability (AC)*, *Collection Limitation (CL)*, *Data Quality (DQ)*, *Individual Participation (IP)*, *Openness (OP)*, *Purpose Specification (PS)*, *Security Safeguards (SS)*, and *Use Limitation (UL)*. Table 6 summarizes the eight OECD principles and questions used to measure each OECD principle.

Table 6: Eight Principles of OECD Guideline and Survey Questions

| Principle | Description | Survey Questions | Max. Score |
|-------------------------------|---|-------------------------|-------------------|
| Accountability (AC) | Who is responsible for the Web site’s policies and practices and for complying with measures which give effect to the principles | Q38 Q39 | 2 |
| Collection Limitation (CL) | Whether the site collects only necessary information and obtains consent before the collection | Q5 Q6 Q8 Q9 | 4 |
| Data Quality (DQ) | Whether the site makes sure that personal data is relevant to the purposes for which they are to be used and collected data is accurate, complete, and kept up-to-date | Q34 Q35 Q36 | 3 |
| Individual Participation (IP) | Whether the site addresses the right of individuals to access and challenge personal data such as allowing users to challenge the accuracy of the information and having it amended | Q23 Q24 Q26 Q27 Q28 Q40 | 6 |
| Openness (OP) | Whether the site makes available to users specific information about its privacy policies and practices with respect to personal information | Q25 Q37 | 2 |
| Purpose Specification (PS) | What information the site collects and what it is going to do with the information | Q2 Q3 Q4 Q7 Q13 | 5 |
| Security Safeguards (SS) | How well the site protects personal information against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. | Q29 Q30 Q31 Q32 Q33 | 5 |
| Use Limitation (UL) | Whether the site uses the information only for purposes for which it was collected except with the consent of users or by the authority of law. | Q10 Q12 Q21 | 3 |

* All questions are available on Appendix VI.

All questions were True/False questions coded as ‘1’ for True and ‘0’ for False. The score of each OECD principle was calculated by adding each question. For instance, if a company’s privacy policy statement explains its practice about CL principle (i.e., Q5 - the domain limits its collection of

personal information to what is necessary for specified purposes), one point is assigned to CL score. Thus, the company will be assigned the maximum four of CL score if the company's privacy policy statement addresses all four questions (Q5, Q6, Q8 and Q9). On the other hand, if none of the information is described in the privacy policy statement, CL score will be zero. Accordingly, the maximum scores of each OECD principle are AC(2), CL(4), DQ(3), IP(6), OP(2), PS(5), SS(5), and UL(3). The sum of each principle score represents the OECD principle score, and thus the maximum OECD principle score is 30.

6.4. Privacy Gap Study

The individuals' perceived importance of OECD principles was measured for H16, H17 and H19. Based on the respondents' answers about information that they feel the most and least reluctant to provide, several questions were automatically generated to assess their perceived importance of OECD principles in an online shopping site and a banking site (see Appendix II – Internet privacy user survey page 10 and 11). Particularly, a randomly selected half of the participants (i.e., 105 respondents) were requested to identify the two most important and the two least important company's privacy policies from the list of privacy policies developed based on OECD principles when they asked to provide two pieces of information that they feel *most* reluctant to provide in an online shopping site. On the other hand, the rest of participants (i.e., 105 respondents) were requested to identify the two most important and the two least important company's privacy policies when asked to provide two pieces of information that they feel *least* reluctant to provide in an online shopping site. Same questions were also asked to each participant for an online banking site. Then, the scores of most important privacy policy and least important privacy policy were calculated by counting the answers of each respondent.

In addition, this study identified the rank order of eight OECD principles across six countries. Since the number of questions used to measure for each OECD principle was not the

same, the proportion score of each OECD principle was calculated. That is, each OECD principle score was converted into a score scale from 0 to 1 based on the proportion of a principle mean score to its maximum score. For instance, the mean scores of AC and CL principles in U.S. were .66 and .54, and the maximum scores of both principles were 2 and 4, respectively (see Table 6). Each proportion score was calculated by dividing each mean score by its maximum principle score. Thus, the proportion score of AC principle was .33 ($= .66/2$) and that of CL principle was .14 ($= .54/4$). Then, the rank order of proportion scores was determined and used to assess H18 and H19.

7. Research Results

In this section, the results of the study are addressed. First, the analysis of the Internet privacy study is discussed with the results of seven hypotheses which examine the effect of involvement on individuals' privacy behaviour. This is followed by the analysis of the privacy policy disclosure study and the results of eight hypotheses which assess companies' privacy policies stated in their privacy policy statements across six countries. Finally, the results of four research hypotheses in the privacy gap study are discussed.

7.1. Internet Privacy Study

An analysis of variance (ANOVA) and non-parametric tests, such as Chi-square and Wilcoxon signed-rank test, were conducted to assess whether there is a difference in individuals' privacy behaviour among experimental groups. In particular, the study assessed individuals' privacy behaviour in terms of *Reading Privacy Policy Statement* and *Providing Personal Information*.

7.1.1. Manipulation Checks

The results of the debriefing questionnaire suggest that all the participants correctly indicated their privacy policy disclosure conditions (i.e., existence or absence of privacy policy statement and privacy seal). The results also indicates that respondents were satisfied with their experience with the experimental site ($M = 4.73$ and $SD = 1.78$). However, their stratification varied depending on their involvement condition. As expected, the ANOVA test shows that respondents in the high involvement condition were less satisfied than those in the low involvement condition ($F_{(1, 208)} = 11.375, p = .001$). Many participants in the high involvement condition stated that they were not comfortable about Gift4U asking for their sensitive information. Finally, the results indicate that respondents in the high

involvement condition were more involved with privacy than those in the low involvement condition ($F_{(1, 208)} = 85.980, p < .001$). Hence, the involvement manipulation was successful.

7.1.2. Descriptive Statistics

A total of 210 students participated in the Web-based user survey. The demographic information of survey participants is shown in Table 7.

Table 7: Demographic Information of Participants

| Characteristics | | | Characteristics | | |
|---|------------------|--------------|---|--------------|--------------|
| | | <i>N</i> (%) | | | <i>N</i> (%) |
| Gender | Male | 137 (65.2%) | Privacy Policy Statement Experience | Yes | 179 (85.2%) |
| | Female | 73 (34.8%) | | No | 31 (14.8%) |
| Age | < 21 years | 105 (50.0%) | Number of Times Reading Privacy Policy Statement in the Past Twelve Months (<i>N</i> = 204) | None | 65 (36.3%) |
| | 21 – 30 years | 102 (48.6%) | | 1 statement | 44 (24.6%) |
| | > 30 years | 3 (1.4%) | | 2 statements | 28 (15.6%) |
| Ethnicity | Caucasian | 66 (31.4%) | | 3 statements | 15 (8.4%) |
| | Black | 3 (1.4%) | | 4 statements | 4 (2.2%) |
| | Asian | 108 (51.4%) | | 5 statements | 5 (2.8%) |
| | Hispanic | 2 (1.0%) | | 6 statements | 4 (2.2%) |
| | Other | 24 (11.4%) | 7 statements | 1 (0.6%) | |
| | Rather Not Say | 7 (3.4%) | > 10 statements | 13 (7.3%) | |
| School Year | First Year | 55 (26.2%) | Privacy Seal Experience | Yes | 91 (43.3%) |
| | Second Year | 51 (24.3%) | | No | 119 (56.7%) |
| | Third Year | 42 (20.0%) | Privacy Seal* (<i>N</i> = 104) | BBBOnLine | 15 (16.5%) |
| | Fourth Year | 36 (17.1%) | | TRUSTe | 47 (51.6%) |
| | Graduate Student | 26 (12.4%) | | WebTrust | 11 (12.1%) |
| | | BetterWeb | | 3 (3.3%) | |
| Online Transaction Experience in the Past Twelve Months | None | 17 (8.1%) | ESRB | 25 (27.5%) | |
| | 1 – 10 times | 108 (51.4%) | VeriSign | 73 (80.2%) | |
| | 11 – 20 times | 34 (16.2%) | Other | 5 (5.5%) | |
| | > 20 times | 51 (24.3%) | | | |

* Participants were asked to indicate all privacy seals that they seen before.

More than half of the participants (65.2%) were male. The mean age was approximately 21 years, and the age range was from 18 and 43 years. The majority of participants were from Asian (51.4%) and

Caucasian (31.4%) ethnic groups. About 88 percent of the respondents were undergraduate students. Of the participants, about 92 percent reported that they had online transaction experiences such as ordering things, subscribing to services or registering on Web sites for online services.²⁶ On average, they conducted online transactions 10 times in the past twelve months. A total of 179 participants (85.2%) had seen the privacy policy statement attached to some Web site. Of the respondents, roughly 36 percent did not read the privacy policy statement attached to any Web site in the past twelve months. In terms of privacy seals, only 91 (43.3%) participants had seen the privacy seal attached to any Web site. Among them, VeriSign (80.2%) had the highest percentage, followed by TRUSTe (51.6%), ESRB (27.5%), BBBOnLine (16.5%), WebTrust (12.1%), other seals such as VISA (5.5%), and BetterWeb (3.3%). This is an interesting finding because VeriSign and other seals are not privacy seals. This finding is consistent with Moores (2005). That is, although individuals had a basic understanding about privacy seals, quite a number of them failed to recognize genuine privacy seals. This result, therefore, justifies the use of a concocted seal in this study to reduce the effect of prior knowledge of a specific seal on the online ordering experiment.

In addition, several questions were developed to measure other characteristics of respondents using a seven-point scale ranging from 1 (low) and 7 (high). The trustworthiness of organizations was assessed by asking the degree to which respondents feel that each organization is trustworthy in terms of protecting their privacy (see Figure 8.a). The majority of participants felt that financial organizations ($M = 6.23$ and $SD = .97$), health service providers ($M = 5.45$ and $SD = 1.3$), and government organizations ($M = 5.34$ and $SD = 1.55$) are trustworthy. However, respondents tended to have low trust in e-commerce companies ($M = 3.56$ and $SD = 1.44$). The trustworthiness of privacy seal providers was also examined. The 91 respondents who had seen the privacy seal attached to any Web sites believe that privacy seal providers are less trustworthy ($M = 4.78$ and $SD = 1.36$) than financial organizations, health service

²⁶ The analysis was conducted without 17 participants who did not have online transaction experience in the past 12 months. The results were the same as with 17 participants. Hence, the followed analysis of the Internet privacy study was based on 210 participants.

providers, and government organizations, but more trustworthy than e-commerce companies. The results of paired comparisons using the Wilcoxon test revealed that respondents tend to trust financial organizations more than other organizations (Wilcoxon signed-rank test, all $p < .01$). There was no difference between health service providers and government organizations. In addition, respondents felt that e-commerce companies are less trustworthy than other organizations (Wilcoxon signed-rank test, $p < .01$).

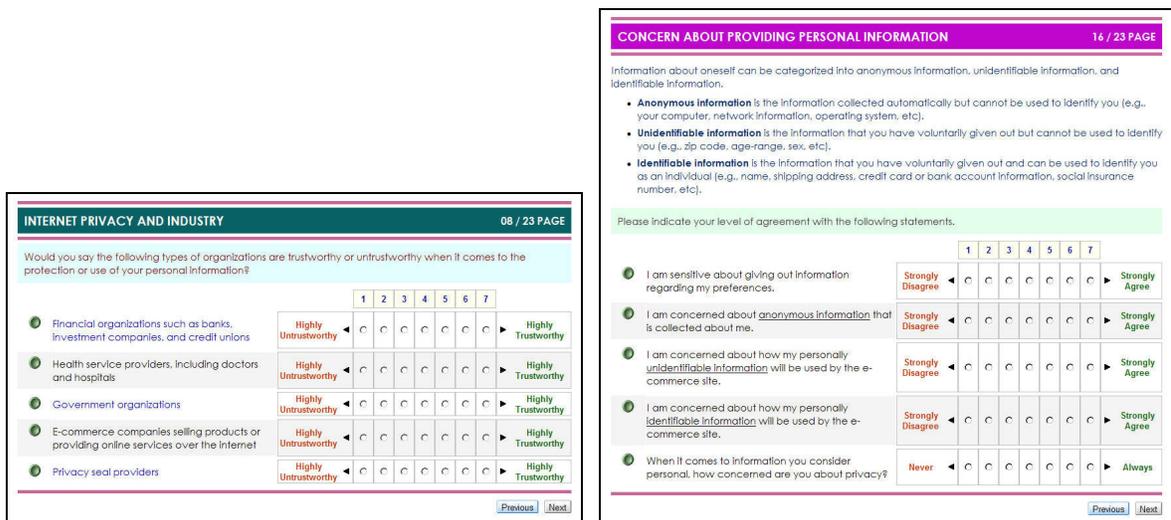


Figure 8: Trustworthiness of Organizations and Privacy Concern Measure

Respondents were also asked how concerned they were about their privacy (see Figure 8.b). A scale developed by Chellappa and Sin (2005) was employed for measuring the respondent's specific concern for privacy of his or her anonymous, personally unidentifiable, and personally identifiable information. The results from the questions measuring individuals' privacy concerns suggest that respondents had strong privacy concerns ($M = 5.88$ and $SD = 1.15$). Privacy concerns also varied in type of personal information. The majority of respondents were concerned about how their personally identifiable information is used by e-commerce sites ($M = 5.92$ and $SD = 1.29$). However, they were less concerned with information regarding their preferences ($M = 3.77$ and $SD = 1.72$), anonymous

information ($M = 3.76$ and $SD = 1.88$), and unidentifiable information ($M = 3.78$ and $SD = 1.7$). Differences in individuals' privacy concerns regarding the types of information were examined using the Wilcoxon signed-rank test. Significance tests show that respondents were more concerned with identifiable information than other types of information (Wilcoxon signed-rank test, all $p < .01$), but there were no significant differences in their concerns about preferences, anonymous information, and unidentifiable information.

7.1.3. Self-reported Privacy Behaviour

Table 8 shows the mean scores and standard deviations of the five self-reported measurement items. In addition, the ANOVA results of the five items are shown in Table 9 and Table 10.

Table 8: Means and Standard Deviations for Self-reported Privacy Behaviour

| | | <i>N</i> * | <i>ITEM 1</i> | | <i>ITEM 2</i> | | <i>ITEM 3</i> | | <i>ITEM 4</i> | | <i>ITEM 5</i> | |
|---------------------|-----------|------------|---------------|---------------|---------------|-----------|---------------|-----------|---------------|-----------|---------------|-----------|
| | | | <i>M</i> ** | <i>SD</i> *** | <i>M</i> | <i>SD</i> | <i>M</i> | <i>SD</i> | <i>M</i> | <i>SD</i> | <i>M</i> | <i>SD</i> |
| High Involvement | HI_SEAL | 35 | 4.51 | 2.32 | 3.77 | 2.30 | 3.06 | 1.94 | 1.97 | 1.52 | 1.91 | 1.63 |
| | HI_POLICY | 35 | 5.00 | 1.86 | 3.80 | 2.17 | 2.17 | 1.72 | 2.06 | 1.26 | 2.03 | 1.64 |
| | HI_NONE | 35 | | | | | 1.40 | 0.74 | 2.17 | 1.48 | 1.83 | 1.46 |
| Low Involvement | LI_SEAL | 35 | 2.57 | 1.61 | 2.20 | 1.51 | 5.71 | 1.71 | 4.31 | 1.66 | 3.91 | 1.82 |
| | LI_POLICY | 35 | 3.03 | 1.40 | 2.46 | 1.60 | 5.43 | 1.52 | 3.71 | 1.78 | 3.89 | 1.89 |
| | LI_NONE | 35 | | | | | 5.46 | 1.44 | 4.34 | 1.78 | 4.49 | 1.90 |
| Total | | 210 | 3.78 | 2.07 | 3.06 | 2.04 | 3.87 | 2.32 | 3.10 | 1.89 | 3.01 | 2.04 |

* Number of Web sites

** Mean of OECD principle score

*** Standard deviation of OECD principle score

ITEM 1: I would read the privacy policy statement of the Web site when it requests [*two pieces of personal information*].

ITEM 2: During the past 6 months, did you read the privacy policy statement of the Web site when it requested [*two pieces of personal information*]?

ITEM 3: How likely would you be to complete this form when [*two pieces of personal information*] are requested?

If the Web site had a privacy policy statement, how likely would you be to complete this form when [*two pieces of personal information*] are requested?

If the Web site had a privacy policy statement and a privacy seal how likely would you be to complete this form when [*two pieces of personal information*] are requested?

ITEM 4: I would provide my [*two pieces of personal information*] when the Web site’s privacy policy does NOT address [*two important company privacy practices*] as defined above.

ITEM 5: During the past 6 months, did you provide your [*two pieces of personal information*] when the Web site’s privacy policy does NOT address [*two important company privacy practices*] as defined above?

7.1.3.1. Reading Privacy Policy Statement

ITEM 1 and ITEM 2 measured the self-reported privacy behaviour with respect to reading the privacy policy statement (henceforth, self-reported reading behaviour).²⁷ The mean values for ITEM 1 indicate that respondents in the high involvement condition (hereafter, HI condition) were more willing to read the privacy policy statements than those in the low involvement condition (henceforth, LI condition).

Table 9: Analysis of Variance for Self-reported Privacy Behaviour

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|--------------------------|-----------|-----------|----------|----------|----------|
| ITEM 1 | | | | | |
| INVOLVEMENT | 1 | 134.064 | 39.959 | .001 | .227 |
| DISCLOSURE | 1 | 7.779 | 2.318 | .130 | .017 |
| INVOLVEMENT * DISCLOSURE | 1 | .007 | .002 | .963 | .001 |
| Error | 136 | 3.355 | | | |
| ITEM 2 | | | | | |
| INVOLVEMENT | 1 | 74.314 | 20.051 | .001 | .128 |
| DISCLOSURE | 1 | .714 | .193 | .661 | .001 |
| INVOLVEMENT * DISCLOSURE | 1 | .457 | .123 | .726 | .001 |
| Error | 136 | 3.706 | | | |

ITEM 1: I would read the privacy policy statement of the Web site when it requests [*two pieces of personal information*].

ITEM 2: During the past 6 months, did you read the privacy policy statement of the Web site when it requested [*two pieces of personal information*]?

²⁷ Only four groups (i.e., HI_SEAL, HI_POLICY, LI_SEAL, and LI_POLICY) were used for examining self-reported reading behaviour due to experimental condition (see Table 1).

The ANOVA results (Table 9) indicate significant differences in self-reported reading privacy behaviour between INVOLVEMENT groups ($F_{(1, 136)} = 39.959, p < .001, \eta^2 = .227$).²⁸ Eta (η) for INVOLVEMENT was about .48, which is a large effect.²⁹ However, both the main effect of DISCLOSURE on self-reported reading behaviour and the interaction effect between INVOLVEMENT and DISCLOSURE were not statistically significant.

A similar trend was observed in ITEM 2. The ANOVA results confirm this finding ($F_{(1, 136)} = 20.051, p < .001, \eta^2 = .128$). There was a significant difference in self-reported reading privacy behaviour between INVOLVEMENT groups. Thus, respondents in HI condition read the privacy policy statement of the Web site more often than those in LI condition during the past 6 months. Eta for INVOLVEMENT was about .36, which, according to Cohen (1988), can be considered as a large effect. However, both the main effect of DISCLOSURE and the interaction effect were not statistically significant. In addition, this study examined whether there is a difference between responses in ITEM 1 and ITEM 2. The results of a paired comparison using the Wilcoxon test revealed that respondents planned to read privacy policy statements more often than they did during the past 6 months (Wilcoxon signed-rank test, $p < .01$).

Based on the above observations, H1 is supported for self-reported reading behaviour. That is, individuals in the high privacy involved situation stated that they are more willing to read the privacy policy statement than those in the low privacy involved situation. In addition, the insignificant DISCLOSURE and interaction effects suggest that H3 is also supported. In other

²⁸ Levene's test result of the homogeneity of variances was significant ($p < .01$) which indicated the departure from the homogeneity assumption. Although the assumptions of ANOVA was violated, the study used ANOVA because it is robust to the violation of homogeneity variance if group are equal size (Maxwell and Delaney, 1990).

²⁹ Cohen (1988) provided guidelines for interpreting the size of the "effect" for common effect size measures such as γ , η , and ϕ . According to Cohen, $\eta > .10$ is a small effect, $\eta > .24$ is a medium effect, and $\eta > .37$ is a large effect in social science research.

words, the existence of a privacy seal had no effect on individuals' tendency to read the privacy policy statement posted on Web sites.

7.1.3.2. *Providing Personal Information*

Three measurement items (i.e., ITEM 3, ITEM 4, and ITEM 5) were used to assess respondents' self-reported privacy behaviour with respect to providing personal information (henceforth, self-reported providing behaviour). Among these three measurement items, one item was particularly related to the online ordering experiment. That question was used as a measure for the respondent's self-reported personal information providing behaviour given a scenario that is similar to his or her experimental condition (ITEM 3).

Table 10: Analysis of Variance for Self-reported Privacy Behaviour

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|--------------------------|-----------|-----------|----------|----------|----------|
| ITEM 3 | | | | | |
| INVOLVEMENT | 1 | 580.005 | 238.715 | .001 | .539 |
| DISCLOSURE | 2 | 16.300 | 6.709 | .002 | .062 |
| INVOLVEMENT * DISCLOSURE | 2 | 8.633 | 3.553 | .030 | .034 |
| Error | 204 | 2.430 | | | |
| ITEM 4 | | | | | |
| INVOLVEMENT | 1 | 222.171 | 87.767 | .001 | .301 |
| DISCLOSURE | 2 | 2.533 | 1.001 | .369 | .010 |
| INVOLVEMENT * DISCLOSURE | 2 | 2.229 | .880 | .416 | .009 |
| Error | 204 | 2.531 | | | |
| ITEM 5 | | | | | |
| INVOLVEMENT | 1 | 247.543 | 82.553 | .001 | .288 |
| DISCLOSURE | 2 | 1.176 | .392 | .676 | .004 |
| INVOLVEMENT * DISCLOSURE | 2 | 3.186 | 1.062 | .348 | .010 |
| Error | 204 | 2.999 | | | |

- ITEM 3: How likely would you be to complete this form when [*two pieces of personal information*] are requested?
 If the Web site had a privacy policy statement, how likely would you be to complete this form when [*two pieces of personal information*] are requested?
 If the Web site had a privacy policy statement and a privacy seal how likely would you be to complete this form when [*two pieces of personal information*] are requested?
- ITEM 4: I would provide my [*two pieces of personal information*] when the Web site's privacy policy does NOT address [*two important company privacy practices*] as defined above.
- ITEM 5: During the past 6 months, did you provide your [*two pieces of personal information*] when the Web site's privacy policy does NOT address [*two important company privacy practices*] as defined above?

The ANOVA results (Table 10) indicate that respondents in HI condition provided their personal information less than those in LI condition ($F_{(1, 204)} = 238.715, p < .001, \eta^2 = .539$). There were also a significant main effect of DISCLOSURE ($F_{(2, 204)} = 6.709, p = .002, \eta^2 = .062$) and an interaction effect between INVOLVEMENT and DISCLOSURE ($F_{(2, 204)} = 3.553, p = .03, \eta^2 = .034$). The effect size (eta) of three variables was .73 (INVOLVEMENT), .25 (DISCLOSURE), and .18 (interaction); according to Cohen (1988), they are a large effect, a medium effect, and a small effect.

When a significant interaction is obtained, it is generally preferable to consider effects within individual levels of other factors instead of interpreting the main effects themselves. Thus, the effect of DISCLOSURE at each level of INVOLVEMENT was examined. The one-way ANOVA results (not provided in tabular form) indicate that there was a significant effect of DISCLOSURE when respondents were in HI condition ($F_{(2, 102)} = 9.928, p < .001, \eta^2 = .163$), but the effect was not statistically significant when they were in LI condition. Post hoc multiple comparisons were used to determine whether there are significant differences across DISCLOSURE in HI condition. Follow-up Dunnett's T3 test results indicate a significant difference between *HI_NONE* and *HI_SEAL* groups ($p < .001$).³⁰ Also, there was a marginally significant difference between *HI_NONE* and *HI_POLICY* groups ($p = .055$). However, there was no difference between *HI_SEAL* and *HI_POLICY* groups.

³⁰ Dunnett's T3 is employed due to the violation of the homogeneity assumption (Maxwell and Delaney, 1990).

Based on the above results, H2 is supported for self-reported providing behaviour. That is, individuals in the high privacy involved situation stated that they are less willing to provide personal information than those in the low privacy involved situation. However, H4 is not supported.³¹

ITEM 4 and ITEM 5 were designed to assess if respondents provide their personal information when the Web site's privacy policy statement does not address two important privacy practices. The mean values for ITEM 4 indicate that respondents in HI condition were less likely to provide their personal information than those in LI condition ($F_{(1, 204)} = 87.767, p < .001, \eta^2 = .301$). Eta for INVOLVEMENT was about .55, which is a large effect according to Cohen (1988). However, DISCLOSURE had no significant effect, and also the interaction effect between INVOLVEMENT and DISCLOSURE was not significant. ITEM 5 shows a similar trend. The mean values of the high involvement group were less than those in the low involvement group ($F_{(1, 204)} = 82.553, p < .001, \eta^2 = .288$). Respondents in HI condition provided their personal information less than those in LI condition during the past 6 months. Eta was about .54, and thus the effect of INVOLVEMENT is large. The Wilcoxon signed-rank test conducted to investigate whether there is a difference between responses in ITEM 4 and ITEM 5 indicates no significant difference.

The results for ITEM 4 and ITEM 5 suggest that H2 is supported, but H5 is not supported. That is, individuals in the high privacy involved situation provided their personal information less than those in the low privacy involved situation when the Web site's privacy policy did not

³¹ Interestingly, the results indicate that the opposite of H4 was true. That is, individuals' behaviour with respect to providing personal information is influenced by a privacy seal when they are in the high privacy involved situation, but not in the low privacy involved situation. A plausible explanation for this finding could be found in Miyazaki and Krishnamurthy (2002); that is, a firm's participation in a seal program favourably influences customers' perceptions of a Web site's privacy policy and the level of information disclosure. Thus, when individuals were told that a Web site participates in a privacy seal program, it leads to individuals' positive perceptions of the Web site's privacy practices, and thus increases their willingness to provide personal information. This positive effect on the company's privacy practices can be only observed in the high privacy involved situation because individuals in the high privacy involved situation consider their information privacy. Individuals in the low privacy involved situation, however, consider their information privacy less, and thus their perceptions may not be substantially influenced by the existence of privacy seal. That is, it may not generate considerable positive effect on individuals' perceptions of the Web site's privacy practices while making an information disclosure decision.

address privacy policies important to them. However, the existence of a privacy seal did not influence individuals' willingness to provide their personal information.

7.1.4. Actual Privacy Behaviour

The actual privacy behaviour was captured while participants were performing an online ordering task. Five measurement items (i.e., ITEM 6 – ITEM 10) were used to assess respondents' actual privacy behaviour.

7.1.4.1. Reading Privacy Policy Statement

ITEM 6 measured the actual reading behaviour in terms of opening the privacy policy statement posted on the Web site.³² To investigate whether individuals' actual reading behaviour differs depending on involvement conditions and privacy policy disclosure conditions, a chi-square statistic was used. The Pearson chi-square results (Table 11) indicate that respondents in HI condition were more likely to open a privacy policy statement posted on the Web site than those in LI condition ($\chi^2 = 7.064$, $df = 1$, $N = 140$, $p = .008$). Phi, which indicates the strength of the association between the two variables, is .225 and, thus, the effect size is considered to be medium according to Cohen (1988).³³ On the other hand, respondents' actual reading behaviour was not significantly affected by a privacy seal.³⁴ Hence, similar to the self-reported reading behaviour, H1 and H3 are supported for actual reading behaviour.

³² Since only participants in HI_SEAL, HI_POLICY, LI_SEAL, and LI_POLICY were provided a privacy policy statement, only these groups were used for examining actual reading behaviour.

³³ According to the guidelines suggested by Cohen (1988), $\phi > .10$ is a small effect, $\phi > .30$ is a medium effect, and $\phi > .50$ is a large effect in social science research.

³⁴ This study also examined whether there are differences on respondents' actual reading behaviour across DISCLOSURE in each level of INVOLVEMENT, no differences were found.

Table 11: Chi-square Analysis of Actual Reading Behaviour

| | | High Involvement | | Low Involvement | | |
|--------|-------|------------------|------|-----------------|------|--------|
| | | N | SEAL | POLICY | SEAL | POLICY |
| ITEM 6 | | | | | | |
| | Yes | 49 | 14 | 18 | 7 | 10 |
| | No | 91 | 21 | 17 | 28 | 25 |
| | Total | 140 | 35 | 35 | 35 | 35 |

| | χ^2 | <i>p</i> | ϕ |
|-------------|----------|----------|--------|
| INVOLVEMENT | 7.064 | .008 | .215 |
| DISCLOSURE | 1.538 | .225 | .105 |

SEAL: Privacy Seal and Privacy Policy Statement

POLICY: Privacy Policy Statement

ITEM 6: Does the participant click the privacy policy statement of Gift4U?

Since it is possible that respondents did not read the privacy policy statement even if they opened it, the number of seconds that respondents spent on reading the privacy policy statement was also examined (ITEM 7). Table 12 shows mean scores, standard deviations, and ANOVA results. The mean values for ITEM 7 indicate that respondents in HI condition spent more time reading the privacy policy statement than those in LI condition ($F_{(1, 136)} = 8.874, p = .003, \eta^2 = .061$). Eta for INVOLVEMENT was about .25, which, according to Cohen (1988), can be considered roughly as a medium effect. However, both the main effect of DISCLOSURE and interaction effect were not statistically significant.

Table 12: Analysis of Variance for Time Spending to Read Privacy Policy Statement

| | <i>N</i> | SEAL | | POLICY | |
|------------------|----------|----------|-----------|----------|-----------|
| | | <i>M</i> | <i>SD</i> | <i>M</i> | <i>SD</i> |
| High Involvement | 70 | 32.71 | 65.19 | 35.89 | 60.03 |
| Low Involvement | 70 | 5.17 | 13.85 | 14.89 | 35.34 |
| Total | 140 | 18.94 | 48.80 | 25.39 | 50.03 |

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|--------------------------|-----------|-----------|----------|----------|----------|
| ITEM 7 | | | | | |
| INVOLVEMENT | 1 | 20618.579 | 8.874 | .003 | .061 |
| DISCLOSURE | 1 | 1452.864 | .625 | .430 | .005 |
| INVOLVEMENT * DISCLOSURE | 1 | 374.579 | .161 | .689 | .001 |
| Error | 136 | 2323.568 | | | |

SEAL: Privacy Seal and Privacy Policy Statement

POLICY: Privacy Policy Statement

ITEM 7: How long does the participant open the privacy policy statement of Gift4U?

7.1.4.2. *Providing Personal Information*

ITEM 8 measured the respondents' actual behaviour in terms of providing personal information to the Web site. Chi-square tests were conducted to examine whether individuals' actual behaviour differs on involvement conditions and privacy policy disclosure conditions.

Table 13: Chi-square Analysis of Actual Providing Behaviour

| | N | High Involvement | | | Low Involvement | | |
|-------------|-----|------------------|---------|----------|-----------------|---------|------|
| | | SEAL | PRIVACY | NONE | SEAL | PRIVACY | NONE |
| ITEM 8 | | | | | | | |
| Yes | 112 | 6 | 3 | 9 | 32 | 32 | 30 |
| No | 98 | 29 | 32 | 26 | 3 | 3 | 5 |
| Total | 210 | 35 | 35 | 35 | 35 | 35 | 35 |
| | | χ^2 | | <i>p</i> | | ϕ | |
| INVOLVEMENT | | 110.510 | | .001 | | .725 | |
| DISCLOSURE | | .497 | | .780 | | .049 | |

SEAL: Privacy Seal and Privacy Policy Statement

POLICY: Privacy Policy Statement

NONE: No Privacy Policy Disclosure

ITEM 8: Does the participant provide his or her true personal information?

Pearson chi-square result (Table 13) shows that respondents in LI condition provided their personal information more than those in HI condition ($\chi^2 = 110.51, df = 1, N = 210, p < .001$). Phi was about .725, which is a large effect according to Cohen (1988). However, respondents' behaviour was not significantly affected by whether the site had a privacy policy statement and whether it had a privacy seal.³⁵ The above observations suggest that H2 is supported, but H4 and H5 are not supported.

There are two possible explanations for the insignificant effect of privacy policy disclosure on respondents' information disclosure. One possible explanation is that respondents may not carefully read the privacy policy statement. Therefore, their decisions about providing personal information may not be influenced by the content of the privacy policy statement. To test this explanation, this study included the number of seconds that respondents spent reading the privacy policy statement (ITEM 7). Logistic regression was conducted to assess whether INVOLVEMENT, DISCLOSURE, and ITEM 7 significantly predict whether respondents revealed their information. When all three predictor variables are considered together, they significantly predict whether respondent provided their personal information ($\chi^2 = 99.859, df = 3, N = 140, p < .001$).³⁶ The results (Table 14) indicate that INVOLVEMENT was significant, but DISCLOSURE and ITEM 7 were not significant.

Table 14: Logistic Regression Predicting Actual Providing Behaviour

| Variable | β | <i>SE</i> | <i>p</i> |
|-------------|---------|-----------|----------|
| INVOLVEMENT | -4.340 | .583 | .001 |
| DISCLOSURE | .460 | .559 | .410 |
| ITEM 7 | .001 | .005 | .888 |
| Constant | 1.691 | .899 | .060 |

³⁵ The differences in respondents' actual providing behaviour across DISCLOSURE in each level of INVOLVEMENT were also examined, no differences were found.

³⁶ Only four groups (i.e., HI_SEAL, HI_POLICY, LI_SEAL, and LI_POLICY) were included for the logistic regression because participants in these groups were provided a privacy policy statement.

Another possible explanation is related to the TRUSTWEB seal used in the experiment. Since TRUSTWEB is a concocted seal, respondents might fail to recognize it as a privacy seal. For instance, they might think TRUSTWEB is a security seal, and thus they might not take the existence of the privacy seal into account when they make a decision about providing personal information. To test this explanation, this study assessed respondents' actual behaviour in terms of opening the privacy seal posted on the Web site (ITEM 9) as well as the time spent reading the information about the seal (ITEM 10). Table 15 shows the number of respondents who opened the privacy seal, the mean, and standard deviation of the number of seconds that they spent reading the information about the seal. Approximately 23% of respondents opened the privacy seal when they were asked to provide sensitive information, and they spent, on average, 13.5 seconds to get the information about the seal. On the contrary, only one respondent in the low involvement condition opened the privacy seal and spent 4 seconds to read the information about the seal. Respondents in the high privacy involved situation opened the privacy seal more ($\chi^2 = 6.248, df = 1, N = 70, p = .012$) and spent more time to get the information about the seal posed on the Web site compared to those in the low privacy involved situation ($F_{(1, 136)} = 6.261, p = .015$). This result suggests that the insignificant effect of the privacy seal was not due to the failure to recognize TRUSTWEB as a privacy seal.

Table 15: Descriptive Statistics of Respondents' Behaviour With Respect to Privacy Seal

| | <i>N</i> | ITEM 9 | | ITEM 10 | |
|------------------|----------|----------------|---------------|----------|-----------|
| | | <i>Yes (%)</i> | <i>No (%)</i> | <i>M</i> | <i>SD</i> |
| High Involvement | 35 | 8 (22.86%) | 27 (77.14%) | 13.50 | 8.77 |
| Low Involvement | 35 | 1 (2.86%) | 34 (97.14%) | 4.00 | - |
| Total | 70 | 9 (12.86%) | 61 (87.14%) | 12.44 | 8.79 |

ITEM 9: Does the participant click the TRUSTWEB page of Gift4U?

ITEM 10: How long does the participant open the TRUSTWEB page of Gift4U?

Based on the above observations, it appears that both the content of the privacy policy statement and the existence of a privacy seal did not affect individuals' actual behaviour in

providing personal information. Only individuals' degree of involvement influences their behaviour.

7.1.5. Self-reported versus Actual Privacy Behaviour

The gap between self-reported privacy behaviour and actual privacy behaviour was assessed by comparing two types of privacy behaviour: 1) *Reading Privacy Policy Statement* and 2) *Providing Personal Information*. Actual privacy behaviour was dichotomous in nature (i.e., *Read* versus *Do not read* and *Provide* versus *Do not provide*) whereas self-reported behaviour was measured on seven-point scales. For comparison, each item for self-reported privacy behaviour measure was transformed into a dichotomous variable based on a median split. Accordingly, two new variables (i.e., ITEM 1a and ITEM 2a) were created for self-reported reading behaviour. For self-reported providing behaviour, three new variables were generated (i.e., ITEM 3a, ITEM 4a, and ITEM 5a). These five new variables were then compared with each actual privacy behaviour measure.

McNemar's Chi-square test was employed to compare self-reported and actual measures.³⁷ With respect to reading the privacy policy statement, McNemar's Chi-square test for the comparison between the first self-reported measure and the actual measure (i.e., ITEM 1a vs. ITEM 6) was insignificant ($\chi^2 = .980, p = .322, N = 140$), as was the test for the comparison between the second self-reported measure and the actual measure (i.e., ITEM 2a vs. ITEM 6) ($\chi^2 = .595, p = .440, N = 140$).³⁸ However, McNemar's tests for the respondents' behaviour related to providing personal information (i.e., ITEM 3a vs. ITEM 8, ITEM 4a vs. ITEM 8, and ITEM 5a vs. ITEM 8) were significant ($\chi^2 = 5.891, p = .015, N = 210$; $\chi^2 = 41.440, p < .001, N = 210$; $\chi^2 = 36.012, p < .001, N = 210$, respectively). These results indicate that although respondents behaved akin to what they said with respect to reading the privacy policy

³⁷ Since the two variables are dichotomous in nature and are not normally distributed, McNemar's Chi-square test was conducted (Huck, 2004).

³⁸ Because of the privacy policy disclosure manipulation, 140 responses were used to test the difference between self-reported and actual behaviour.

statement, their behaviour was different from what they said in terms of providing personal information. Therefore, H6 is not supported, but H7 is supported.

7.2. Privacy Policy Disclosure Study

An analysis of variance (ANOVA) and correlation analysis were conducted to assess whether there is a difference in companies' privacy policies across six countries, whether companies' privacy policies in information-sensitive industries are different from those in less information-sensitive industries, and whether governmental involvement and cultural values influence companies' privacy policy disclosures.

7.2.1. General Profile

A total of 420 sites, 70 Web sites for each of six countries, were accessed and investigated. Table 16 shows the profile of 420 companies. On average, the number of employees is 68,005. The mean values of total assets and revenue are \$ 91,620,393,647 and \$ 17,404,109,030. Companies in less information-sensitive industries tend to have more employees and make more revenue. The total assets of information-sensitive industries are higher than those of less information-sensitive industries.

In terms of Web sites' profile, Table 17 presents the information regarding participation in privacy seal programs and adoption of technologies (P3P). Only 5% of 420 Web sites participate in privacy seal programs: BBBOnLine (2), TRUSTe (11), プライバシーマーク®制度 (5)³⁹, and Bobby Approved (1)⁴⁰. Among these sites, half of them are U.S. sites (10 sites). In China, none of

³⁹ 'プライバシーマーク®制度' is a Japanese privacy seal. It is issued by Japanese privacy seal authority (JIPDEC) and has the mutual accreditation with BBBOnLine (BBBOnLine, 2006).

⁴⁰ Bobby is provided by CAST (Centre for Applied Special Technology) and is a free Web-based service that analyzes Web pages. It analyses the accessibility of a Web site based on the World Wide Web Consortium's (W3C) Web Accessibility Initiative (WAI) and Section 508 guidelines from the Architectural and

sites participate in privacy seal programs. Furthermore, 13 sites are in less information-sensitive industries (e.g., manufacturing and retail industries), and 6 sites are in information-sensitive industries (e.g., financial and insurance industries). In terms of adoption of technologies (P3P), only 15 sites implement P3P: U.S. (8), Canada (2), U.K. (3), and Germany (2). Among these sites, 7 sites are in less information-sensitive industries, and 8 sites are in information-sensitive industries.

Transportation Barriers Compliance Board (Access Board) of the U.S. Federal Government. A Web site that successfully addressed all issues that Bobby identifies becomes “Bobby Approved” site and displays the Bobby Approved icon (www.cast.org). Although it is not a genuine third-party privacy seal, this study includes Bobby Approved because it not only provides a report about a Web site’s privacy but also works similar to third-party privacy seals.

Table 16: Company Profile

| | | U.S. | | CANADA | | U.K. | | GERMANY | | JAPAN | | CHINA | | Overall | |
|--------------------|-------------|-----------|-----------|---------|---------|---------|-----------|---------|---------|---------|-----------|---------|---------|-----------|-----------|
| | | LS* | S** | LS | S | LS | S | LS | S | LS | S | LS | S | LS | S |
| Incorporated Year | <i>Min</i> | 1888 | 1894 | 1870 | 1817 | 1886 | 1853 | 1756 | 1825 | 1899 | 1880 | 1960 | 1912 | 1756 | 1817 |
| | <i>Max</i> | 1999 | 1999 | 1999 | 1999 | 2001 | 2001 | 1998 | 1999 | 1987 | 2002 | 2000 | 1998 | 2001 | 2002 |
| Number of Employee | <i>Min</i> | 117,000 | 27,000 | 6,900 | 236 | 35,584 | 3,141 | 34,400 | 3,336 | 44,080 | 5,655 | 1,026 | 3,017 | 1,026 | 236 |
| | <i>Max</i> | 1,500,000 | 253,000 | 145,000 | 60,000 | 402,375 | 180,000 | 419,200 | 193,516 | 306,876 | 71,015 | 422,554 | 188,716 | 1,500,000 | 253,000 |
| | <i>M</i> | 243,941 | 60,436 | 34,894 | 9,752 | 80,773 | 31,301 | 117,029 | 23,777 | 104,187 | 16,590 | 19,523 | 48,775 | 102,835 | 29,048 |
| | <i>SD</i> | 234,605 | 46,875 | 33,636 | 16,321 | 74,067 | 40,254 | 105,947 | 43,245 | 70,647 | 15,222 | 79,150 | 73,491 | 138,838 | 40,398 |
| | <i>T***</i> | 152,188 | | 22,323 | | 56,037 | | 70,403 | | 60,388 | | 24,685 | | 68,055 | |
| Assets**** | <i>Min</i> | 2,780 | 503 | 411 | 4 | 2,754 | 409 | 3,378 | 268 | 19,866 | 669 | 21 | 29,817 | 21 | 4 |
| | <i>Max</i> | 647,483 | 1,264,030 | 31,957 | 351,726 | 266,995 | 1,034,220 | 59,220 | 401,201 | 85,452 | 1,294,850 | 6,476 | 464,132 | 647,483 | 1,294,850 |
| | <i>M</i> | 97,395 | 217,473 | 7,831 | 56,685 | 39,925 | 169,739 | 18,052 | 92,936 | 45,948 | 136,072 | 1,049 | 149,307 | 37,021 | 138,485 |
| | <i>SD</i> | 154,219 | 281,679 | 7,829 | 96,036 | 71,176 | 292,972 | 18,356 | 120,496 | 28,120 | 297,887 | 1,729 | 210,238 | 88,622 | 234,362 |
| | <i>T***</i> | 164,807 | | 32,778 | | 104,832 | | 64,135 | | 117,296 | | 28,005 | | 91,620 | |
| Revenue**** | <i>Min</i> | 5,003 | 961 | 610 | 24 | 2,671 | 56 | 1,035 | -210 | 11,428 | 732 | 9 | 1,024 | 9 | -210 |
| | <i>Max</i> | 185,524 | 94,713 | 22,342 | 20,655 | 232,571 | 79,252 | 48,502 | 57,122 | 70,466 | 47,850 | 2,825 | 15,020 | 232,571 | 94,713 |
| | <i>M</i> | 52,242 | 20,771 | 5,735 | 4,081 | 27,774 | 11,988 | 17,527 | 10,800 | 34,313 | 13,990 | 492 | 4,818 | 22,896 | 12,604 |
| | <i>SD</i> | 47,478 | 18,145 | 6,235 | 6,066 | 53,212 | 21,360 | 13,674 | 14,561 | 24,378 | 12,240 | 810 | 6,809 | 37,771 | 15,969 |
| | <i>T***</i> | 34,574 | | 4,890 | | 20,106 | | 13,456 | | 18,224 | | 1,278 | | 17,404 | |

* Less information-sensitive industries

** Information-sensitive industries

*** Total (Millions)

**** Millions

Table 17: Participation in Privacy Seal Programs and Adoption of Technologies (P3P)

| | | | U.S. (70 Sites) | CANADA (70 Sites) | U.K. (70 Sites) | GERMANY (70 Sites) | JAPAN (70 Sites) | CHINA (70 Sites) | Overall (420 Sites) |
|---|---|-----|--------------------|----------------------|--------------------|-----------------------|---------------------|---------------------|------------------------|
| Is a privacy seal posted on the domain? | Less Information-Sensitive Industry (35 Sites per country) | Yes | 8 (11%) | 1 (1%) | 1 (1%) | 0 (0%) | 3 (4%) | 0 (0%) | 13 (3%) |
| | | No | 27 (39%) | 34 (49%) | 34 (49%) | 33 (50%) | 32 (46%) | 35 (50%) | 197 (47%) |
| | Information-Sensitive Industry (35 Sites per country) | Yes | 2 (3%) | 0 (0%) | 0 (0%) | 2 (3%) | 2 (3%) | 0 (0%) | 6 (1%) |
| | | No | 33 (47%) | 35 (50%) | 35 (50%) | 33 (47%) | 33 (47%) | 35 (50%) | 204 (49%) |
| | Total | Yes | 10 (14%) | 1 (1%) | 1 (1%) | 3 (4%) | 5 (7%) | 0 (0%) | 19 (5%) |
| | | No | 60 (86%) | 69 (99%) | 69 (99%) | 67 (96%) | 65 (93%) | 70 (100%) | 401 (95%) |
| Does the domain implement P3P? | Less Information-Sensitive Industry (35 Sites per country) | Yes | 5 (7%) | 1 (1%) | 1 (1%) | 0 (0%) | 0 (0%) | 0 (0%) | 7 (2%) |
| | | No | 30 (43%) | 34 (49%) | 34 (49%) | 35 (50%) | 35 (50%) | 35 (50%) | 203 (48%) |
| | Information-Sensitive Industry (35 Sites per country) | Yes | 3 (4%) | 1 (1%) | 2 (3%) | 2 (3%) | 0 (0%) | 0 (0%) | 8 (2%) |
| | | No | 32 (46%) | 34 (49%) | 33 (47%) | 33 (47%) | 35 (50%) | 35 (50%) | 202 (48%) |
| | Total | Yes | 8 (11%) | 2 (3%) | 3 (4%) | 2 (3%) | 0 (0%) | 0 (0%) | 15 (4%) |
| | | No | 62 (89%) | 68 (97%) | 67 (96%) | 68 (97%) | 70 (100%) | 70 (100%) | 405 (96%) |

7.2.2. Differences in Privacy Policy Disclosures across Industries and Countries

In this study, companies' privacy practices were assessed by examining the content of companies' privacy policy statements with respect to eight OECD principles. Table 18 shows the mean scores and standard deviations of OECD principle scores among six countries. The mean values indicate that approximately 10 pieces of information from a maximum of 30 were stated in companies' privacy policy statements across six countries. The low mean values of OECD principle suggest that many Web sites among six countries were unsuccessful in covering all OECD principles in their privacy policy statements. Japan had the highest score (15.16), followed by Canada (13.24), U.S. (10.91), U.K. (8.81), Germany (6.83), and China (4.27). In terms of industry, Web sites in less information-sensitive industries disclosed more OECD principles than those in information-sensitive industries. Again Japan had the highest score in both industries, and China had the lowest score.

Table 18: OECD Principle Score between Non-sensitive and Sensitive Industry across Countries

| Industry | N | US. | | CANADA | | U.K. | | GERMANY | | JAPAN | | CHINA | | TOTAL | | |
|----------------|----|-------|------|--------|------|------|------|---------|------|-------|------|-------|------|-------|-------|------|
| | | M | SD | M | SD | M | SD | M | SD | M | SD | M | SD | n | M | SD |
| Less Sensitive | 35 | 11.69 | 5.52 | 13.26 | 8.26 | 9.46 | 4.74 | 7.34 | 4.29 | 15.57 | 2.48 | 3.49 | 3.74 | 210 | 10.13 | 6.46 |
| Sensitive | 35 | 10.14 | 4.70 | 13.23 | 7.66 | 8.17 | 4.20 | 6.31 | 3.98 | 14.74 | 2.87 | 5.06 | 3.83 | 210 | 9.61 | 5.88 |
| Total* | 70 | 10.91 | 5.15 | 13.24 | 7.91 | 8.81 | 4.49 | 6.83 | 4.14 | 15.16 | 2.70 | 4.27 | 3.84 | 420 | 9.87 | 6.18 |

* The maximum OECD principle score is 30.

The ANOVA (Table 19) indicates three important findings about OECD principle disclosure in companies' privacy policy statements. A significant difference in OECD principle

score across countries was found ($F_{(5, 408)} = 46.495, p < .001, \eta^2 = .363$).⁴¹ This indicates that OECD principle disclosure varies across countries, supporting H8. Eta (η) was about .60, which can be considered as a large effect size.⁴² Another main effect (i.e., INDUSTRY) was not significant, suggesting that OECD principle disclosure does not differ between less information-sensitive industry and information-sensitive industry. Also, the interaction effect was not statistically significant. These results are inconsistent with H9. That is, companies in information-sensitive industries did not incorporate more OECD principles in their privacy policy statements than those in less information-sensitive industries. In addition, this study conducted ANOVAs for each country to examine the differences in industry level. The ANOVA results indicate that OECD principle disclosure was not significantly different between the two industry classifications in all six countries.

Table 19: Analysis of Variance for OECD Principle as Function of Country and Industry

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|--------------------|-----------|-----------|----------|----------|----------|
| OECD Principle | | | | | |
| COUNTRY | 5 | 1149.811 | 46.495 | .001 | .363 |
| INDUSTRY | 1 | 28.810 | 1.165 | .281 | .003 |
| COUNTRY * INDUSTRY | 5 | 23.107 | 0.934 | .458 | .011 |
| Error | 408 | 24.730 | | | |

7.2.3. Analysis of Each OECD Principle

An analysis for each OECD principle was performed to examine whether companies in information-sensitive industries perceive each OECD principle differently than those in less

⁴¹ Levene's test result indicated the departure from the homogeneity of variances assumption. Since ANOVA is robust to the violation of homogeneity variance when group are equal size, this study conducted AVOVA (Maxwell and Delaney, 1990).

⁴² According to Cohen (1988), $\eta > .10$ is small effect size, $\eta > .24$ relates to medium size, and $\eta > .37$ is large effects in social science research.

information-sensitive industries. Prior to the analysis of data, the means and standard deviations of each principle score were examined. Table 20 shows the descriptive statistics of each principle score.

Table 20: Means and Standard Deviations for OECD Principles between Non-sensitive and Sensitive Industry across Countries

| OECD Principles | Max. Score* | Industry | N | US. | | CANADA | | U.K. | | GERMANY | | JAPAN | | CHINA | | TOTAL | | |
|-------------------------------|-------------|----------------|----|------|------|--------|------|------|------|---------|------|-------|------|-------|------|-------|------|------|
| | | | | M | SD | M | SD | M | SD | M | SD | M | SD | M | SD | N | M | SD |
| Accountability (AC) | 2 | Less Sensitive | 35 | 0.86 | 0.65 | 1.26 | 0.92 | 0.69 | 0.87 | 0.80 | 0.80 | 1.94 | 0.24 | 0.03 | 0.17 | 210 | 0.93 | 0.89 |
| | | Sensitive | 35 | 0.46 | 0.56 | 1.26 | 0.89 | 0.74 | 0.85 | 0.80 | 0.80 | 1.94 | 0.34 | 0.29 | 0.62 | 210 | 0.91 | 0.89 |
| | | Total | 70 | 0.66 | 0.63 | 1.26 | 0.90 | 0.71 | 0.85 | 0.80 | 0.79 | 1.94 | 0.29 | 0.16 | 0.47 | 420 | 0.92 | 0.89 |
| Collection Limitation (CL) | 4 | Less Sensitive | 35 | 0.63 | 0.97 | 1.94 | 1.45 | 1.11 | 0.80 | 0.49 | 0.61 | 1.43 | 1.01 | 0.51 | 0.56 | 210 | 1.02 | 1.08 |
| | | Sensitive | 35 | 0.46 | 0.78 | 1.89 | 1.16 | 0.71 | 0.67 | 0.69 | 0.63 | 1.03 | 0.95 | 0.54 | 0.51 | 210 | 0.89 | 0.94 |
| | | Total | 70 | 0.54 | 0.88 | 1.91 | 1.31 | 0.91 | 0.76 | 0.59 | 0.63 | 1.23 | 1.00 | 0.53 | 0.53 | 420 | 0.95 | 1.01 |
| Data Quality (DQ) | 3 | Less Sensitive | 35 | 0.83 | 0.62 | 0.60 | 0.78 | 0.14 | 0.36 | 0.11 | 0.32 | 0.29 | 0.46 | 0.17 | 0.38 | 210 | 0.36 | 0.57 |
| | | Sensitive | 35 | 0.63 | 0.60 | 0.97 | 1.07 | 0.06 | 0.24 | 0.26 | 0.51 | 0.09 | 0.28 | 0.46 | 0.51 | 210 | 0.41 | 0.67 |
| | | Total | 70 | 0.73 | 0.61 | 0.79 | 0.95 | 0.10 | 0.30 | 0.19 | 0.43 | 0.19 | 0.39 | 0.31 | 0.47 | 420 | 0.38 | 0.62 |
| Individual Participation (IP) | 6 | Less Sensitive | 35 | 2.29 | 1.56 | 2.69 | 1.92 | 2.14 | 1.56 | 1.31 | 1.28 | 4.20 | 0.72 | 0.57 | 1.09 | 210 | 2.20 | 1.80 |
| | | Sensitive | 35 | 1.77 | 1.80 | 2.57 | 1.84 | 1.80 | 1.57 | 1.03 | 1.18 | 3.83 | 1.38 | 1.23 | 1.37 | 210 | 2.04 | 1.79 |
| | | Total | 70 | 2.03 | 1.69 | 2.63 | 1.87 | 1.97 | 1.56 | 1.17 | 1.23 | 4.01 | 1.11 | 0.90 | 1.28 | 420 | 2.12 | 1.79 |
| Openness (OP) | 2 | Less Sensitive | 35 | 1.14 | 0.81 | 1.17 | 0.86 | 0.83 | 0.75 | 0.69 | 0.58 | 1.91 | 0.28 | 0.06 | 0.24 | 210 | 0.97 | 0.84 |
| | | Sensitive | 35 | 0.69 | 0.68 | 1.11 | 0.68 | 0.63 | 0.69 | 0.57 | 0.50 | 1.91 | 0.28 | 0.14 | 0.43 | 210 | 0.84 | 0.79 |
| | | Total | 70 | 0.91 | 0.78 | 1.14 | 0.77 | 0.73 | 0.72 | 0.63 | 0.54 | 1.91 | 0.28 | 0.10 | 0.35 | 420 | 0.90 | 0.82 |
| Purpose Specification (PS) | 5 | Less Sensitive | 35 | 3.46 | 0.95 | 2.60 | 1.77 | 2.74 | 1.15 | 2.06 | 1.39 | 2.34 | 1.03 | 1.46 | 1.42 | 210 | 2.44 | 1.44 |
| | | Sensitive | 35 | 2.69 | 1.30 | 2.29 | 1.74 | 2.37 | 1.33 | 1.20 | 1.05 | 2.51 | 1.15 | 1.57 | 1.07 | 210 | 2.10 | 1.39 |
| | | Total | 70 | 3.07 | 1.20 | 2.44 | 1.75 | 2.56 | 1.25 | 1.63 | 1.30 | 2.43 | 1.08 | 1.51 | 1.25 | 420 | 2.27 | 1.42 |
| Security Safeguards (SS) | 5 | Less Sensitive | 35 | 2.17 | 2.01 | 2.00 | 1.75 | 1.49 | 1.46 | 1.66 | 1.45 | 2.06 | 1.06 | 0.60 | 1.04 | 210 | 1.66 | 1.58 |
| | | Sensitive | 35 | 3.03 | 1.56 | 2.29 | 1.64 | 1.63 | 1.40 | 1.34 | 1.35 | 2.34 | 0.64 | 0.77 | 1.14 | 210 | 1.90 | 1.51 |
| | | Total | 70 | 2.60 | 1.84 | 2.14 | 1.69 | 1.56 | 1.42 | 1.50 | 1.40 | 2.20 | 0.88 | 0.69 | 1.08 | 420 | 1.78 | 1.55 |
| Use Limitation (UL) | 3 | Less Sensitive | 35 | 0.31 | 0.58 | 1.00 | 0.91 | 0.31 | 0.58 | 0.23 | 0.43 | 1.40 | 0.60 | 0.09 | 0.28 | 210 | 0.56 | 0.76 |
| | | Sensitive | 35 | 0.43 | 0.61 | 0.86 | 0.81 | 0.23 | 0.49 | 0.43 | 0.50 | 1.09 | 0.45 | 0.06 | 0.24 | 210 | 0.51 | 0.64 |
| | | Total | 70 | 0.37 | 0.59 | 0.93 | 0.86 | 0.27 | 0.54 | 0.33 | 0.47 | 1.24 | 0.55 | 0.07 | 0.26 | 420 | 0.54 | 0.70 |

* Maximum score of each OECD principle

Japan (1.94) had the highest mean in the AC principle, followed by Canada (1.26), Germany (0.8), U.K. (0.71), U.S. (0.66), and China (0.16). With respect to the CL principle, Canada (1.91) had the highest mean, and China (0.53) had the lowest mean. Table 20 also shows that all countries were unsuccessful to providing enough information regarding the DQ principle in companies' privacy statements among six countries (all $M < .8$). In addition, the mean scores in the IP principle indicated that Web sites in six countries, on average, provide more than two pieces of information about the IP principle in their privacy statements. In terms of the OP principle, Japan (1.91) had the highest mean, followed by Canada (1.14), U.S. (0.91), U.K. (0.73), Germany (0.63), and China (0.1). On average, except Germany and China, all countries provided more than two pieces of information about the PS principle, and all countries except China addressed more than one piece of information about the SS principle in companies' privacy policy statements. Finally, most countries except Japan (1.24) and Canada (0.93) did not provide enough information regarding the UL principle.

To investigate the differences in country and industry levels, ANOVAs for each OECD principle were conducted. The ANOVA results are shown in Table 21. The results indicate that all OECD principles were significantly different across countries (all $p < .001$). Each eta (η) of eight OECD principles was greater than .39, which is a large effect according to Cohen (1988). However, not all OECD principles were significantly different between less information-sensitive industry and information-sensitive industry. Only the OP and PS principles were significantly different between two industries ($p = .035$ and $p = .008$, respectively). The SS principle was marginally significant ($p = .086$). In terms of interaction, the DQ principle was statistically significant ($p = .004$), and the PS principle was marginally significant ($p = .093$). Based on the ANOVA results and mean scores in Table 21, H9 is not supported. Contrary to the expectation, companies in less information-sensitive industries incorporate more OP and PS principles in their privacy policy statements than do companies in information-sensitive industries.

Table 21: Analysis of Variance for Eight OECD Principles as Function of Country and Industry

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|--------------------------|-----------|-----------|----------|----------|----------|
| Accountability (AC) | | | | | |
| COUNTRY | 5 | 26.147 | 55.087 | .001 | .403 |
| INDUSTRY | 1 | .021 | .045 | .832 | .001 |
| COUNTRY * INDUSTRY | 5 | .799 | 1.682 | .138 | .020 |
| Error | 408 | .475 | | | |
| Data Quality (DQ) | | | | | |
| COUNTRY | 5 | 6.220 | 20.067 | .001 | .197 |
| INDUSTRY | 1 | .288 | .930 | .336 | .002 |
| COUNTRY * INDUSTRY | 5 | 1.088 | 3.511 | .004 | .041 |
| Error | 408 | .310 | | | |
| Openness (OP) | | | | | |
| COUNTRY | 5 | 25.632 | 71.019 | .001 | .465 |
| INDUSTRY | 1 | 1.610 | 4.459 | .035 | .011 |
| COUNTRY * INDUSTRY | 5 | .632 | 1.752 | .122 | .021 |
| Error | 408 | .361 | | | |
| Security Safeguards (SS) | | | | | |
| COUNTRY | 5 | 32.284 | 16.061 | .001 | .164 |
| INDUSTRY | 1 | 5.952 | 2.961 | .086 | .007 |
| COUNTRY * INDUSTRY | 5 | 2.472 | 1.230 | .294 | .015 |
| Error | 408 | 2.010 | | | |

| Source | <i>df</i> | <i>MS</i> | <i>F</i> | <i>p</i> | η^2 |
|-------------------------------|-----------|-----------|----------|----------|----------|
| Collection Limitation (CL) | | | | | |
| COUNTRY | 5 | 20.787 | 26.651 | .001 | .246 |
| INDUSTRY | 1 | 1.867 | 2.393 | .123 | .006 |
| COUNTRY * INDUSTRY | 5 | 1.004 | 1.287 | .269 | .016 |
| Error | 408 | .780 | | | |
| Individual Participation (IP) | | | | | |
| COUNTRY | 5 | 87.718 | 40.251 | .001 | .330 |
| INDUSTRY | 1 | 2.752 | 1.263 | .262 | .003 |
| COUNTRY * INDUSTRY | 5 | 3.112 | 1.428 | .213 | .017 |
| Error | 408 | 2.179 | | | |
| Purpose Specification (PS) | | | | | |
| COUNTRY | 5 | 24.671 | 14.504 | .001 | .151 |
| INDUSTRY | 1 | 12.002 | 7.056 | .008 | .017 |
| COUNTRY * INDUSTRY | 5 | 3.231 | 1.899 | .093 | .023 |
| Error | 408 | 1.701 | | | |
| Use Limitation (UL) | | | | | |
| COUNTRY | 5 | 14.136 | 43.485 | .001 | .348 |
| INDUSTRY | 1 | .193 | .593 | .442 | .001 |
| COUNTRY * INDUSTRY | 5 | .593 | 1.824 | .107 | .022 |
| Error | 408 | .325 | | | |

A plausible explanation for these findings is that companies in information-sensitive industries have their own standards or regulations, especially with respect to the security issues of personal information. Hence, such standards and regulations may not be addressed in their privacy policy statements. It is also possible that companies in less information-sensitive industries incorporate more OECD principles in their privacy policy statements to build customers' trust on their Web sites. Compared to companies in information-sensitive industries (e.g., online banking site), companies in less information-sensitive industries (e.g., online shopping site) often need more personal information for customizing their products and services. In the meantime, customers are less likely to provide their personal information to companies in less information-sensitive industries when compared to information-sensitive industries (Earp and Baumer, 2003). Therefore, companies in less information-sensitive industries may try to gain consumer trust by posting high-quality privacy policy statements, and thus they can boost customers' willingness to provide personal information.

7.2.4. Government Involvement and Privacy Policy Disclosures

H10 suggests that there will be a difference in the degrees of privacy practices associated with different governmental involvement structures. Specifically, companies' privacy policy disclosures will be positively associated with governmental involvement structures. An ANOVA was performed to assess the significance of difference in companies' privacy policy disclosures with respect to governmental involvement. Table 22 shows that the means and standard deviations of OECD principle scores comparing governmental involvement as well as ANOVA results. As hypothesized, the degree of companies' privacy policy disclosures varied significantly among various levels of governmental involvement ($F_{(2, 416)} = 33.167, p < .001$). Governmental involvement had significant, positive relationship with OECD principle score (r

= .316, $p < .001$), suggesting that companies in high governmental involvement countries have higher levels of privacy policy disclosures than those in low governmental involvement countries. Therefore, H10 is supported.

Table 22: Analysis of Variance for OECD Principle Score as Function of Governmental Involvement

| Governmental Involvement | N | M | SD |
|--|-----|-------|------|
| No Formal Information Privacy Regulation | 70 | 4.27 | 3.84 |
| Voluntary Control | 70 | 10.91 | 5.15 |
| Data Commissioner | 210 | 11.74 | 6.44 |
| Registration | 70 | 8.81 | 4.49 |
| Total | 420 | 9.87 | 6.18 |

| Source | <i>df</i> | <i>SS</i> | <i>MS</i> | <i>F</i> | <i>p</i> |
|----------------|-----------|-----------|-----------|----------|----------|
| OECD Principle | | | | | |
| Between Groups | 3 | 3085.029 | 1028.34 | 33.167 | 0.00 |
| Within Groups | 416 | 12898.03 | 31.01 | | |
| Total | 419 | 15983.06 | | | |

Follow-up Dunnett's T3 results indicate that no formal information privacy regulation was significantly different from other governmental involvement structures (all, $p < .001$).⁴³ There is also a significant difference on OECD principle score on data commissioner and registration ($p < .001$). The mean score of data commissioner (11.74) was higher than that of registration (8.81). These are interesting findings because it is the opposite of H10. That is, the significant difference between data commissioner and registration indicates that companies in registration countries (i.e., higher governmental involvement) incorporate fewer OECD principles in their privacy policy statements than those in data commissioner (i.e., lower governmental involvement). A plausible explanation is that companies in registration countries

⁴³ Dunnett's T3 was used due to the departure from the homogeneity assumption (Maxwell and Delaney, 1990).

have more strict regulations (e.g., data security and integrity requirements in financial industry), and hence, they may not need to address such requirements in their privacy policy statements.

7.2.5. Cultural Values and Privacy Policy Disclosures

H11 through H15 suggest that cultural values influence companies' privacy disclosures. To test these hypotheses, correlation analyses were performed to assess the significance of each cultural dimension (i.e., power distance, uncertainty avoidance, individualism, masculinity, and long-term orientation) on companies' privacy policy disclosures (i.e., OECD principle score). The means, standard deviations, and intercorrelations are shown in Table 23.

Table 23: Means, Standard Deviations, and Intercorrelation for OECD Principle Score

| | <i>M</i> | <i>SD</i> | Power Distance (PDI) | Uncertainty Avoidance (UAI) | Individualism (IDV) | Masculinity (MAS) | Long-Term Orientation (LTO) |
|----------------------|----------|-----------|----------------------|-----------------------------|---------------------|-------------------|-----------------------------|
| OECD Principle Score | 9.87 | 6.18 | -.224 | .381 | .211 | .210 | -.190 |
| <i>p</i> | | | .001 | .001 | .001 | .001 | .001 |

The Pearson correlation shows a statistically significant association between power distance and OECD principle score ($r = -.224, p < .001$). If OECD principle score was correlated positively and significantly with the power distance, it indicates that there is a positive relationship between PDI and the degree of OECD principle a company discloses in its privacy policy statement. The direction of the correlation was negative, which means that countries with high power distance tend to have lower level of privacy policy disclosure and vice versa. Therefore, H11 is supported. A strong relationship was also observed between UAI and OECD principle score ($r = .381, p < .001$). The positive correlation coefficient suggests that countries with high uncertainty avoidance tend to have a higher level of privacy policy disclosure, supporting H12. As hypothesized (H13), IDV was positively associated with OECD principle score ($r = .211, p < .001$), suggesting

companies in individualist cultures have higher levels of privacy policy disclosures than those in collectivist cultures.

MAS also had a significant, positive relationship with OECD principle score ($r = .21, p < .001$). Interestingly, this finding is the exact opposite of H14, suggesting countries with feminine cultures tend to have lower levels of privacy policy disclosure. One possible explanation is that e-commerce sites are more likely designed for males because males tend to perform online transactions (e.g., participate in auctions and trade stocks) more than females. Hence, to build customers' trust on their Web sites, companies in masculine societies may tend to address more OECD principles in their privacy policy statements than those in feminine cultures. Finally, in support of H15, LTO was negatively associated with OECD principle score ($r = -.19, p < .001$). That is, countries with short-term oriented cultures (i.e., societies' values are oriented towards the past and present) have higher levels of privacy policy disclosures than those in long-term oriented cultures (i.e., societies' values are oriented towards the future).

7.3. Privacy Gap Study

A gap between individual's perceived importance of companies' privacy policies and what companies emphasize in the privacy policy statements is examined in this section. Friedman tests were conducted to assess the individuals' perceived importance of OECD principles and the frequently addressed OECD principles in companies' privacy policy statements. Then, a gap in the perceived importance of OECD principles between individuals and companies was analyzed using Spearman's rho.

7.3.1. Important Companies' Privacy Policies that Individuals Want to Know

Two questions were designed to capture the important companies' privacy policies that respondents want to know (see Appendix II – Internet privacy user survey page 10 and 11). Table 24 shows the summary of respondents' perceived importance of each OECD principle. The results indicate that regardless of the type of Web site and the type of information requested, respondents perceived the SS and UL principles as the two most important companies' privacy practices that they want to know. On the other hand, the DQ and IP principles were the two least important companies' privacy policies.

Table 24: Individual's Perceived Importance of OECD Principles

| OECD Principle | Online Banking Site (Sensitive Industry) | | | | | | | | | | | | Online Shopping Site (Non-sensitive Industry) | | | | | | | | | | | |
|-------------------------------|--|-----------------|-------------------------|-----------------------------------|------|----------|-----------------------------------|------|----------|-----------------------------------|------|----------|---|------|----------|-----------------------------------|------|----------|-----------------------------------|------|----------|-----------------------------------|------|----------|
| | Most Important Privacy Practices | | | | | | Least Important Privacy Practices | | | | | | Most Important Privacy Practices | | | | | | Least Important Privacy Practices | | | | | |
| | Sensitive Information (IND1) | | | Less sensitive Information (IND2) | | | Sensitive Information (IND3) | | | Less sensitive Information (IND4) | | | Sensitive Information (IND5) | | | Less sensitive Information (IND6) | | | Sensitive Information (IND7) | | | Less sensitive Information (IND8) | | |
| | <i>N</i> [*] | % ^{**} | <i>R</i> ^{***} | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> | <i>N</i> | % | <i>R</i> |
| Accountability (AC) | 23 | 11.0 | 4 | 25 | 11.9 | 4 | 28 | 13.3 | 4 | 26 | 12.4 | 3 | 27 | 12.9 | 4 | 30 | 14.3 | 4 | 18 | 8.6 | 4 | 22 | 10.5 | 3 |
| Collection Limitation (CL) | 10 | 4.8 | 5 | 13 | 6.2 | 5 | 20 | 9.5 | 6 | 26 | 12.4 | 3 | 10 | 4.8 | 5 | 18 | 8.6 | 5 | 18 | 8.6 | 4 | 16 | 7.6 | 5 |
| Data Quality (DQ) | 7 | 3.3 | 7 | 8 | 3.8 | 6 | 46 | 21.9 | 1 | 55 | 26.2 | 1 | 1 | 0.5 | 8 | 2 | 1.0 | 7 | 65 | 31.0 | 1 | 66 | 31.4 | 1 |
| Individual Participation (IP) | 5 | 2.4 | 8 | 7 | 3.3 | 7 | 37 | 17.6 | 2 | 39 | 18.6 | 2 | 3 | 1.4 | 7 | 0 | 0.0 | 8 | 53 | 25.2 | 2 | 56 | 26.7 | 2 |
| Openness (OP) | 9 | 4.3 | 6 | 7 | 3.3 | 7 | 34 | 16.2 | 3 | 24 | 11.4 | 5 | 8 | 3.8 | 6 | 11 | 5.2 | 6 | 27 | 12.9 | 3 | 22 | 10.5 | 3 |
| Purpose Specification (PS) | 32 | 15.2 | 3 | 32 | 15.2 | 3 | 25 | 11.9 | 5 | 21 | 10.0 | 6 | 41 | 19.5 | 3 | 33 | 15.7 | 3 | 18 | 8.6 | 4 | 16 | 7.6 | 5 |
| Security Safeguards (SS) | 83 | 39.5 | 1 | 81 | 38.6 | 1 | 5 | 2.4 | 8 | 2 | 1.0 | 8 | 78 | 37.1 | 1 | 78 | 37.1 | 1 | 3 | 1.4 | 8 | 0 | 0.0 | 8 |
| Use Limitation (UL) | 41 | 19.5 | 2 | 37 | 17.6 | 2 | 15 | 7.1 | 7 | 17 | 8.1 | 7 | 42 | 20.0 | 2 | 38 | 18.1 | 2 | 8 | 3.8 | 7 | 12 | 5.7 | 7 |

* Number of respondents who indicated the OECD principle as important
 ** Percentage of respondents who indicated the OECD principle as important
 *** Rank order of the OECD principle

Friedman tests were conducted to assess if there were differences in participants' importance ratings of OECD principles regarding the type of information requested. The results of Friedman tests between IND1 and IND2, between IND3 and IND4, between IND5 and IND6, and between IND7 and IND8 were found to be insignificant ($\chi^2_{(7,N=2)} = 13.707, p = .057$; $\chi^2_{(7,N=2)} = 13.036, p = .071$; $\chi^2_{(7,N=2)} = 13.833, p = .054$; and $\chi^2_{(7,N=2)} = 13.741, p = .056$, respectively). These reveal that the participants' perceived importance of FIP principles did not differ depending on the type of information requested.

This study also examined whether there were differences in the participants' importance ratings of OECD principles depending on the type of industry. The Friedman tests between IND1 and IND5, between IND2 and IND6, between IND3 and IND7, and between IND4 and IND8 were all statistically insignificant, which indicate no difference on the respondents' perceived importance of OECD principles depending on the type of industry the Web site belongs to ($\chi^2_{(7,N=2)} = 13.833, p = .054$; $\chi^2_{(7,N=2)} = 13.707, p = .057$; $\chi^2_{(7,N=2)} = 13.829, p = .054$; and $\chi^2_{(7,N=2)} = 13.448, p = .062$, respectively). Therefore, H16 and H17 are not supported. That is, individuals did not perceive OECD principles differently depending on the type of information requested and the type of industry a Web site belongs to.

7.3.2. Frequently Addressed OECD Principles in Companies' Privacy Policy Disclosures

To examine which OECD principle is frequently disclosed in companies' privacy policy statements, the rank order of each OECD principle was identified based on the proportion score of each OECD principle. The results are shown in Table 25.

Table 25: Proportion Score of OECD Principles

| OECD Principles | U.S. | | | CANADA | | | U.K. | | | GERMANY | | | JAPAN | | | CHINA | | | Overall (By Principle) | | |
|-------------------------------|-----------|-------------|-------------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|---------------------------|-----------|----------|
| | <i>S*</i> | <i>NS**</i> | <i>T***</i> | <i>S</i> | <i>NS</i> | <i>T</i> | <i>S</i> | <i>NS</i> | <i>T</i> |
| Accountability (AC) | .23 | .43 | .33 | .63 | .63 | .63 | .37 | .34 | .36 | .40 | .40 | .40 | .97 | .97 | .97 | .14 | .01 | .08 | .46 | .46 | .46 |
| Collection Limitation (CL) | .11 | .16 | .14 | .47 | .49 | .48 | .18 | .28 | .23 | .17 | .12 | .15 | .26 | .36 | .31 | .14 | .13 | .13 | .22 | .25 | .24 |
| Data Quality (DQ) | .21 | .28 | .24 | .32 | .20 | .26 | .02 | .05 | .03 | .09 | .04 | .06 | .03 | .10 | .06 | .15 | .06 | .10 | .14 | .12 | .13 |
| Individual Participation (IP) | .30 | .38 | .34 | .43 | .45 | .44 | .30 | .36 | .33 | .17 | .22 | .20 | .64 | .70 | .67 | .20 | .10 | .15 | .34 | .37 | .35 |
| Openness (OP) | .34 | .57 | .46 | .56 | .59 | .57 | .31 | .41 | .37 | .29 | .34 | .32 | .96 | .96 | .96 | .07 | .03 | .05 | .42 | .48 | .45 |
| Purpose Specification (PS) | .54 | .69 | .61 | .46 | .52 | .49 | .47 | .55 | .51 | .24 | .41 | .33 | .50 | .47 | .49 | .31 | .29 | .30 | .42 | .49 | .45 |
| Security Safeguards (SS) | .61 | .43 | .52 | .46 | .40 | .43 | .33 | .30 | .31 | .27 | .33 | .30 | .47 | .41 | .44 | .15 | .12 | .14 | .38 | .33 | .36 |
| Use Limitation (UL) | .14 | .10 | .12 | .29 | .33 | .31 | .08 | .10 | .09 | .14 | .08 | .11 | .36 | .47 | .41 | .02 | .03 | .02 | .17 | .19 | .18 |

| Rank Order**** | U.S. | U.S. | U.S. | CANADA | CANADA | CANADA | U.K. | U.K. | U.K. | GERMANY | GERMANY | GERMANY | JAPAN | JAPAN | JAPAN | CHINA | CHINA | CHINA | Overall | Overall | Overall |
|-------------------------------|-----------|-------------|-------------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|----------|-----------|----------|
| | <i>S*</i> | <i>NS**</i> | <i>T***</i> | <i>S</i> | <i>NS</i> | <i>T</i> |
| Accountability (AC) | 5 | 3 | 5 | 1 | 1 | 1 | 2 | 4 | 3 | 1 | 2 | 1 | 1 | 1 | 1 | 5 | 8 | 6 | 1 | 3 | 1 |
| Collection Limitation (CL) | 8 | 7 | 7 | 3 | 4 | 4 | 6 | 6 | 6 | 5 | 6 | 6 | 7 | 7 | 7 | 5 | 2 | 4 | 6 | 6 | 6 |
| Data Quality (DQ) | 6 | 6 | 6 | 6 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 8 | 3 | 5 | 5 | 8 | 8 | 8 |
| Individual Participation (IP) | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 5 | 3 | 3 | 3 | 2 | 4 | 2 | 5 | 4 | 5 |
| Openness (OP) | 3 | 2 | 3 | 2 | 2 | 2 | 4 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 2 | 7 | 6 | 7 | 2 | 2 | 2 |
| Purpose Specification (PS) | 2 | 1 | 1 | 4 | 3 | 3 | 1 | 1 | 1 | 4 | 1 | 2 | 4 | 4 | 4 | 1 | 1 | 1 | 2 | 1 | 2 |
| Security Safeguards (SS) | 1 | 3 | 2 | 4 | 6 | 6 | 3 | 5 | 5 | 3 | 4 | 4 | 5 | 6 | 5 | 3 | 3 | 3 | 4 | 5 | 4 |
| Use Limitation (UL) | 7 | 8 | 8 | 8 | 7 | 7 | 7 | 7 | 7 | 6 | 7 | 7 | 6 | 4 | 6 | 8 | 6 | 8 | 7 | 7 | 7 |

* Proportion score of the OECD principle in information-sensitive industries
 ** Proportion score of the OECD principle in less information-sensitive industries
 *** Total proportion score of the OECD principle
 **** Rank order of the proportion score

The results reveal that the most frequently addressed OECD principle in the U.S., U.K., and China was the PS principle. The AC principle was the most frequently addressed OECD principle in Canada, Germany, and Japan. On the other hand, the least frequently addressed OECD principle in Canada, U.K., Germany, and Japan was the DQ principle. The UL was the least frequently addressed principle in U.S. and China. A Friedman test was conducted to examine if there was a difference among the mean ranks of the OECD principles across countries. The result of the Friedman test reveals a difference across countries ($\chi^2_{(7,N=6)} = 27.068, p < .001$). That is, companies perceived each OECD principle as having different importance among six countries.⁴⁴

The overall rank order of proportion score in the last three columns of Table 25 reveals a potential difference between two industries. Across six countries, AC was the most frequently addressed OECD principle, followed by OP, PS, SS, IP, CL, UL, and DQ. On the other hand, in less information-sensitive industries, a slightly different order was observed. However, the result of Friedman test indicates that there was no difference in frequently addressed OECD principles between two industries ($\chi^2_{(7,N=2)} = 13.287, p = .065$).⁴⁵ This indicates that in six countries, the companies' perceived importance of OECD principles was not different between two industries. Hence, H18 is not supported.

7.3.3. Gap in Perceived Importance of OECD Principles

⁴⁴ The differences among counties with respect to each industry were also examined. Friedman tests showed the same results indicating that the companies' perceived importance of OECD principles was different across six countries in both information-sensitive industries and less information-sensitive industries ($\chi^2_{(7,N=6)} = 23.66, p = .001$ and $\chi^2_{(7,N=6)} = 23.501, p = .001$, respectively).

⁴⁵ This study also investigated whether a difference in frequently addressed OECD principles between two industries was observed within each country. The contrasts between two industries were found to insignificant among six countries: U.S. ($\chi^2_{(7,N=6)} = 12.868, p = .075$), Canada ($\chi^2_{(7,N=6)} = 13.287, p = .065$), U.K. ($\chi^2_{(7,N=6)} = 12.667, p = .081$), Germany ($\chi^2_{(7,N=6)} = 12.952, p = .073$), Japan ($\chi^2_{(7,N=6)} = 13.707, p = .057$), and China ($\chi^2_{(7,N=6)} = 11.667, p = .112$).

The gap between the individuals' perceived importance of OECD principles and the frequently addressed OECD principles in companies' privacy policy statements was examined by comparing the rank order of each OECD principle. Table 26 shows the comparison between the rank order of the number of respondents who indicated each OECD principle as important and the rank order of the number of Web sites disclosing each OECD principle.

Table 26: Rank Order of OECD Principles

| OECD Principles | Information-sensitive Industry | | | Less Information-sensitive Industry | | |
|-------------------------------|--------------------------------|------------------------|------------------------|-------------------------------------|----------------------|---------------------|
| | <i>S*</i> (INFO1) | <i>LS**</i> (INFO2) | <i>CO***</i> (COM1) | <i>S</i> (INFO3) | <i>LS</i> (INFO4) | <i>CO</i> (COM2) |
| Accountability (AC) | 4 | 4 | 1 | 4 | 4 | 3 |
| Collection Limitation (CL) | 5 | 5 | 6 | 5 | 5 | 6 |
| Data Quality (DQ) | 7 | 6 | 8 | 8 | 7 | 8 |
| Individual Participation (IP) | 8 | 7 | 5 | 7 | 8 | 4 |
| Openness (OP) | 6 | 7 | 2 | 6 | 6 | 2 |
| Purpose Specification (PS) | 3 | 3 | 2 | 3 | 3 | 1 |
| Security Safeguards (SS) | 1 | 1 | 4 | 1 | 1 | 5 |
| Use Limitation (UL) | 2 | 2 | 7 | 2 | 2 | 7 |

* Rank order of individuals' perceived importance of each OECD principle when they were requested to provide sensitive personal information

** Rank order of individuals' perceived importance of each OECD principle when they were requested to provide less sensitive personal information

*** Rank order of the number of Web sites which disclose at least a piece of information about the OECD principle

The rank order of each OECD principle shows a difference in the perceived importance of OECD principles between individuals and companies in information-sensitive industries. When individuals were requested to provide personal information, the SS and UL principles were the two most important companies' privacy policies that individuals want to know regardless of the sensitivity of personal information. However, the two most frequently addressed OECD principles in companies' privacy policy statements were the AC and PS or OP principles. To investigate if there was a statistically significant difference in the perceived importance of OECD

principles between individuals and companies, Spearman's rho was used. The results of Spearman's rho between INFO1 and COM1 and between INFO2 and COM1 were found to be insignificant ($\gamma_s(8) = .204, p = .629$ and $\gamma_s(8) = .042, p = .921$, respectively). This indicates that in information-sensitive industries, the important companies' privacy policies that individuals want to know were not frequently addressed in companies' privacy policy statements.

Similarly, the difference in the perceived importance of OECD principles between individuals and companies was also observed in less information-sensitive industries. While the SS and UL principles were the two most important companies' privacy policies that individuals want to know when they were requested to provide both sensitive and less sensitive personal information, PS and OP were the two most frequently addressed OECD principles in companies' privacy policy statements. The Spearman's rho tests between INFO3 and COM2 and between INFO4 and COM2 indicate an insignificant association in the perceived importance of OECD principles between individuals and companies ($\gamma_s(8) = .143, p = .736$ and $\gamma_s(8) = .048, p = .911$, respectively). Thus, in less information-sensitive industries, there is a difference between the participants' perceived importance of OECD principles and the frequently addressed principles in companies' privacy policy statements. This suggests that companies' privacy policy statements failed to address the important OECD principles that individuals want to know in less information-sensitive industries. Based on these results, H19 is not supported. That is, there is a gap between what privacy practices individuals value and what companies disclose in their privacy policy statements.

8. Discussion

There have been a number of works that explore whether individuals' behaviour is influenced by their privacy concerns, companies' privacy practices, and company characteristics such as the trustworthiness of a company. However, there has been a dearth of studies that deal with the effect of an individual's involvement on his or her privacy behaviour, the effect of governmental involvement and cultural values on companies' privacy policies, and the gap between what individuals value and what companies emphasize. By conducting a Web-based user survey and an online ordering experiment, this study investigated whether individuals' behaviour is influenced by their level of involvement with privacy and the privacy policy disclosures of Web sites and whether there is a discrepancy between self-reported privacy behaviour and actual privacy behaviour. This study also performed a Web site survey of corporations, in order to examine the country and industry level differences in companies' privacy policy disclosures. These two studies are combined to examine the gap between the individuals' perceived importance of OECD principles and the frequently addressed OECD principles in companies' privacy policy statements.

8.1. Summary of Findings

The analysis of 420 Web sites' privacy policy statements and 210 participants' responses offers several interesting findings. Table 25 shows the summary of this study's findings.

Table 27: Summary of Study Findings

| Hypothesis | Self-reported Privacy Behaviour | Actual Privacy Behaviour |
|--|---------------------------------|--------------------------|
| H1 Individuals in a high privacy involved situation are more willing to perform an information search regarding companies' privacy practices (i.e., read privacy policy statement) than those in a low privacy involved situation. | Supported | Supported |
| H2 Individuals in a high privacy involved situation are less willing to provide their personal information than those in a low privacy involved situation. | Supported | Supported |

| | | | |
|---------|---|---------------|---------------|
| H3 | Individuals' behaviour with respect to reading a privacy policy statement is not influenced by a privacy seal in both high and low privacy involved situations. | Supported | Supported |
| H4 | Individuals' behaviour related to providing personal information is more influenced by a privacy seal under a low privacy involved situation than under a high privacy involved situation. | Not Supported | Not Supported |
| H5 | When the privacy policy statement of a company does not address the important privacy practices that individuals want to know, individuals are more willing to provide personal information to the Web site with a privacy seal compared to without a privacy seal. | Not Supported | Not Supported |
| <hr/> | | | |
| Results | | | |
| <hr/> | | | |
| H6 | There is a difference between self-reported privacy behaviour and actual privacy behaviour with respect to reading a privacy policy statement. | Not Supported | |
| H7 | There is a difference between self-reported privacy behaviour and actual privacy behaviour with respect to providing personal information. | Supported | |
| H8 | FIP principles addressed in companies' privacy policy statements vary across countries. | Supported | |
| H9 | Companies in information-sensitive industries (e.g., financial and health industries) incorporate more FIP principles in their privacy policy disclosures than do companies in less information-sensitive industries (e.g., manufacturing and retail industries). | Not Supported | |
| H10 | Companies that operate their business in high governmental involvement countries incorporate more FIP principles in their privacy policy disclosures than do companies in low governmental involvement countries. | Supported | |
| H11 | Companies in low power distance countries incorporate more FIP principles in their privacy policy disclosures than do companies in high power countries. | Supported | |
| H12 | Companies in high uncertainty avoidance countries incorporate more FIP principles in their privacy policy disclosures than do companies in low uncertainty avoidance countries. | Supported | |
| H13 | Companies in individualist cultures incorporate more FIP principles in their privacy policy disclosures than do companies in collectivist cultures. | Supported | |
| H14 | Companies in feminine cultures incorporate more FIP principles in their privacy policy disclosures than do companies in masculine cultures. | Not Supported | |
| H15 | Companies in short-term oriented cultures incorporate more FIP principles in their privacy policy disclosures than do companies in long-term oriented cultures. | Supported | |
| H16 | Individuals' perceived importance of FIP principles differs depending on the type of information requested. | Not Supported | |
| H17 | Individuals' perceived importance of FIP principles differs depending on the type of Web site. | Not Supported | |
| H18 | Companies in information-sensitive industries perceive FIP principles as having a different importance when compared to less information-sensitive industries. | Not Supported | |

H19 Companies incorporate more FIP principles that individuals perceived as important principles in their privacy policy disclosures than FIP principles that individuals perceived as less important.

Not Supported

First, the level of involvement has an influence on individuals' behaviour: *reading privacy policy statement* and *providing personal information* (H1 and H2). Respondents in the high privacy involved situation were more willing to read privacy policy statements than those in the low privacy involved situation, but they were less willing to provide their personal information than their counterpart. That is, the type of personal information requested is not only correlated with individuals' privacy concern but also influences their decision about information disclosure.

Second, respondents' behaviour with respect to reading a privacy policy statement was not affected by whether a Web site had a privacy seal (H3). Individuals were more likely read a privacy policy statement when they were requested to provide sensitive information. However, the existence of a privacy seal did not affect individuals' behaviour regardless of involvement conditions.

Third, when ordering a gift from an online shopping site, individuals in the high involved situation were less willing to provide their personal information than those in the low privacy involved situation. However, individuals' self-reported behaviour was influenced by the privacy policy disclosure of the site when they were in the high involvement condition, but not in the low involvement condition (H4). That is, when respondents were requested to provide sensitive information, they were less likely to provide their personal information to the Web site with no privacy disclosure than the site with a privacy policy statement or a privacy seal.

Fourth, individuals provided their personal information less often in the high privacy involved situation, compared to the low privacy involved situation. However, there was no association between actual behaviour and privacy policy disclosure (H4). Similar to self-reported behaviour, individuals' actual behaviour was not influenced by the privacy policy disclosure when they were requested to provide less sensitive information. However, unlike self-reported behaviour,

their actual behaviour was also not influenced by the privacy policy disclosure when they were asked to provide sensitive information.

Fifth, when the privacy policy statement did not address important privacy practices, individuals in the high privacy involved situations provided their personal information less than those in the low privacy involved situation. However, their behaviour was not influenced by the existence of a privacy seal (H5).

Sixth, there were mixed findings about the gap between self-reported behaviour and actual behaviour (H6 and H7). With respect to the reading privacy policy statement, individuals behaved close to what they said, but they behaved differently from what they said in terms of providing personal information.

Seventh, despite the possibility that the rapid advances in technologies and the widespread of the Internet may have diminished a difference in companies' privacy practices across countries, the results of this study suggest that there was indeed a difference in companies' privacy policies stated in privacy policy statements across six countries (H8). In addition, no difference was found between two industries (H9). That is, overall OECD principle disclosure was not significantly different between less information-sensitive industries and information-sensitive industries in all six countries. However, the analysis of each OECD principle reveals some differences between two industries regarding *Openness*, *Purpose Specification*, and *Security Safeguard* principles.

Eighth, there was a difference in the degrees of privacy policies associated with different governmental involvement structures (H10). Companies in high governmental involvement countries have higher levels of privacy policy disclosures than those in low governmental involvement countries.

Ninth, companies' privacy policies are also influenced by cultural values. Companies in high power distance cultures tend to have a lower level of privacy policy disclosure (H11). Companies in high uncertainty avoidance tend to have a higher level of privacy policy disclosure

(H12). Furthermore, companies in individualist cultures have higher levels of privacy practices than those in collectivist cultures (H13). Companies in feminine cultures tend to have lower level of privacy policy disclosure than their counterpart (H14). Finally, companies in short-term oriented cultures have higher levels of privacy practices than those in long-term oriented cultures (H15).

Tenth, respondents indicated that *Security Safeguards* and *Use Limitation* were the two most important OECD principles while *Data Quality* and *Individual Participation* were the two least important OECD principles. However, there was no difference in individuals' perceived importance of OECD principles with respect to the type of information and the type of industry (H16 and H17). That is, individuals did not perceive OECD principles differently depending on the type of information requested as well as the type of industry the Web site belongs to.

Eleventh, there was no difference in frequently addressed OECD principles between the two industry types (H18). Across country, certain OECD principles that were often addressed in companies' privacy policy statements in information-sensitive industries were also addressed in less information-sensitive industries, and vice versa.

Finally, the results of this study revealed a difference in the perceived importance of OECD principles between individuals and companies (H19). OECD principles that respondents perceived as important were not incorporated in companies' privacy policy statements. In general, this result concurs with those of Earp et al. (2005) who discover the gap between what individuals value and what companies emphasize in their privacy policies, although the research questions considered by Earp et al. are slightly different.

8.2. Implications

The findings of this study have several practical implications for individuals, companies, government, and privacy seal issuers. Customers' growing concerns about privacy have put pressure on e-commerce companies to develop customer-focused privacy practices (Culnan, 2000; Culnan and

Armstrong, 1999; Shapiro and Baker, 2001). Prior research has shown that by posting a privacy policy statement or a privacy seal on their Web sites, companies can reduce their customers' perceived privacy concerns about providing personal information (Palmer et al., 2000; Spiekermann et al., 2001). However, according to the findings of this study, it appears that even though the existence of a privacy policy statement affects individuals' behaviour, the privacy policy statement's content does not influence their behaviour. That is, individuals' decision about information disclosure is more affected by the fact that a company posts a privacy policy statement than the details of the company's privacy practices.

If individuals do not pay attention to the content of a privacy policy statement while they are making information disclosure decisions, it is likely that they may not come to an appropriate decision. The analysis of the gap between self-reported behaviour and actual behaviour indicated that there is a difference between what participants said and what they did with respect to providing personal information. However, there was no difference between what they said and what they did with respect to reading the privacy policy statement. Such differences in individual behaviour could reduce consumer trust in online transactions. This could have a negative impact on the proliferation of e-commerce and could in turn cause government to contemplate corrective legislation. Therefore, companies need to develop a more thoughtful managerial approach which includes a proactive focus on privacy issues before excessively restrictive regulation.

One possible way to address this issue would be by implementing P3P (Platform for Privacy Preferences) on corporate Web sites. P3P is a standardized, machine readable protocol, which is designed to block access to Web sites or automatically notify online users if a Web site's privacy policy is not in line with their pre-specified privacy preferences; the consumer is then left to decide whether he or she still wants to use the service. Coupled with a P3P user agent, P3P can reduce customers' privacy concerns. It builds trust and promotes the disclosure of personal information. One example of a P3P user agent is the AT&T Privacy Bird. It is a piece of software that reads privacy policies written in P3P and discloses the Web site's policies by displaying a bird icon. A green bird icon appears for

Web sites that match users' privacy preferences, but a red bird icon is shown for Web sites that do not. A yellow bird icon indicates Web sites that have not implemented P3P.

For individuals, they need to be proactive to protect their personal information from inappropriate use. For instance, when individuals are requested to provide personal information, they need to carefully examine not only the privacy policy statement but also the privacy seal posted on a Web site, instead of barely checking them. Then, they should make a decision about providing their personal information.

This study also found no association between privacy seals and individuals' behaviour. As indicated by the analysis of participants' responses to the question about privacy seals, quite a number of respondents specified VeriSign and other seals (e.g., VISA) as privacy seals. This suggests that many individuals fail to recognize genuine privacy seals, and possibly they do not have a clear understanding about privacy seals. Respondents also felt that privacy seal providers are less trustworthy than financial organizations, health service providers, and government organizations even though they are more trustworthy than e-commerce companies. Thus, privacy seals appear to be unsuccessful in attaining their objective, and the insignificant effect of a privacy seal on individuals' behaviour about providing personal information justifies this conjecture. To reach the intended goals and potential of privacy seals, privacy seal providers need to commit more effort and resources to educate consumers. They also need to establish a trust relationship with consumers by developing and promoting comprehensive standards and to ensure that the participants of privacy seal programs adhere to those standards. For the accounting profession, it is important to be aware of the significance of privacy in the electronic business environment and to take actions to establish the profession as a key player in privacy assurance services. Since the primary focus of privacy seal is to implement and test whether companies' privacy practices comply with existing privacy standards or regulations, public practice accountants can play a key role in privacy assurance services, given their experience and familiarity with financial reporting and auditing.

The results of this study show that companies' privacy policy disclosures vary across countries and cultures. The proliferation of the Web allows companies to reach potential customers

all around the world and thus makes a global marketplace possible. In a global marketplace, the flow of computerized information is a prerequisite for business transactions and also plays an important role. With the growing number of business transactions in the global marketplace, the flow of data and information often goes beyond borders and creates individuals' privacy concerns connected with this transborder data flow. To address these privacy concerns, companies and governments, therefore, need to develop a mechanism for providing assurance to their customers about their fair collection and use of customers' personal information, including data transfer beyond a border.⁴⁶

The results of this study also reveal that important companies' privacy practices that individuals want to know are not sufficiently addressed in companies' privacy policy disclosures. This gap suggests that companies need to respond effectively to customers' privacy concerns. According to the results, individuals' perceived important privacy practices did not vary due to the type of information requested and the type of industry a company belongs to. In general, this is in contrast with how information sensitivity affects customer behaviour (as seen in the first part of the study). Many respondents would like to know about how companies protect their personal information (i.e., security) and whether companies use personal information only for purposes which it was collected (i.e., use limitation). Hence, companies should communicate up front such customer needs by emphasizing related privacy practices in privacy policy statements, and thus they can reduce their customers' privacy concerns and build customer trust.

8.3. Limitations and Future Research

There are several limitations in this study. First, the findings of this study are specific to a particular customer group and thus could limit the generalizability of the findings. The respondents of the Internet privacy user survey and the online ordering experiment were all college students and from one

⁴⁶ As a part of such mechanism, the United States Department of Commerce and the European Commission in June 2000 made an agreement on the Safe Harbor negotiations which aim to harmonize data privacy practices in trading between the US and the stricter privacy controls of the European Union.

country (i.e., Canada). Therefore, their perceived information of OECD principles might not represent customers in other countries. In addition, compared to others, college students usually have enough computer skill and more online transaction experiences such as ordering goods, subscribing to services or registering on Web sites for online services. Hence, students may not be a completely representative of other consumer populations. Another possible avenue for future research examines whether individuals from various populations and countries perceive OECD principles differently and whether there is a gap between what they value and what companies emphasize in their privacy policy statements.

Second, the findings are specific to the particular e-commerce site (i.e., a Web site on which customers can order free gifts) and the particular task. Although the task of ordering a free gift from the experimental site is similar to the ordering process in real e-commerce sites, it is considerably different from the typical online transaction because it does not involve money and good exchange (i.e., no risk in purchasing decision). As a result, participants' behaviour on real e-commerce sites might be different.

Third, this study used a concocted seal (i.e., TRUSTWEB) because the prior experiences or the acquaintance with a specific privacy seal may influence individuals' behaviour. Although the results of the manipulation check showed that all participants recognize the TRUSTWEB seal, it is possible that the insignificant effect of the privacy seal on individuals' behaviour might be due to the use of a contrived seal. Future research could expand the research design by using one of the actual seals such as TRUSTe.

Fourth, based on ELM, this study anticipated that when individuals are under a low privacy involved situation, their behaviour would be affected by a cue, but not when individuals are under a high privacy involved situation. A privacy seal was used as a proxy for cue, and the study results reveal that the privacy seal did not influence individuals' behaviour in both situations. That is, the existence of the privacy seal failed to work as a cue. Another possible avenue for future research would examine other factors such as trustworthiness and reputation and assess whether such factors can play a role as a cue as described in ELM.

Fifth, there are also some limitations in measures. Individuals' behaviour with respect to reading a privacy policy statement was measured by examining whether they opened the privacy policy statement

Web page as well as the number of seconds they spent on the Web page. However, this study did not measure whether respondents in fact read the privacy policy statement or their understanding of the statement. This might limit the findings because individuals' behaviour with respect to providing personal information is substantially influenced by their understanding of companies' privacy practices. Furthermore, individuals' self-reported behaviour was measured by a small number of items due to time considerations, and thus it limits the reliability of self-reported measures.

Sixth, the 420 sample Web sites consist of top 70 Web sites each from six countries. While companies selected in this study are large companies, it is possible that the results may not necessarily reflect the practices of medium and small companies. Further, the Mergent Online database was used for sample selection. Although Mergent Online is a reliable source for company information, it does not have the list of all companies in each country. Especially, this study found that several big companies from China were not listed in the database of Mergent Online. Future research should not only include medium and small companies, but must also use other sources such as government databases to obtain sample companies. Also, this study simply classified industry into two categories based on the sensitivity of information and examined the difference in companies' privacy practices between these two industry types. Further research is also needed examining the differences among various industries.

Seventh, this study used OECD principles to compare companies' privacy policies across six countries. As discussed before, several FIPs have been developed across a variety of governments and organizations. Therefore, it is important to understand that the results of this study cannot be used for generalizing other FIPs. Future research could verify the findings of this study by using different FIP such as PIPEDA (Canada), EU Directive (EU), and GAPP (AICPA/CICA).

Eighth, this study used Hofstede's (1980) cultural dimensions as the operationalization of culture. Several concerns have been addressed with respect to Hofstede' country scores. Major concerns are including the limitations of gathering data from employees of a single organisation (i.e., IBM) in order to make inferences about national cultures and the relevance of Hofstede's original data (almost forty year old) to the present conditions (for more details see Goodstein, 1981;

McSweeney, 2002). Since Hofstede's study, several other studies have been undertaken to offer alternative models of cultures and new sets of cultural indices (e.g., House, 2004; Schwartz, 1994; Trompenaars, 1994). Additional research could investigate other typologies of cultural dimensions.

Finally, one of the important findings of this study is that important companies' privacy practices perceived by individuals were not sufficiently addressed in companies' privacy policy statements. However, the study did not provide an answer to the question of why this gap is presented. A thorough investigation of this matter is needed. Furthermore, there are some possible avenues for future research. They include: 1) whether the privacy policy statements currently disclosed by companies are effective in dealing with consumer knowledge and privacy concerns; 2) whether companies benefit by addressing customers' concerns about privacy; 3) whether companies provide sufficient privacy protection as required by various governments; and 4) what are the differences between Web sites that post privacy policies and sites that do not?

9. Conclusion

This study has addressed three research issues: (i) how an individual's privacy behaviour varies with respect to the level of privacy involvement and privacy policy disclosure; (ii) whether there is a difference in companies' privacy policies across countries and industries, whether governmental involvement and cultural values influence companies' privacy policies; and (iii) whether there is a gap between an individual's perceived importance of company practices and the privacy disclosures of companies.

Based on the Web-based user survey and the online ordering experiment involving 210 participants, this study found that individuals are more likely to read the privacy policy statements posted on Web sites and less likely to provide personal information when they are under a high privacy involved situation (i.e., when they requested to provide sensitive information) compared to a low privacy involved situation (i.e., when they asked to provide less sensitive personal information). However, the existence of

privacy seal did not affect individuals' behaviour regardless of involvement conditions. This study also found a gap between self-reported privacy behaviour and actual privacy behaviour. Furthermore, the analysis of 420 companies' privacy policy statements revealed the difference in companies' privacy policy disclosures across countries, and across varying governmental involvement and cultural values. Finally, a gap was found between individuals' importance ratings of companies' privacy practices and privacy policies that companies emphasize in their privacy policy disclosures.

Despite the limitations mentioned earlier, in general, the results of this study broaden our understanding of the relationship between the customer and company perspectives. Thus, the findings of the study would provide information as to whether individuals' privacy concerns are adequately addressed in companies' privacy policy disclosures and suggest a useful basis for identifying strategies which can reduce individuals' privacy concerns by empathizing privacy policies that they value in companies' privacy policy statements. Furthermore, the results of the privacy policy disclosure study would add important information to the debate of self-regulation versus government regulation.

References

- Ackerman, M. S., Cranor, L. F., and Reagle, J. (1999, November). *Privacy in e-commerce: examining user scenarios and privacy preferences*. Paper presented at the 1st ACM conference on Electronic Commerce, Denver, Colorado, United States
- Adler, N. J. (1991). *International Dimensions of Organizational Behavior* (2nd ed.). Boston, Mass.: PWS-KENT Pub. Co.
- AICPA/CICA. (2004). AICPA/CICA Privacy Framework. Retrieved April 10, 2005, from http://www.cica.ca/multimedia/Download_Library/Research_Guidance/Privacy/English/PrivacyFramework0304.pdf
- AICPA/CICA. (2006). Generally Accepted Privacy Principles: A Global Privacy Framework. Retrieved April 3, 2007, from http://infotech.aicpa.org/NR/rdonlyres/49B27EE4-4A2A-4EAF-A2A5-83067F32CE43/0/GAPP_Business_092006.pdf
- Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. In J. Kuhl and J. Beckman (Eds.), *Action-control: From cognition to behavior* (pp. 11-39). Heidelberg: Springer.
- Ajzen, I. (1987). Attitudes, traits, and actions: Dispositional prediction of behavior in personality and social psychology. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 20, pp. 1-63). New York: Academic Press.
- Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211.
- Altman, I. (1975). *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*. Monterey, Calif.: Brooks/Cole Pub. Co.
- Andrew, D. P. and Habte, G. S. (2003). Are cultural differences overrated? Examining the influence of national culture on international buyer-seller relationships. *Journal of Consumer Behaviour*, 2(4), 354.
- Antón, A. I., Earp, J. B., and Reese, A. (2002, September 9-13). *Analyzing Website Privacy Requirements Using a Privacy Goal Taxonomy*. Paper presented at the 10th Anniversary IEEE Joint International Conference on Requirements Engineering (RE).
- Ashley, P., Hada, S., Karjoth, G., and Schunter, M. (2002a, November 21-21). *E-P3P privacy policies and privacy authorization*. Paper presented at the The 2002 ACM Workshop on Privacy in the Electronic Society, Washington, DC.
- Ashley, P., Powers, C., and Schunter, M. (2002b, September 23-26). *From privacy promises to privacy management: a new approach for enforcing privacy throughout an enterprise*. Paper presented at the New Security Paradigms Workshop, Virginia Beach, Virginia.
- Aycan, Z., Kanungo, R. N., Mendonca, M., Yu, K., Deller, J., Stahl, G., et al. (2000). Impact of Culture on Human Resource Management Practices: A 10Country Comparison. *Applied Psychology: An International Review*, 49(1), 192-221.
- BBBOnline. (2006). BBBOnline Programs. Retrieved October 11, 2006, from <http://www.bbbonline.com/business/>
- Bellman, S., Johnson, E. J., Kobrin, S. J., and Lohse, G. L. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society*, 20(5), 313-324.
- Bellman, S., Lohse, G. L., and Johnson, E. J. (1999). Predictors of Online Buying Behavior. *Association for Computing Machinery. Communications of the ACM*, 42(12), 32.
- Bellotti, V. (1997). Design for privacy in multimedia computing and communications environments. In *Technology and privacy: the new landscape* (pp. 63-98). Cambridge, MA: MIT Press.
- Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, 19(4), 451-467.

- Berendt, B., Gunther, O., and Spiekermann, S. (2005). Privacy in E-commerce: Stated preferences vs. actual behavior. *Communications of the ACM*, 48(4), 101-106.
- Branscum, D. and Tanaka, J. (2000). Guarding Online Privacy. *Newsweek*, 135(23), 77.
- Burgoon, J. K. (1982). Privacy and communication. In M. Burgoon (Ed.), *Communication Yearbook* (Vol. 6, pp. 206-249): Beverly Hills, CA: Sage.
- Business Week. (2000, March 20). Business Week/Harris Poll: A Growing Threat. Retrieved March 24, 2004, from http://www.businessweek.com/2000/00_12/b3673010.htm?scriptFramed
- Caudill, E. M. and Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing*, 19(1), 7-19.
- Chakraborty, G., Lala, V., and Warren, D. (2002). An empirical investigation of antecedents of B2B Websites' effectiveness. *Journal of Interactive Marketing*, 16(4), 51-72.
- Chellappa, R. K. and Sin, R. G. (2005). Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, 6(2-3), 181.
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences (2nd ed.)*. Hillsdale, N.J. : Lawrence Erlbaum Assoc Inc.
- Coombs, W. and Cutbirth, C. (1998). Mediated political communication, the Internet, and the new knowledge elites: prospects and portents. *Telematics and Informatics*, 15(3), 203-217.
- Cranor, L. F., Arjula, M., and Guduru, P. (2002, November 21). *Use of a P3P user agent by early adopters*. Paper presented at the Workshop On Privacy In The Electronic Society, Washington, DC.
- Cranor, L. F. and AT&T Labs-Research. (2003). P3P: Making Privacy Policies More Useful. *IEEE Security & Privacy*, 1(6), 50-55.
- Culnan, M. J. (1999). *The Georgetown Internet Privacy Policy Survey: Report to the Federal Trade Commission*. Washington, DC: Georgetown University.
- Culnan, M. J. (2000). Protecting Privacy Online: Is Self-Regulation Working? *Journal of Public Policy & Marketing*, 19(1), 20-26.
- Culnan, M. J. and Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1), 104-115.
- Culnan, M. J. and Bies, R. J. (2003). Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), 323-342.
- Darley, W. K. and Smith, R. E. (1993). Advertising Claim Objectivity - Antecedents and Effects. *Journal of Marketing*, 57(4), 100-113.
- Desai, M. S., Richards, T. C., and Desai, K. J. (2003). E-commerce policies and customer privacy. *Information Management & Computer Security*, 11(1), 19-27.
- Dhillon, G. S. and Moores, T. T. (2001). Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14(4), 33-37.
- Diney, T. and Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Dommeier, C. J. and Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing*, 17(2), 35-51.
- Earp, J. B., Anton, A. I., Aiman-Smith, L., and Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, 52(2), 227-237.
- Earp, J. B. and Baumer, D. (2003). Innovative Web use to learn about consumer behavior and online privacy. *Communications of the ACM*, 46(4), 81-83.

- Federal Trade Commission (FTC). (1999). *Self-Regulation and Privacy Online: A Report to Congress*. Washington, DC.
- Federal Trade Commission (FTC). (2000). *Privacy online: Fair information practices in the electronic marketplace - A report to Congress*. Washington, DC.
- George, J. F. (2002). Influences on the intent to make Internet purchases. *Internet Research-Electronic Networking Applications and Policy*, 12(2), 165-180.
- George, J. F. (2004). The theory of planned behavior and Internet purchasing. *Internet Research-Electronic Networking Applications and Policy*, 14(3), 198-212.
- Goodstein, L. D. (1981). American Business Values and Cultural Imperialism. *Organizational Dynamics*, 10(1), 49-54.
- Graeff, T. R. and Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. *The Journal of Consumer Marketing*, 19(4), 302-318.
- Greenstein, M., M and Hunton, J. E. (2003). Extending the Accounting Brand to Privacy Services. *Journal of Information Systems*, 17(2), 87.
- Grimm, R. and Rossnagel, A. (2000, October 30-November 3). *Can P3P help to protect privacy worldwide?* Paper presented at the The 2000 ACM Workshops on Multimedia Los Angeles, California, United States.
- Gurau, C., Ranchhod, A., and Gauzente, C. (2003). "To legislate or not to legislate": a comparative exploratory study of privacy/personalisation factors affecting French, UK and US Web sites. *The Journal of Consumer Marketing*, 20(7), 652-664.
- Harris Interactive. (2002). *Privacy On and Off the Internet: What Consumers Want*. Hackensack, NJ.: Privacy & American Business.
- Harris Interactive. (2003). Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. Retrieved March 21, 2004, from www.harrisinteractive.com/harris_poll/index.asp?PID=365
- Hinde, S. (2003). Privacy legislation: a comparison of the US and European approaches. *Computers & Security*, 22(5), 378-387.
- Hochheiser, H. (2002). The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Transactions on Internet Technology (TOIT)*, 2(4), 276-306.
- Hoffman, D. L., Novak, T. P., and Peralta, M. (1999a). Building consumer trust online. *Communications of the ACM*, 42(2), 80-85.
- Hoffman, D. L., Novak, T. P., and Peralta, M. (1999b). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. *Information Society*, 15(2), 129-139.
- Hofstede, G. H. (1980). *Culture's Consequences: International Differences in Work-Related Values*. Beverly Hills, Calif.: Sage Publications.
- Hofstede, G. H. (1991). *Cultures and Organizations: Software of the Mind*. London: McGraw-Hill.
- Hofstede, G. H. (2001). *Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations* (2nd ed.). Thousand Oaks, Calif.: Sage Publications.
- Horton, R. P., Buck, T., Waterson, P. E., and Clegg, C. W. (2001). Explaining intranet use with the technology acceptance model. *Journal of Information Technology*, 16(4), 237-249.
- House, R. J. (2004). *Culture, Leadership and Organizations: The GLOBE Study of 62 Societies*. Thousand Oaks, CA: Sage.
- Huck, S. W. (2004). *Reading statistics and research* (4th ed.). Boston, MA: Allyn and Bacon.
- Hui, K.-L., Tan, B. C. Y., and Goh, C.-Y. (2006). Online information disclosure. *ACM Transactions on Internet Technology*, 6(4), 415-441.

- Hunton, J. E., Benford, T., Arnold, V., and Sutton, S., G. (2000). The Impact of Electronic Commerce Assurance on Financial Analysts' Earnings Forecasts and Stock Price Estimates. *Auditing*, 19(Supplement), 5-22.
- Jamal, K., Maier, M., and Sunder, S. (2003). Privacy in E-commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Market. *Journal of Accounting Research*, 41(2), 285.
- Johnson-Page, G. F. and Thatcher, R. S. (2001). B2C data privacy policies: Current trends. *Management Decision*, 39(4), 261-271.
- Kapferer, J. N. and Laurent, G. (1986). Consumer Involvement Profiles: A New Practical Approach to Consumer Involvement. *Journal of Advertising Research*, 25(6), 48-56.
- Kaplan, S. E. and Nieschwietz, R. J. (2003). An Examination of the Effects of WebTrust and Company Type on Consumers' Purchase Intentions. *International Journal of Auditing*, 7(2), 155-168.
- Kenny, S. and Korba, L. (2002). Applying digital rights management systems to privacy rights management. *Computers & Security*, 21(7), 648-664.
- Kovar, S. E., Burke, K. G., and Kovar, B. R. (2000). Consumer Responses to the CPA WEBTRUST™ Assurance. *Journal of Information Systems*, 14(1), 17-35.
- Koyuncu, C. and Lien, D. (2003). E-commerce and consumer's purchasing behaviour. *Applied Economics*, 35(6), 721.
- Lala, V., Arnold, V., Sutton, S. G., and Guan, L. (2002). The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior. *International Journal of Accounting Information Systems*, 3, 237-253.
- Laudon, K. C. (1996). Markets and Privacy. *Communications of the ACM*, 39(9), 92-104.
- Laufer, R. S. and Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, 33(3), 22-42.
- Liu, C. and Arnett, K. P. (2002). An Examination of Privacy Policies in Fortune 500 Web Sites. *Mid-American Journal of Business*, 17(1), 13-21.
- Liu, C., Marchewka, J. T., and Ku, C. (2004). American and Taiwanese Perceptions Concerning Privacy, Trust, and Behavioral Intentions in Electronic Commerce. *Journal of Global Information Management*, 12(1), 18-40.
- Long, G., Hogg, M. K., and Hartley, M. (1999). Relationship marketing and privacy: exploring the thresholds. *Journal of Marketing Practice*, 5(1), 4-20.
- Louis Harris and Associates and Westin, A. F. (1994). *Equifax-Harris Consumer Privacy Survey 1994*. Atlanta, GA: Equifax Inc.
- Louis Harris and Associates and Westin, A. F. (1996). *1996 Equifax-Harris Consumer Privacy Survey*. Atlanta, Georgia: Equifax, Inc.
- Louis Harris and Associates and Westin, A. F. (1998). *E-commerce & Privacy: What Net Users Want*. Hackensack, NJ: Privacy & American Business.
- Luo, X. M. (2002). Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. *Industrial Marketing Management*, 31(2), 111-118.
- Lwin, M. O. and Williams, J. D. (2003). A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online. *Marketing Letters*, 14(4), 257-272.
- Mak, B., Schmitt, B. H., and Lyytinen, K. (1997). User participation in knowledge update of expert systems. *Information & Management*, 32(2), 55-63.

- Malhotra, N. K., Kim, S. S., and Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4), 336-355.
- Maxwell, S. E. and Delaney, H. D. (1990). *Designing Experiments and Analyzing Data: A Model Comparison Perspective*. Belmont, Calif.: Wadsworth Pub. Co.
- McCullough, T. and Dodge, H. (2002). Understanding the Role Consumer Involvement Plays in the Effectiveness of Hospital Advertising *Health Marketing Quarterly*, 19(3), 3-20.
- McSweeney, B. (2002). Hofstede's model of national cultural differences and their consequences: A triumph of faith - a failure of analysis. *Human Relations*, 55(1), 89-118.
- Mergent Online. (2006). About Mergent Online. Retrieved May 29, 2006, from <http://www.mergentonline.com/noticesCM.asp?contentscode=About>
- Milberg, S. J., Burke, S. J., Smith, H. J., and Kallman, E. A. (1995). Values, Personal Information Privacy, and Regulatory Approaches. *Communications of the ACM*, 38(12), 65-74.
- Milberg, S. J., Smith, H. J., and Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science*, 11(1), 35-57.
- Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing*, 19(1), 1-6.
- Milne, G. R. and Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, 13(1), 5-24.
- Milne, G. R. and Culnan, M. J. (2002). Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2001 U.S. Web Surveys *Information Society*, 18(5), 345-359.
- Milne, G. R. and Rohm, A. J. (2000). Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives. *Journal of Public Policy & Marketing*, 19(2), 238-249.
- Miyazaki, A. D. and Fernandez, A. (2000). Internet Privacy and Security: An Examination of Online Retailer Disclosures. *Journal of Public Policy & Marketing*, 19(1), 54-61.
- Miyazaki, A. D. and Fernandez, A. (2001). Consumer Perceptions of Privacy and Security Risks for Online Shopping. *Journal of Consumer Affairs*, 35(1), 27-44.
- Miyazaki, A. D. and Krishnamurthy, S. (2002). Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions. *Journal of Consumer Affairs*, 36(1), 28-49.
- Moore, T. T. (2005). Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM*, 48(3), 86-91.
- Moore, T. T. and Dhillon, G. S. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM*, 46(12), 265-271.
- Nijhawan, D. R. (2003). The Emperor has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation *Vanderbilt Law Review*, 56(3), 939-976.
- Nowak, G. J. and Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Interactive Marketing*, 11(4), 94-108.
- O'Neil, D. (2001). Analysis of Internet Users' Level of Online Privacy Concerns. *Social Science Computer Review*, 19(1), 17-31.
- O'Connor, N. G. (1995). The influence of organizational culture on the usefulness of budget participation by Singaporean-Chinese managers. *Accounting, Organizations and Society*, 20(5), 383.
- Odom, M. D., Kumar, A., and Saunders, L. (2002). Web Assurance Seals: How and Why They Influence Consumers' Decisions. *Journal of Information Systems*, 16(2), 231-250.

- Organization for Economic Cooperation and Development (OECD). (1980). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved April 20, 2005, from http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
- Palmer, J. W., Bailey, J. P., and Faraj, S. (2000). The Role of Intermediaries in the Development of Trust on the WWW: The Use and Prominence of Trusted Third Parties and Privacy Statements. *Journal of Computer-Mediated Communication*, 5(3).
- Peterson, R. A. (2001). On the Use of College Students in Social Science Research: Insights from a Second-Order Meta-analysis. *Journal of Consumer Research*, 28(3), 450-461.
- Petty, R. D. (2000). Marketing Without Consent: Consumer Choice and Costs, Privacy, and Public Policy. *Journal of Public Policy & Marketing*, 19(1), 42-53.
- Petty, R. E. and Cacioppo, J. T. (1986). *Communication and Persuasion: Central and Peripheral Routes to Attitude Change*. New York: Springer/Verlag.
- Petty, R. E. and Wegener, D. T. (1999). The Elaboration Likelihood Model: Current Status and Controversies In S. Chaiken and Y. Trope (Eds.), *Dual -Process Theories in Social Psychology*. New York: Guilford.
- Pham, M. T. and Avnet, T. (2004). Ideals and Oughts and the Reliance on Affect versus Substance in Persuasion. *Journal of Consumer Research*, 30(4), 503-518.
- Phelps, J., D'Souza, G., and Nowak, G. (2001). Antecedents and consequences of consumer privacy concerns: An empirical investigation. *Journal of Interactive Marketing*, 15(4), 2-17.
- Phelps, J., Nowak, G., and Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), 27-41.
- Porter, A. M. (2000). Buyers want Web Privacy. *Purchasing*, 129(5), 22-25.
- Quaddus, M. A. and Tung, L. L. (2002). Explaining cultural differences in Decision Conferencing. *Communications of the Acm*, 45(8), 93-98.
- Ranganathan, C. and Ganapathy, S. (2002). Key dimensions of business-to-consumer web sites. *Information & Management*, 39(6), 457-465.
- Reiter, M. K. and Rubin, A. D. (1999). Anonymous Web transactions with Crowds. *Communications of the ACM*, 42(2), 32-38.
- Rezgui, A., Bouguettaya, A., and Eltoweissy, M. Y. (2003, November-December). Privacy on the Web: Facts, Challenges, and Solutions *IEEE Security & Privacy*, 1, 40-49.
- Rothschild, M. L. (1984). Perspectives on Involvement: Current Problems and Future-Directions. *Advances in Consumer Research*, 11, 216-217.
- Rust, R. T., Kannan, P. K., and Peng, N. (2002). The Customer Economics of Internet Privacy *Journal of the Academy of Marketing Science*, 30(4), 455-464.
- Sarathy, R. and Robertson, C. J. (2003). Strategic and Ethical Considerations in Managing Digital Privacy. *Journal of Business Ethics*, 46(2), 111-126.
- Schoder, D. and Yin, P. L. (2000). Building firm trust online. *Communications of the ACM*, 43(12), 73-79.
- Schwaig, K. S., Kane, G. C., and Storey, V. C. (2005). Privacy, fair information practices and the fortune 500: the virtual reality of compliance. *ACM SIGMIS Database*, 36(1), 49-63
- Schwartz, S. H. (1992). Universals in the structure and content of values: theoretical advances and empirical tests in 20 countries. In M. P. Zanna (Ed.), *Awareness in Experimental Social Psychology* (Vol. 25, pp. 1-65). New York: Academic Press.
- Schwartz, S. H. (1994). Beyond Individualism/Collectivism: New Cultural Dimensions of Values. In U. Kim, H. C. Triandis, C. Kagitcibasi, S. C. Choi, and G. Yoon (Eds.), *Individualism and Collectivism: Theory, Method, and Applications*. Thousand Oaks, CA: Sage.

- Shankar, V., Urban, G. L., and Sultan, F. (2002). Online trust: a stakeholder perspective, concepts, implications, and future directions. *Journal of Strategic Information Systems*, 11(3-4), 325-344.
- Shapiro, B. and Baker, C. R. (2001). Information technology and the social construction of information privacy. *Journal of Accounting and Public Policy*, 20(4), 295-322.
- Sheehan, K. B. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4), 24-38.
- Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society*, 18(1), 21-32.
- Sheehan, K. B. and Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28(3), 37-51.
- Sheehan, K. B. and Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing*, 19(1), 62-73.
- Smith, H. J. (1993). Privacy Policies and Practices - Inside the Organizational Maze. *Communications of the ACM*, 36(12), 105-122.
- Smith, H. J. (1994). *Managing Privacy: Information Technology and Corporate America*. Chapel Hill: University of North Carolina Press.
- Smith, H. J. (2001). Information privacy and marketing: What the U.S. should (and shouldn't) learn from Europe. *California Management Review*, 43(2), 8-33.
- Smith, H. J., Milburg, S. J., and Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167-196.
- Spiekermann, S., Grossklags, J., and Berendt, B. (2001, October 14-17). *E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior*. Paper presented at the 3rd ACM conference on Electronic Commerce Tampa, Florida, USA.
- Stewart, K. A. and Segars, A. H. (2002). An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), 36-49.
- Stone, D. L. and Stone, E. F. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. *Research in Personnel and Human Resources Management*, 8, 349-411.
- Straub, D., Boudreau, M.-C., and Gefen, D. (2004). Validation Guidelines for IS Positivist Research. *Communications of the Association for Information Systems* 13, 380-427.
- Swaminathan, V., Lepkowska-White, E., and Rao, B. P. (1999). Browsers or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange. *Journal of Computer-Mediated Communication*, 5(2).
- Szajna, B. (1996). Empirical Evaluation of the Revised Technology Acceptance Model. *Management Science*, 42(1), 85-92.
- Triandis, H. C. (1989). The Self and Social-Behavior in Differing Cultural Contexts. *Psychological Review*, 96(3), 506-520.
- Trompenaars, A. (1994). *Riding the Waves of Culture: Understanding Diversity in Global Business*. Burr Ridge, Illinois: Irwin Professional Pub.
- TRUSTe. (2006, Jan. 10). TRUSTe Fact Sheet. Retrieved October 11, 2006, from http://www.truste.org/about/fact_sheet
- UNISYS. (2006). Global Study on the Public's Perceptions about Identity Management. Retrieved July 3, 2007, from http://www.unisys.com/eprise/main/admin/corporate/doc/ID_Research_w_paper.pdf
- United Press International (UPI). (2007). UPI-Zogby Poll: Concern on Health Privacy. Retrieved July 3, 2007, from http://www.upi.com/Zogby/UPI_Polls/2007/02/21/upi_poll_concern_on_health_privacy/

- Vila, T., Greenstadt, R., and Molnar, D. (2003, September 30-October 3). *Why we can't be bothered to read privacy policies models of privacy economics as a lemons market*. Paper presented at the 5th International Conference on Electronic Commerce Pittsburgh, Pennsylvania.
- Vitell, S. J., Nwachukwu, S. L., and Barnes, J. H. (1993). The effects of culture on ethical decision-making: An application of Hofstede's typology. *Journal of Business Ethics*, 12(10), 753.
- Wang, H. Q., Lee, M. K. O., and Wang, C. (1998). Consumer privacy concerns about Internet marketing. *Communications of the ACM*, 41(3), 63-70.
- Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, IV(5), 193-220.
- WebTrust. (2006). A Sampling of Sites with SysTrust/WebTrust Seals. Retrieved October 11, 2006, from <http://www.webtrust.org/abtseals.htm>
- Westin, A. F. (1967). *Privacy and Freedom* (1st ed.). New York, NY: Atheneum.
- Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431-453.
- Williams, R. M. (1968). Values. In E. Sills (Ed.), *International Encyclopedia for the Social Sciences* (pp. 283-287). New York: Macmillan.
- Williams, R. M. (1970). *American Society: A Sociological Interpretation* (3rd ed.). New York: Knopf.
- Zaichkowsky, J. L. (1985). Measuring the Involvement Construct. *Journal of Consumer Research*, 12(3), 341-352.
- Zogby. (2007). UPI-Zogby International Poll: Most Americans Worry About Identity Theft. Retrieved July 4, 2007, from <http://www.zogby.com/NEWS/ReadNews.dbm?ID=1275>

Appendix I: An Annotated Bibliography of 74 Key Studies

| Study | Description | Research Area | Research Framework |
|---|---|---|---|
| Ackerman, Cranor, and Reagle (1999) | <ul style="list-style-type: none"> Examines Internet users' concerns and preferences about privacy Shows that 1) there are significant differences in comfort level across the various types of information; 2) there are several important factors in decisions about information discourse: the sharing of information with other companies and organizations, the use of information in an identifiable way, the kind of information collected, the purpose for which the information is collected, and so on; and 3) acceptance of the use of persistent identifiers varies according to the purpose; Internet users dislike to receive unsolicited communications and automatic data transfer. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Consumer Perspective |
| Antón, Earp, and Reese (2002) | <ul style="list-style-type: none"> Introduces a privacy goal taxonomy by using Goal-Based Requirements Analysis Method and reports the analysis of 23 Internet privacy policies for companies in three health care industries. | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Privacy and Technology |
| Ashley, Hada, Karjoth, and Schunter (2002a) | <ul style="list-style-type: none"> Describes the formal model of the Platform for Enterprise Privacy Practices (E-P3P), the semantics (XML) of the E-P3P language, and the authorization engine processing for enterprise privacy policies. | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Privacy and Technology |
| Bellman, Johnson, Kobrin, and Lohse (2004) | <ul style="list-style-type: none"> Examines whether the differences in information privacy concerns across countries is due to difference in cultural values, Internet experience, or regulatory structure and also investigates the relation between the desire for privacy regulation and government involvement. Shows that cultural value and Internet experience are related to the country differences in concerns about information privacy and the desire for more privacy regulation affects the level of government involvement. | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Consumer Perspective |
| Ben-Ze'ev (2003) | <ul style="list-style-type: none"> Examines the concept of privacy. Argues that the conflicts between privacy and emotional closeness and between privacy and openness are weaker in cyberspace than in real world because of the relative anonymity of cyberspace and the ability to reveal matters which individuals | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Internet Privacy in General |

| | | | |
|--|--|-----------------------|---|
| | would like to reveal. | | |
| Berendt, Günther, and Spiekermann (2005) | <ul style="list-style-type: none"> • Examine whether there is a discrepancy between self-reported privacy concerns and actual self-disclosing behaviour, and the impact of privacy statements. • Shows a gap between self-reported privacy concerns and actual self-disclosing behaviour | • Information System | • Customer Perspective |
| Caudill and Murphy (2000) | <ul style="list-style-type: none"> • Examines online privacy in conceptual and historical perspectives and discusses approaches for customer privacy such as government regulation and industry self-regulation. • Proposes several suggestions for corporate ethical policy and public policy based on ethical theories and discusses an agenda for future research. | • Marketing | <ul style="list-style-type: none"> • Company Perspective • Government Perspective |
| Chakraborty, Lala, and Warren (2002) | <ul style="list-style-type: none"> • Examines factors affecting customers' perceptions of the effectiveness of Business-to-Business (B2B) Web sites. • Identifies eight factors which may influence B2B Web site effectiveness and shows that informativeness, organization, transaction-related interactivity, and personalization have effect on B2B Web site effectiveness, but non-transaction-related interactivity, privacy/security, accessibility, and entertainment do not. | • Marketing | • Customer Perspective |
| Cranor (2003) | <ul style="list-style-type: none"> • Explains the Platform for Privacy Preferences (P3P) and describes P3P software and services | • Information Systems | • Privacy and Technology |
| Cranor, Arjula, and Guduru (2002) | <ul style="list-style-type: none"> • Examines the impact of P3P on users by using AT&T Privacy Bird, a P3P user agent. • Shows a larger proportion of AT&T Privacy Bird users read privacy policies more often and protect their privacy more proactively. | • Information Systems | • Privacy and Technology |
| Culnan (2000) | <ul style="list-style-type: none"> • Examines whether Web sites (361 commercial Web sites) post privacy disclosures and whether the disclosures reflect fair information practices. • Shows that 1) the majority of the sites collect personal identifying information and/or demographic information; 2) 65.9% of the 361 sites post at least one privacy disclosure; and 3) only 13.6% of the sites that collected personal information and posted a privacy disclosure comprehensively reflects fair information practices. | • Marketing | • Company Perspective |
| Culnan and Armstrong | <ul style="list-style-type: none"> • Examines the role of procedural fairness in addressing the privacy concerns which arise between the collection and use of personal information. | • Management | • Customer Perspective |

| | | | |
|-----------------------------------|--|--|---|
| (1999) | <ul style="list-style-type: none"> Shows that 1) people with a greater concern for privacy are less willing to be profiled when they are not told that fair information practices (procedural fairness) are employed to manage their personal information; 2) there is no difference between people who are willing to be profiled and those who are unwilling to be profiled when they are told that fair information practices is employed; and 3) people who are willing to be profiled are more likely to have prior experience with targeted marketing than those who are unwilling to be profiled. | | |
| Culnan and Bies (2003) | <ul style="list-style-type: none"> Discusses consumer privacy in a justice perspective. Addresses three types of justice factors related to consumer privacy (i.e., distributive justice, procedural justice, international justice) and argues that the violation of these factors may lead consumers' privacy concerns. Explains fair information practices in justice concerns and three implementation alternatives of implementing fair information practices (government regulation, self-regulation, and technological solutions). | <ul style="list-style-type: none"> Psychology and Sociology | <ul style="list-style-type: none"> Customer – Company – Government Interaction |
| Desai, Richards, and Desai (2003) | <ul style="list-style-type: none"> Investigates Internet policies posted on firms' Web sites and examines whether these policies have been changed over three years (between 1999 and 2001). Shows that privacy related policy is the most frequently posted on firms' Web sites and that companies are improving the communication of their policies to customers. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Company Perspective |
| Dhillon and Moores (2001) | <ul style="list-style-type: none"> Examines major issues that could be of potential concern for individuals with respect to Internet privacy. Identifies five fundamental Internet privacy issues and eighteen means objectives in achieving the fundamental Internet privacy objectives. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Customer Perspective |
| Dommeyer and Gross (2003) | <ul style="list-style-type: none"> Investigates consumers' knowledge and awareness of privacy-related regulations and practices as well as the use of privacy protection strategies and examines the relationship between consumers' characteristics and their awareness and user of privacy protection strategies. Shows that; 1) consumers have limited knowledge about direct marketing practices and regulations; 2) consumers do not effectively use privacy protection strategies; 3) males and young consumers are more aware of privacy protection strategies than females and old customers; and 4) privacy protection strategies are most likely used by young people and people who dislike receiving direct marketing solicitations. | <ul style="list-style-type: none"> Marketing | <ul style="list-style-type: none"> Customer Perspective |

| | | | |
|--|--|-----------------------|----------------------------------|
| Earp, Anton, Aiman-Smith, and Stufflebeam (2005) | <ul style="list-style-type: none"> • Examines the information provided in companies' privacy policy statements, the information that users want to know about Internet privacy, and the gap between them. • Shows that the information addressed in Web site privacy policy statements does not fully provide the information that users want to know. | • Information Systems | • Customer - Company Interaction |
| Earp and Baumer (2003) | <ul style="list-style-type: none"> • Examines consumers' behaviour and online privacy. • Shows that; 1) type of Web site and brand status influence the willingness of individuals to reveal their information; 2) the type of information individuals are willing to provide differ with respect to the type of Web site and brand status; and 3) consumers protect themselves by discriminating about information they are willing to reveal. | • Information Systems | • Customer Perspective |
| George (2002) | <ul style="list-style-type: none"> • Examines a structural model which indicates the relationship beliefs about privacy and Internet trustworthiness, attitude, intention, and behaviour. • Shows that beliefs about privacy and Internet trustworthiness influence attitudes towards the Internet, which in turn, affect intent to make Internet purchases. | • Information Systems | • Customer Perspective |
| George (2004) | <ul style="list-style-type: none"> • Examines the relationships between beliefs about privacy and trustworthiness of the Internet and actual purchasing behaviour. • Shows that; 1) attitudes toward Internet purchasing are influenced by beliefs about Internet trustworthiness influence attitudes toward Internet purchasing, but not by beliefs about unauthorized use of personal information; 2) attitudes toward Internet purchasing, in turn, affect actual purchasing behaviour; 3) perceived behavioural control is influenced by beliefs about self-efficacy, which in turn, affects actual purchasing behaviour; and 4) there is a relationship between normative structure and subjective norms, but subjective norms do not have impact on actual purchasing behaviour. | • Information Systems | • Customer Perspective |
| Graeff and Harmon (2002) | <ul style="list-style-type: none"> • Examines customers' concerns about the collection and use of personal information, their knowledge about data collection practices, the influence of demographics factors on their concerns, and the relationship between customers' concerns and their purchasing behaviours. • Shows that 1) customers are concerned about the collection and use of their personal information, and their concerns vary across retailers (retail store, restaurant, purchasing over the phone, and purchasing over the Internet); 2) gender, age and | • Marketing | • Customer Perspective |

| | | | |
|--------------------------------------|---|--|--|
| | income influence customers' privacy concerns; 3) customers' Internet purchasing behaviours are affected by age and income, but not by gender; and 4) customers' privacy concerns are significantly related to their purchasing behaviours over the Internet. | | |
| Greenstein and Hunton (2003) | <ul style="list-style-type: none"> Examines a) skills that potential clients view as necessary to perform privacy services and whether they perceive that CPA firms possess the skills that are necessary to perform privacy services, b) whether potential clients perceive that CPA firms possess the necessary skills, c) whether potential clients view privacy services as part of or separate from audit, d) whether potential clients are likely to hire a CPA firm to perform privacy services, and e) whether a brochure produced by the American Institute of Certified Accountants (AICPA) change potential clients' belief regarding CPA firms' qualifications Identifies four skill level categories that the management of audit client view as necessary: technical skills, legal skills, and control/assurance skills, and strategic skills. Shows that; 1) managers believe that CPA firms had high technical and control assurance skills, but low strategic and legal skills; 2) managers consider that privacy services should be separated from the auditing engagement; 3) managers have low willingness to engage a CPA firm to conduct privacy services; and 4) the brochure produced by AICPA increases managers' perception regarding the ability of CPA firms to perform privacy services. | <ul style="list-style-type: none"> Accounting and Information Systems | <ul style="list-style-type: none"> Privacy and Assurance Services |
| Grimm and Rossnagel (2000) | <ul style="list-style-type: none"> Provides a brief overview about the history and current state of P3P. Examines the effect of P3P with respect to privacy regulations in Germany and Europe. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Privacy and Technology |
| Gurau, Ranchhod, and Gauzente (2003) | <ul style="list-style-type: none"> Examines the privacy-related dimensions of three countries Web sites (French, UK, and US). Shows that there are differences among countries with respect to the form of data request and information provided in the privacy disclosure. | <ul style="list-style-type: none"> Marketing | <ul style="list-style-type: none"> Company Perspective |
| Hochheiser (2002) | <ul style="list-style-type: none"> Provides an overview of the Platform for Privacy Preferences (P3P) and three proposed P3P model of privacy (OECD, U.S FTC, and Canadian). Examines P3P from both historical and technical perspectives by focusing on political, legislative, and regulatory context in the U.S. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Privacy and Technology |

| | | | |
|--|---|-----------------------------------|---|
| Hoffman, Novak, and Peralta (1999a) | <ul style="list-style-type: none"> • Examines key customer perceptions of privacy by analyzing two surveys • Shows that the primary barriers to customers' providing personal information to Web sites are related to trust and the nature of the exchange relationship and customers' online purchasing behaviour is influenced by control over their personal information and their online skills. | • Information Systems (Marketing) | • Customer Perspective |
| Hoffman, Novak, and Peralta (1999b) | <ul style="list-style-type: none"> • Examines how consumers' privacy concerns affect commercial activity on the Web and discusses the implication of these concerns for the commercial uses of online anonymity on the Web. • Addresses the conflict an interest between commercial Web providers and consumers in online transactions due to the customer lack of trust in online commercial environments, and argues that the feasible short-run solution to resolve the conflict is to allow customers to be anonymous and/or pseudonymous in information exchanges and online transaction, but the long-run solution is to gain consumer trust by allowing the balance of power between a business and its customers. | • Information systems | • Customer - Company Interaction |
| Hui, Teo, and Lee (2006) | <ul style="list-style-type: none"> • Examines whether two types of privacy assurance (i.e., privacy statements and privacy seals) influence individuals' behaviour. • Shows that 1) the existence of privacy policy statement encouraged individuals to provide their personal information, but that of a privacy seal did not; 2) the positive effect of monetary incentive on information disclosure; and 3) the negative effect of the amount of information requested on individuals' information disclosure. | • Information systems | • Customer - Company Interaction |
| Hunton, Benford, Arnold, and Sutton (2000) | <ul style="list-style-type: none"> • Examines the effect of e-commerce assurance on financial analysts' earnings forecast and stock price estimates. • Shows that financial analysts issue more positive earnings forecasts and stock-price estimates when an e-commerce company acquired e-commerce assurance (i.e., WebTrust) and vendor- and outcome-based risks were high (i.e., the company is unknown and the perceived outcome risk from transactions is high). | • Accounting | • Privacy and Assurance Services |
| Jamal, Maier, and Sunder (2003) | <ul style="list-style-type: none"> • Examines privacy disclosure and the effectiveness of opt-out practices of high traffic e-commerce Web sites with respect to Notice/Awareness and Choice/Consent privacy principles to see what corporations do in the absence of regulatory standards. • Shows that the stated privacy policies in e-commerce Web sites closely comply with actual disclosure and opt-out practices with respect to Notice/Awareness and | • Accounting | <ul style="list-style-type: none"> • Company Perspective • Company – Government Interaction |

| | | | |
|---------------------------------------|---|---|--|
| | Choice/Consent privacy principles and argues that there is no evidence to intervene government regulation since the e-commerce industry shows signs of developing industry standards or norms in the absence of government regulation. | | |
| Johnson-Page and Thatcher (2001) | <ul style="list-style-type: none"> Examines the data privacy policies on B2C Web sites in nine countries (USA, Canada, Germany, Hungary, UK, China, Singapore, Brazil, and Venezuela) and five industries (banking and financial services, Internet service providers, newspapers, online retailers, and telecommunications). Claims that data privacy policies on B2C Web sites are more commonly found in countries which establish market economy with clear business regulations and in which customers have more access to the Web as well as the experience of using it. | • Management | • Company Perspective |
| Kenny and Korba (2002) | <ul style="list-style-type: none"> Provides an overview of Digital Rights Management (DRM). Addresses the use of DRM technology as a potential tool for the management of personal information and proposes the adaptation of DRM technology to address the challenges in Privacy Rights Management (PRM). | • Information Systems | • Privacy and Technology |
| Koyuncu and Lien (2003) | <ul style="list-style-type: none"> Examines the effect of sexual preferences, primary place of online access, online experiences, and demographic and economic factors as well as certain critical Internet issues such as taxation, privacy, and censorship on the consumer's purchasing decision. Shows that; 1) sexual preferences have a significant effect on online purchasing; 2) primary place of online access and online experience affect online users' purchasing behaviour; and 3) the issues of taxation of services and privacy influence online purchasing decisions. | • Economics | • Customer Perspective |
| Lala, Arnold, Sutton, and Guan (2002) | <ul style="list-style-type: none"> Examines the impact of assurance seals (i.e., BBBOnLine and WebTrust) and the information quality provided by such seals on consumers' Internet purchasing behaviour. Shows that assurance seals have a positive effect on consumers' purchasing behaviour and the impact of assurance seals with the different level of information quality. | <ul style="list-style-type: none"> Accounting Information Systems | <ul style="list-style-type: none"> Customer - Company Interaction Privacy and Assurance Services |
| Laudon (1996) | <ul style="list-style-type: none"> Introduces market-based mechanisms based on individual ownership of personal information and proposes a National Information Market (NIM) in which individuals can receive fair compensations for the use of information about themselves. | • Information Systems | • Government Perspective |

| | | | |
|--|---|-----------------------|------------------------|
| Liu and Arnett (2002) | <ul style="list-style-type: none"> Examines the use of stated privacy policies in large U.S. companies for responding to customers' privacy concerns, and investigates the use of fair information practices in privacy policies. Shows that; 1) slightly more than 50 percent of Fortune 500 Web sites provide privacy policy; 2) the use of privacy policies to address customers' privacy concerns is not limited to certain industries; and 3) many Fortune 500 Web sites fail to cover all four privacy dimensions recommended by FTC, but most of them address opt-out, access/correction, and internal privacy protection. | • Business | • Company Perspective |
| Liu, Marchewka, and Ku (2004) | <ul style="list-style-type: none"> Compares American and Taiwanese perceptions concerning online privacy and how it relates to the level of trust with a company's e-commerce Web site. Shows that; 1) privacy concerns have a positive influence on the level of trust concerning an e-commerce Web site; 2) the level of trust have a positive relationship with behaviour intentions for online transactions; and 3) the cultural backgrounds do not have influence on the results. | • Information Systems | • Customer Perspective |
| Long, Hogg, Hartley, and Angold (1999) | <ul style="list-style-type: none"> Examines how customers consider the collecting and use of their personal information in a various situations by companies pursuing relationship marketing strategies. Shows that; 1) customers have different levels of involvement with respect to information privacy; 2) they have different perceptions of revealing, receiving, and sharing information in different situational settings; and 3) customers have various levels of trustworthiness of firms in different sectors of the service industry. | • Marketing | • Customer Perspective |
| Luo (2002) | <ul style="list-style-type: none"> Examines the nature of customers' privacy concerns and their trust of electronic business and investigates three trust building mechanisms that can increase customers' trust and decrease their privacy concerns. | • Marketing | • Customer Perspective |
| Lwin and Williams (2003) | <ul style="list-style-type: none"> Develops a conceptual model to examine factors driving fabrication of information online based on Laufer and Wolfe's (1977) Multidimensional Developmental Theory of Privacy and Ajzen's (1987, 1991) Theory of Planned Behaviour with Perceived Moral Obligation and tests the conceptual model based on Theory of Planned Behaviour Shows that attitudes, perceived behavioural control, and perceived moral obligation are significant drivers for fabricating information, while subjective norms are not. | • Marketing | • Customer Perspective |

| | | | |
|--|--|---|---|
| <p>Malhotra, Kim, and Agarwal (2004)</p> | <ul style="list-style-type: none"> • Examines the nature and dimensionality of Internet users' information privacy concerns (IUIPC), introduces a measure for IUIPC, and proposes a casual model which describes the relationship between IUIPC and customer's decision to release or not personal information. • Develops a 10-tem scale of IUIPC which categorized as collection, control, and awareness. • Shows that 1) Internet users' information privacy concerns (IUIPC) have a negative effect on trusting beliefs, but a positive effect on risk beliefs; 2) trusting beliefs have a negative impact on risk beliefs; 3) intention is influenced positively by trusting beliefs, but negatively by risk beliefs; and 4) more sensitive information (the type of information) have a negative effect on trusting beliefs, a positive effect on risk beliefs, and a negative effect on intension. | <ul style="list-style-type: none"> • Information Systems | <ul style="list-style-type: none"> • Customer Perspective |
| <p>Milberg, Burke, Smith, and Kallman (1995)</p> | <ul style="list-style-type: none"> • Examines the relationships among nationality, cultural values, information privacy regulatory approaches, and the nature and level of information privacy concerns. • Shows that; 1) the level of personal information privacy concern varies across countries, but the relative importance or hierarchy of the dimensions (e.g., collection and secondary use) of those concerns does not; 2) cultural values do not influence the level of personal information privacy concern; 3) the amount of government involvement in information privacy regulation is affected by cultural values in the various countries; and 4) there are differences in privacy concerns associated with difference regulatory structures. | <ul style="list-style-type: none"> • Information Systems (Business) | <ul style="list-style-type: none"> • Government Perspective • Customer – Government Interaction • Customer Perspective |
| <p>Milberg, Smith, and Burke (2000)</p> | <ul style="list-style-type: none"> • Develops a conceptual framework that considers the dynamic interrelationships among key factors in information privacy (cultural values, individual privacy concerns, regulatory approaches, corporate privacy environment, and regulatory preferences) and tests it with a cross-cultural sample from 19 different countries. • Shows that; 1) cultural values are associated with differences in levels of consumer information privacy concerns and are associated marginally with differences in regulatory approaches; 2) privacy concerns have an effect on regulatory approaches; 3) regulatory approach has some effect on both corporate privacy environment and regulatory preferences; and 4) corporate privacy management environment affects privacy-related problems and regulatory preferences. | <ul style="list-style-type: none"> • Organization Science (Business) | <ul style="list-style-type: none"> • Government Perspective • Customer – Government Interaction • Customer Perspective |
| <p>Milne (2000)</p> | <ul style="list-style-type: none"> • Provides a research framework that illustrates four types of market and consumer | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Research |

| | | | |
|-------------------------|---|---|--|
| | <p>relationships that can occur due to consumer information privacy: (1) information requests and disclosures statements, (2) information provision and marketing contact, (3) information capturing without consent, and (4) information practices.</p> <ul style="list-style-type: none"> • Provides an overview of prior researches based on the research framework and discusses avenues for revenue research. | | Framework |
| Milne and Boza (1999) | <ul style="list-style-type: none"> • Examines the relationship between trust and concerns related to privacy, the antecedents and consequences of trust and concerns, and what consumers feel leads them to trust an organization with their personal information. • Shows that; 1) consumers' perceptions of trust and level of concern about privacy vary across industries; 2) trust is negatively related to privacy concerns and affected by several factors: age, gender, knowledge of information practices, attitude toward relationship marketing, incomes, and computer usage. • Argues that improving trust may be a more effective strategy than reducing privacy concerns. | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Customer Perspective |
| Milne and Culnan (2002) | <ul style="list-style-type: none"> • Examines the changes and trends of Web sites that voluntarily post privacy notices based on fair information principles from the 1998, 1999, 2000, and 2001 Web surveys. • Shows that; 1) the number of site posting privacy disclosure based on fair information practices statements is increased over time; 2) there is a significant increase on privacy notices about information collection, third-party disclosures, and choice; and 3) the most popular sites have posted more privacy disclosure than the random sample of sites across four years. | <ul style="list-style-type: none"> • Information Systems | <ul style="list-style-type: none"> • Company Perspective |
| Milne and Rohm (2000) | <ul style="list-style-type: none"> • Examines whether customers' awareness of data collection and knowledge of name removal mechanism influence their desire to remove their name from direct response lists across the mail, telephone, and e-mail channels. • Shows that; 1) name removal preferences are affected by customers' awareness of data collection and knowledge of name removal mechanism; 2) customers have different name removal preferences across channels (mail, telephone, and e-mail), and more likely to desire name removal from telephone lists than mail or e-mail lists; 3) customer's likelihood to desire name removal is influenced by individual factors such as computer use, income, age, and political philosophy; and 4) many customers are willing to consider alternative formats and notification schedules for controlling | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Customer Perspective |

| | | | |
|-----------------------------------|---|-----------------------|----------------------------------|
| | their personal information. | | |
| Miyazaki and Fernandez (2000) | <ul style="list-style-type: none"> Examines whether the prevalence of security and privacy disclosure relates to customer risk perceptions and purchase intention. Shows that; 1) the disclosure level varies across shopping categories; 2) there is no relation between the prevalence of privacy and security related disclosures and customer risk perceptions; but 3) the prevalence of privacy- and security-related disclosures are related to online purchase intention. | • Marketing | • Customer - Company Interaction |
| Miyazaki and Fernandez (2001) | <ul style="list-style-type: none"> Examines the relationships among the levels of Internet experience, perceived risks of conducting online purchasing, and online shopping activity. Shows that; 1) Internet experience and the adoption of remote purchase methods have a negative relation with both perceived risks and concerns regarding online purchasing; 2) the perceived risks of conducting online purchasing is associated with online purchasing activity; 3) security concerns toward online purchasing is related with online purchasing activity, but privacy concerns is not; and 4) Internet experience and the adoption of remote purchase method are related to online purchasing activity, and such relations are motivated by the perceived risks of conducting online purchasing | • Marketing | • Customer Perspective |
| Miyazaki and Krishnamurthy (2002) | <ul style="list-style-type: none"> Examines the relationship between participation in seal programs and the degree to which a firm's privacy reflects privacy standards and the influence of seals programs on customers' judgments of firms' privacy practices. Shows that; 1) there is no relationship between participation in seal programs and the privacy policy compliance with privacy standards; 2) the seal programs influence customer perception of favorableness toward Web site privacy policy; and 3) the seals affect the level of information disclosure and increase site patronage for high risk customers. | • Marketing | • Customer - Company Interaction |
| Moore and Dhillon (2003) | <ul style="list-style-type: none"> Examines privacy seals and discusses whether privacy seals work. Provides an overview of three major privacy seals and argues that legislation is needed to be enacted to define the basic principles of data privacy. | • Information Systems | • Company Perspective |
| Moore (2005) | <ul style="list-style-type: none"> Examines whether consumers care about privacy seals and whether privacy seals influence consumers' tendency to shop online. Shows that; 1) although participants have a basic understating about privacy seals | • Information Systems | • Customer - Company Interaction |

| | | | |
|-----------------------------------|---|-----------------------|----------------------------------|
| | and the function of seals, quite a number of them did not how a seal is obtained and failed to recognize genuine privacy seals, and 2) few participants consider privacy seals as important in deciding to trust a Web site. | | |
| Nowak and Phelps (1997) | <ul style="list-style-type: none"> • Explains privacy concerns that arise when the direct markers collect and use customer information by identifying the underlying dimensions of customer privacy concerns and the relation between those dimensions and marketer's information practices. | • Marketing | • Customer - Company Interaction |
| O'Neil (2001) | <ul style="list-style-type: none"> • Examines the relationship between concern about online privacy and four factors: sex, education level, income level, and race. • Shows that; 1) Whites and Asian/Pacifics Islanders have the lowest levels of concerns with privacy on the Internet, and Latinos and Hispanics have the highest level of concerns; 2) education level does not affect the level of concern about online privacy; 3) individuals with higher income levels are less concerned about privacy than those with lower income levels; 4) women have higher concerns about privacy than men have; and 5) all demographic groups prefer privacy protection to convenience. | • Social Science | • Customer Perspective |
| Palmer, Bailey, and Faraj (2000) | <ul style="list-style-type: none"> • Examines how firms use trusted third parties and privacy statements to build trust on their Web sites. • Shows that privacy statements and trusted third-party involvement can improve trust and that the history of firm has a negative effect on the use of privacy statements and trusted third parties. | • Information Systems | • Customer - Company Interaction |
| Phelps, Nowak, and Ferrell (2000) | <ul style="list-style-type: none"> • Examines the relationship between customers' information concerns and behaviour and factors related to customer privacy concerns. • Shows 1) several factors that correlate with customers' privacy concern (the type of personal information requested, consumers' ability and desire to control subsequent dissemination of personal information, consumers' perceptions regarding marketers' knowledge about them and their interests, consumers' attitude toward direct mail, consumers' preferences with respect to catalogue and advertising mail volume, and previous name removal request behaviour) and 2) the type of information companies' collect and the amount of information control have effect on customers' purchase intention. | • Marketing | • Customer Perspective |

| | | | |
|-----------------------------------|---|----------------------------|------------------------------------|
| Phelps, D'Souza, and Nowak (2001) | <ul style="list-style-type: none"> Examines the interrelationships between factors affecting customers' privacy concerns and their behaviour. Shows that customers' privacy concerns are influenced by attitude toward direct marketing and desire for control over personal information and finds that these privacy concerns, in turn, influence customers' purchase behaviour. | • Marketing | • Customer Perspective |
| Ranganathan and Ganapathy (2002) | <ul style="list-style-type: none"> Examines key underlying dimensions of B2C Web sites which are perceived by online consumers. Identifies four key dimensions of B2C web sites: information content, design, security, and privacy and shows that security and privacy have greater effect on the purchase intention of consumers. | • Information & Management | • Customer - Company Interaction |
| Reiter and Rubin (1999) | <ul style="list-style-type: none"> Explains a system called Crowds that makes browsing anonymous, so that allows users to access Websites without revealing so much personal information to Web servers and other parties. | • Information Systems | • Privacy and Technology |
| Rust, Kannan, and Peng (2002) | <ul style="list-style-type: none"> Examines the erosion of privacy on the Internet by using a simple economic model under the assumption that there is no government intervention and privacy is left to free-market forces. Shows that under such conditions, as time goes by, the amount of privacy will decline and customers will bear more expenses to maintain their privacy. | • Marketing | • Privacy and Economic Perspective |
| Schwaig, Kane, and Storey (2005) | <ul style="list-style-type: none"> Examines privacy policies of Fortune 500 and explains the actual role of privacy policies in Fortune 500 based on the four type of social action in Habermas' Theory of Communicative Action; communicative, instrumental, discursive, and strategic. Shows that; 1) organizations are not want to others to know whether they keep their privacy policies (communication); 2) companies limit their scope of privacy policies to reduce their liabilities (instrumental); 3) firms adhere to the principles embodied in the Fair Information Practices (discursive); and 4) companies, however, use the privacy policies as a strategic mechanism that conveys the positive public image without providing actual protection. | • Information Systems | • Company Perspective |
| Shankar, Urban, and Sultan (2002) | <ul style="list-style-type: none"> Proposes a stakeholder perspective on online privacy based on prior studies. Proposes a conceptual framework of online trust its antecedents (e.g., privacy, security, and feeling of control) and consequences (e.g., willingness to buy, satisfaction, and loyalty). | • Information Systems | • Customer Perspective |

| | | | |
|------------------------------|---|---|---|
| Sarathy and Robertson (2003) | <ul style="list-style-type: none"> • Develops a model of factors influencing privacy strategy which incorporates the environmental context, ethical perspectives and firm-specific considerations and provides a framework to help companies develop a strategy for handling digital privacy concerns. | <ul style="list-style-type: none"> • Business Ethics | <ul style="list-style-type: none"> • Company Perspective |
| Shapiro and Baker (2001) | <ul style="list-style-type: none"> • Explains how information privacy is socially constituted by a complex network of social institutions and practices and examines the conflict between information privacy and information technology (judicial, legislative, and private sector approaches in North American and Europe). | <ul style="list-style-type: none"> • Accounting | <ul style="list-style-type: none"> • Government Perspective |
| Sheehan (1999) | <ul style="list-style-type: none"> • Examines the role of gender in online privacy concerns and behaviour. • Shows that woman are more concerned than men about personal privacy, and men are more likely than women to change their behaviour to protect their privacy in the face of privacy concerns. | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Customer Perspective |
| Sheehan (2002) | <ul style="list-style-type: none"> • Examines whether online users privacy concerns fit well into Westin's typology. • Suggests that depending on the level of privacy concern, online users can be segmented into four distinct groups (unconcerned Internet users, circumspect Internet users, wary Internet users, and alarmed Internet users) and shows that online users' privacy concern is influenced by their age and their level of education. | <ul style="list-style-type: none"> • Information Systems | <ul style="list-style-type: none"> • Customer Perspective |
| Sheehan and Hoy (1999) | <ul style="list-style-type: none"> • Examines the relation between online users' privacy concerns and their behaviour • Shows that; 1) as privacy concern increased, online users are less likely to register for a Web site; 2) the level of privacy concern is not related to the frequency which users falsify information as well as the frequency with which they read unsolicited email; and 3) as privacy concern increased, online users are more likely to provide incomplete information, to notify Internet Service Providers (IPSS) about unsolicited email, to request their name removal from mailing lists, and to send negative message to those sending unsolicited email. | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Customer Perspective |
| Sheehan and Hoy (2000) | <ul style="list-style-type: none"> • Examines whether FTC's core principles of fair information practice reflect the underlying dimensions of customer's privacy concerns • Shows that many underlying dimensions of online customers' privacy concerns are addressed in FTC's core principles, but two facts that may influence consumer's privacy concerns are not reflected in the FTC's core principles: the relationships between entities and online users and the exchange of information for appropriate | <ul style="list-style-type: none"> • Marketing | <ul style="list-style-type: none"> • Customer – Government Interaction |

| | | | |
|--|---|--|---|
| | compensation. | | |
| Smith (2001) | <ul style="list-style-type: none"> Examines the differences in privacy approaches in the U.S. and Europe, identifies problems with the U.S. privacy approach (i.e., voluntary approach to address privacy concerns and secondary uses of personal information), and suggests some recommendations. | <ul style="list-style-type: none"> Business (Marketing) | <ul style="list-style-type: none"> Government Perspective |
| Smith, Milberg, and Burke (1996) | <ul style="list-style-type: none"> Develops and validates an instrument (15-item measure) that identifies and measures the primary dimension of individual's concerns about organizational information privacy practices. | <ul style="list-style-type: none"> Information Systems | <ul style="list-style-type: none"> Privacy Concern Instrument Customer Perspective |
| Stewart and Segars (2002) | <ul style="list-style-type: none"> Examines the factor structure of the concern for information privacy (CFIP) instrument posited by Smith et al. (1996). Shows that each dimension of the instrument is reliable and distinct and also suggests the use of a higher-order factor structure for CFIP instead of using a correlated set of first-order factors. | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Privacy Concern Instruments Customer Perspective |
| Swaminathan, Lepkowska-White, and Rao (1999) | <ul style="list-style-type: none"> Examines factors influencing online purchasing behaviour: vendor characteristics, perceived security, concern for privacy, and customer characteristics. Shows that; 1) customers' online purchasing behaviour is influenced by vendor characteristics such as the reliability of a vendor, the convenience of placing order and contacting vendor, and price competitiveness and access to information; 2) an average customer is not as concerned about the security or privacy, but customers who purchase frequently on the Internet are interested in creation of new law protecting privacy on the Internet; 3) customers who are primarily motivated by convenience are more likely to make purchases online; and 4) customers who value social interactions are less interested in the Internet use for shopping and shop less frequently on the Internet. | <ul style="list-style-type: none"> Marketing | <ul style="list-style-type: none"> Customer - Company Interaction |
| Vila, Greenstadt, and Molnar (2003) | <ul style="list-style-type: none"> Examines why there is not an efficient Web site privacy market even though people are concerned about their privacy. Argues privacy policies as signals in a lemon market, introduces a model for privacy in a lemon market, and explains previous trends in the Web site privacy market using the model. | <ul style="list-style-type: none"> Information System | <ul style="list-style-type: none"> Privacy and Economic Perspective |

| | | | |
|----------------------------|---|--|---|
| Wang, Lee, and Wang (1998) | <ul style="list-style-type: none">• Addresses the consumer's privacy perspective such as consumer privacy concerns, regulatory privacy protection, and privacy protection technologies. | <ul style="list-style-type: none">• Information System | <ul style="list-style-type: none">• Internet Privacy in General |
|----------------------------|---|--|---|

Appendix II: Internet Privacy User Survey Questionnaire

Internet Privacy User Survey Main Page

WEB-BASED SURVEY

Internet Privacy Survey

INFORMATION LETTER FOR INTERNET PRIVACY RESEARCH

Title of Research : The Effect of Internet Privacy on Customer Behaviour

Investigator : Won Gyun No
University of Waterloo, Department of Management Sciences
(519) 888-4567 Ext. 3422 wqno@engmail.uwaterloo.ca

This study is being conducted by Won Gyun No as part of his Ph.D. dissertation under the supervision of Dr. R. P. Sundarraj (Management Sciences) and Dr. Efrim Boritz (School of Accountancy) of the University of Waterloo. We are conducting research about the effect of internet privacy on individuals' behaviour. Several opinion polls reveal increasing levels of concern about privacy among Internet users. Such individuals' privacy concerns may influence their behaviour while they are conducting online transactions such as buying products from e-commerce sites. In response to these observations, we are asking for your participation in the study.

If you agree to participate in this study, you will be asked to complete a Web-based Internet privacy questionnaire. The questionnaire will ask general background questions and your opinions about privacy in e-commerce environment. Once you completed the questionnaire, you will be asked to visit a Web site and order a free gift from the site. **The free gift will be sent to you** as a token of appreciation for the time you have given to this study. You will also be eligible for **three draws of \$100 each**, at the end of the study. In addition, if you are MSci 211 student, you will receive one research participation credit.

Internet Privacy User Survey Consent Page

| WEB-BASED SURVEY | |
|---|---|
| <h2>Internet Privacy Survey</h2> | |
| Please provide following information. (If you have already participated in the survey, but you did not complete the survey. Please click HERE to continue.) | |
| The following information is required to create your survey ID and gift coupon. In addition, your student ID and name are recorded to make sure that no one responds more than once. Your email address is also recorded to send you a research report if you are interested in obtaining the results of this survey. | |
| Student ID | <input type="text"/> <input type="checkbox"/> Please check if you are MSci 211 student. |
| First Name | <input type="text"/> |
| Last Name | <input type="text"/> |
| Email | <input type="text"/> |
| <input type="checkbox"/> I agree to participate in a study being conducted by Won Gyun No of the Department of Management Sciences, University of Waterloo. I am also aware that I may withdraw from the study at any time without penalty. I have made this decision based on the information I have read in the 'Information Letter for Internet Privacy Research.' | |
| I also understand that this project has been reviewed by, and received ethics clearance through, the Office of Research Ethics at the University of Waterloo, and that I may contact this office if I have any concerns or comments resulting from my involvement in the study. | |
| Please indicate your birthday. | |
| YEAR | <input type="text" value="2006"/> MONTH <input type="text" value="10"/> DAY <input type="text" value="19"/> <input type="text" value="Thurs."/> |
| Providing your date of birth helps ensure that a person, not an automated program, has agreed to participate in this survey. However, your date of birth is not recorded. | |
| <input type="button" value="Previous"/> <input type="button" value="Continue"/> | |

Internet Privacy User Survey Page 1



Internet Privacy Survey



DEMOGRAPHIC
01 / 23 PAGE

What is your gender?

MALE FEMALE

What is your age?

Although this is a sensitive question, the answer can help the study to understand the needs of current Web users. It is not intended to offend, and completing this question is voluntary.

How would you classify yourself?

Which of the following income categories best describes your total current household income?

Privacy Survey Page 2



Internet Privacy Survey



DEMOGRAPHIC
02 / 23 PAGE

You are a _____.

First Year Second Year Third Year Fourth Year Graduate Student

Which of the following best describes the area you lived in most of your life?

How comfortable do you feel using the Internet?

| | | | | | | | | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
| Very Uncomfortable ◀ | <input type="radio"/> | ▶ Very Comfortable |

Internet Privacy User Survey Page 3

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

ONLINE TRANSACTION EXPERIENCE 03 / 23 PAGE

Online transactions refer to ordering things, subscribing to services or registering on Web sites for online services (e.g., free email).

How many times have you conducted online transactions in the past twelve months?

[Select]

How often did you experience any misuse personal information (e.g., unsolicited email, credit card fraud)?

| | | | | | | | | |
|---------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
| Never ◀ | <input type="radio"/> | ▶ Always |

How comfortable are you about your knowledge about protecting your personal information?

| | | | | | | | | |
|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
| Very Uncomfortable ◀ | <input type="radio"/> | ▶ Very Comfortable |

[Previous](#) [Next](#)

Internet Privacy User Survey Page 4

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

PRIVACY POLICY STATEMENT 04 / 23 PAGE

Often, Web sites post **privacy policy statement** that addresses particular information practices such as how companies use and protect personal information.

Have you ever seen the privacy policy statement attached to any Web site?

YES NO

[Previous](#) [Next](#)

If YES, go to Survey Page 5a.

If NO, go to Survey Page 5b.

Internet Privacy User Survey Page 5a

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

PRIVACY POLICY STATEMENT 05 / 23 PAGE

How many times have you read the privacy policy statement attached to any Web site in the past twelve months?

(Select) ▾

Previous Next

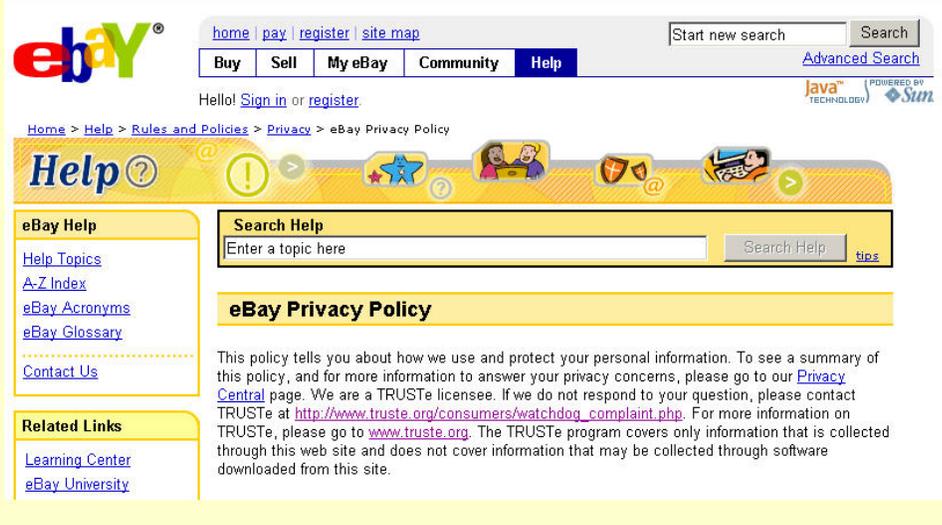
Internet Privacy User Survey Page 5b

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

PRIVACY POLICY STATEMENT 05 / 23 PAGE

Often, Web sites post privacy policy disclosures about particular information practices. Privacy policy refers to the set of implicit and explicit rules that determine whether and how companies collect, use, and transfer personal information. Such a policy is usually stated in the **Privacy Policy Statement**.

Privacy policy statement example (eBay):



Home > Help > Rules and Policies > Privacy > eBay Privacy Policy

eBay Help

- [Help Topics](#)
- [A-Z Index](#)
- [eBay Acronyms](#)
- [eBay Glossary](#)
- [Contact Us](#)

Related Links

- [Learning Center](#)
- [eBay University](#)

Search Help

Enter a topic here [tips](#)

eBay Privacy Policy

This policy tells you about how we use and protect your personal information. To see a summary of this policy, and for more information to answer your privacy concerns, please go to our [Privacy Central](#) page. We are a TRUSTe licensee. If we do not respond to your question, please contact TRUSTe at http://www.truste.org/consumers/watchdog_complaint.php. For more information on TRUSTe, please go to www.truste.org. The TRUSTe program covers only information that is collected through this web site and does not cover information that may be collected through software downloaded from this site.

Previous Next

University of Waterloo  **Internet Privacy Survey** *Department of Management Sciences* 

PRIVACY SEALS 06 / 23 PAGE

Several '**Seal of Approval Programs**' have been developed that license **privacy seals** to online companies whose information practices meet sealer's standards.

Have you ever seen the privacy seal attached to any Web site?

YES NO

[Previous](#) [Next](#)

If YES, go to Survey Page 7a.

If NO, go to Survey Page 7b.



Internet Privacy Survey

Department of Management Sciences


PRIVACY SEALS
07 / 23 PAGE

What privacy seal have you seen before? *(Please check all that apply.)*















Other

Previous
Next



Internet Privacy Survey

Department of Management Sciences


WHAT ARE PRIVACY SEALS?
07 / 23 PAGE

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site not only has implemented effective privacy practices, but is also abiding by those practices.

Privacy seals are developed to build consumer confidence regarding privacy by sending a signal to customers that companies' privacy practices comply with effective privacy practices.

Privacy seal examples:







Although several Internet seal programs exist in various forms, the majority of companies involved in such programs currently participate in one of three dominant programs: TRUSTe, BBBOnline, and WebTrust.

Previous
Next



Internet Privacy Survey



INTERNET PRIVACY AND INDUSTRY
08 / 23 PAGE

Would you say the following types of organizations are trustworthy or untrustworthy when it comes to the protection or use of your personal information?

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| <input type="radio"/> Financial organizations such as banks, investment companies, and credit unions | Highly Untrustworthy | <input type="radio"/> | Highly Trustworthy |
| <input type="radio"/> Health service providers, including doctors and hospitals | Highly Untrustworthy | <input type="radio"/> | Highly Trustworthy |
| <input type="radio"/> Government organizations | Highly Untrustworthy | <input type="radio"/> | Highly Trustworthy |
| <input type="radio"/> E-commerce companies selling products or providing online services over the internet | Highly Untrustworthy | <input type="radio"/> | Highly Trustworthy |
| <input type="radio"/> Privacy seal providers | Highly Untrustworthy | <input type="radio"/> | Highly Trustworthy |

[Previous](#) [Next](#)



Internet Privacy Survey



PERSONAL INFORMATION
09 / 23 PAGE

When providing your personal information to Web sites, what types of information do you feel reluctant to provide?
Please select the two types of information you are most reluctant to provide, and the two types of information you are least reluctant to provide.

Age

Date of Birth

Email Address

Gender

Occupation

SIN(Social Insurance Number)

Student ID

Two MOST Reluctant Information

Two LEAST Reluctant information

* To **ADD** or **REMOVE** a reluctant information, select personal information from the box and click the **LEFT** or **RIGHT ARROW BUTTON**.

[Previous](#) [Next](#)



Internet Privacy Survey



PERSONAL INFORMATION and ONLINE SHOPPING SITE

10 / 23 PAGE

Privacy policy statements contain particular information about Web sites' practices such as how companies collect, use, and transfer personal information.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

While surfing the Internet, you find **an online shopping site** for students that has some really interesting information.

It is sponsored by **a company you've never heard of**, but it seems to be very informative. You find a form on the site that **you can fill out to get a free gift** for one of the company's products. The form requires that you supply **your personal information**.



1 2 3 4 5 6 7

| | | | | | | | | | | |
|---|---------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------------|
| <p>1 How likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested?</p> | Very Unlikely | <input type="radio"/> | Very Likely |
| <p>2 If the Web site had a privacy policy statement, how likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested?</p> | Very Unlikely | <input type="radio"/> | Very Likely |
| <p>3 If the Web site had both a privacy policy statement and a privacy seal (e.g., TRUSTe), how likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested?</p> | Very Unlikely | <input type="radio"/> | Very Likely |

4 When the **online shopping site** asks you to provide *SIN(Social Insurance Number)* and *Student ID*, what would you like to know about its privacy practices?
Please select the two most important and the two least important privacy practices (i.e., policies).

- Accountability - Who is responsible for the site's policies and practices
- Collection Limitation - Collects only necessary information and obtains consent before the collection
- Data Quality - Makes sure that collected data is accurate, complete, and kept up-to-date
- Openness - Makes available to users specific information about the site's privacy policies and practices
- Participation - Allows users to challenge the accuracy of the information and have it amended
- Purpose - What information the site collects and what it is going to do with the information
- Security - Protects the information against unauthorized access and use
- Use Limitation - Uses the information only for purposes for which it was collected

Two MOST Important Privacy Practices

Two LEAST Important Privacy Practices

* To **ADD** or **REMOVE** privacy practices, select a privacy practice from the box and click the **UP** or **DOWN ARROW** **BUTTON**.

[Previous](#) [Next](#)



Internet Privacy Survey



PERSONAL INFORMATION and ONLINE BANKING SITE
11 / 23 PAGE

Privacy policy statements contain particular information about Web sites' practices such as how companies collect, use, and transfer personal information.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

While surfing the Internet, you find **an online banking site** that proposes a really interesting offer.

It **recently started its business**, but it seems to provide very good financial services. You find a credit card application form on the site that **you can fill out to get a premium interest rate as well as a free gift**. The form requires that you supply your **personal information**.



| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|

| | | | | | | | | | | |
|--|---------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------------|
| <input type="radio"/> How likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested? | Very Unlikely | <input type="radio"/> | Very Likely |
| <input type="radio"/> If the Web site had a privacy policy statement, how likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested? | Very Unlikely | <input type="radio"/> | Very Likely |
| <input type="radio"/> If the Web site had both a privacy policy statement and a privacy seal (e.g., TRUSTe), how likely would you be to complete this form when <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> are requested? | Very Unlikely | <input type="radio"/> | Very Likely |

When the **online banking site** asks you to provide *SIN(Social Insurance Number)* and *Student ID*, what would you like to know about its privacy practices?
Please select the two most important and the two least important privacy practices (i.e., policies).

- Accountability - Who is responsible for the site's policies and practices
- Collection Limitation - Collects only necessary information and obtains consent before the collection
- Data Quality - Makes sure that collected data is accurate, complete, and kept up-to-date
- Openness - Makes available to users specific information about the site's privacy policies and practices
- Participation - Allows users to challenge the accuracy of the information and have it amended
- Purpose - What information the site collects and what it is going to do with the information
- Security - Protects the information against unauthorized access and use
- Use Limitation - Uses the information only for purposes for which it was collected

Two MOST Important Privacy Practices

Two LEAST Important Privacy Practices

* To **ADD** or **REMOVE** privacy practices, select a privacy practice from the box and click the **UP** or **DOWN ARROW BUTTON**.

Previous
Next



Internet Privacy Survey



WILLINGNESS TO ENGAGE IN BEHAVIOURS
12 / 23 PAGE

Please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|-------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------|
| <input type="radio"/> It would be fun to be alone on a high mountain peak surveying the scene below. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I would be happy living all alone in a cabin in the woods. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I like to be home with nobody else around. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I like being in a room by myself. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I like to be the centre of attention in a group. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I like other people to notice me when I am in public. | Never | <input type="radio"/> | Usually |

[Previous](#) [Next](#)



Internet Privacy Survey



INTERACTING WITH PEOPLE
13 / 23 PAGE

Please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|-------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------|
| <input type="radio"/> I would be reluctant to engage in a prolonged conversation with someone I had just met. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> I like to meet new people. | Never | <input type="radio"/> | Usually |
| <input type="radio"/> Whenever possible, I avoid being in a crowd. | Never | <input type="radio"/> | Usually |

[Previous](#) [Next](#)



Internet Privacy Survey



MANAGING PERSONAL INFORMATION
14 / 23 PAGE

Below is a list of situations. Imagine yourself in each of the situations and then indicate how willing you would be to disclose information about yourself to the person(s).

I would be willing to discuss only certain topics, and on a superficial level only, if at all, in this situation.

I would be willing to express, in complete detail, personal information about myself in such a way the other person(s) truly understand(s) where I stand in terms of my feelings and thoughts regarding any topic.

(1) ←

→ (7)

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| <input type="radio"/> You are sightseeing with a tour group in Europe. | <input type="radio"/> |
| <input type="radio"/> You are sitting next to a stranger on an airplane. | <input type="radio"/> |
| <input type="radio"/> You are at a party with some friends. | <input type="radio"/> |
| <input type="radio"/> You are eating alone and a stranger asks if he or she may join you. | <input type="radio"/> |
| <input type="radio"/> You and a friend are driving to Vancouver. | <input type="radio"/> |
| <input type="radio"/> You are on a picnic with friends. | <input type="radio"/> |

Previous
Next



Internet Privacy Survey



PROVIDING PERSONAL INFORMATION
15 / 23 PAGE

When you perform online transactions, online companies ask you to provide information about yourself – including your name, phone number, and SIN(Social Insurance Number).

Please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|----------------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-------------------------|
| I am able to keep e-commerce sites from collecting personal information about myself that I would like to keep secret. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |
| I determine the types of information that e-commerce sites can store about me. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |
| I am satisfied that I am able to keep e-commerce sites from collecting personal information about me that I want to keep from them. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |
| I am satisfied in my ability to determine the types of personal information that e-commerce sites collect on me. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |

Previous
Next



Internet Privacy Survey



CONCERN ABOUT PROVIDING PERSONAL INFORMATION

16 / 23 PAGE

Information about oneself can be categorized into anonymous information, unidentifiable information, and identifiable information.

- **Anonymous information** is the information collected automatically but cannot be used to identify you (e.g., your computer, network information, operating system, etc).
- **Unidentifiable information** is the information that you have voluntarily given out but cannot be used to identify you (e.g., zip code, age-range, sex, etc).
- **Identifiable information** is the information that you have voluntarily given out and can be used to identify you as an individual (e.g., name, shipping address, credit card or bank account information, social insurance number, etc).

Please indicate your level of agreement with the following statements.

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|-------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------|
| <input type="radio"/> I am sensitive about giving out information regarding my preferences. | Strongly Disagree | <input type="radio"/> | Strongly Agree |
| <input type="radio"/> I am concerned about <u>anonymous information</u> that is collected about me. | Strongly Disagree | <input type="radio"/> | Strongly Agree |
| <input type="radio"/> I am concerned about how my personally <u>unidentifiable information</u> will be used by the e-commerce site. | Strongly Disagree | <input type="radio"/> | Strongly Agree |
| <input type="radio"/> I am concerned about how my personally <u>identifiable information</u> will be used by the e-commerce site. | Strongly Disagree | <input type="radio"/> | Strongly Agree |
| <input type="radio"/> When it comes to information you consider personal, how concerned are you about privacy? | Never | <input type="radio"/> | Always |

[Previous](#) [Next](#)



Internet Privacy Survey



PRIVACY IN E-COMMERCE
17 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

Two privacy practices are:

- Purpose* - What information the site collects and what it is going to do with the information and
- Security* - Protects the information against unauthorized access and use.

When **a Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|-------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|----------------|
|  I would read the privacy policy statement of the Web site when it requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Strongly Disagree | <input type="radio"/> | Strongly Agree |
|  During the past 6 months, did you read the privacy policy statement of the Web site when it requested your <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> ? | Never | <input type="radio"/> | Usually |
|  I would provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above. | Strongly Disagree | <input type="radio"/> | Strongly Agree |
|  During the past 6 months, did you provide your <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above? | Never | <input type="radio"/> | Usually |

Previous Next



Internet Privacy Survey



PRIVACY IN E-COMMERCE
18 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**.
Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| 1 For me, when a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , reading its privacy policy statement is _____ | Extremely Unimportant | <input type="radio"/> | Extremely Important |
| 2 People who give me good advice would encourage me to read privacy policy statement whenever I provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Definitely False | <input type="radio"/> | Definitely True |
| 3 I intend to read the privacy policy statement of a Web site when it requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Extremely Unlikely | <input type="radio"/> | Extremely Likely |
| 4 When a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , whether or not I read its privacy policy statement is completely up to me. | Definitely False | <input type="radio"/> | Definitely True |

[Previous](#) [Next](#)



Internet Privacy Survey



PRIVACY IN E-COMMERCE
19 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**. **Privacy seals** are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| 1 I will make an effort to read a Web site's privacy policy statement when it requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Extremely Unlikely ◀ | <input type="radio"/> | ▶ Extremely Likely |
| 2 When a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , I am confident that if I wanted to, I could read its privacy policy statement. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |
| 3 Reading the privacy policy statement of a Web site when it requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> is an idea I _____ . | Extremely Dislike ◀ | <input type="radio"/> | ▶ Extremely Like |
| 4 People who influence my behaviour would think I should read the privacy policy statement whenever I provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Definitely False ◀ | <input type="radio"/> | ▶ Definitely True |

[Previous](#) [Next](#)



Internet Privacy Survey



PRIVACY IN E-COMMERCE
20 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| 1 When a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , I have the knowledge and the ability to read its privacy policy statement. | Definitely False | <input type="radio"/> | Definitely True |
| 2 People who are important to me think that I should read the privacy policy statement whenever I provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> . | Extremely Unlikely | <input type="radio"/> | Extremely Likely |
| 3 When a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , I plan to read its privacy policy statement. | Extremely Unlikely | <input type="radio"/> | Extremely Likely |
| 4 When a Web site requests my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> , reading its privacy policy statement is _____. | Extremely Unimportant | <input type="radio"/> | Extremely Important |

Previous
Next



Internet Privacy Survey



PRIVACY IN E-COMMERCE

21 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**. **Privacy seals** are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

Two privacy practices are:

- *Purpose* - What information the site collects and what it is going to do with the information and
- *Security* - Protects the information against unauthorized access and use.

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| <p>1 For me, if the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above, providing my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> is _____.</p> | Extremely Bad ◀ | <input type="radio"/> | ▶ Extremely Good |
| <p>2 When the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above, whether or not to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> is entirely within my control.</p> | Definitely False ◀ | <input type="radio"/> | ▶ Definitely True |
| <p>3 I intend to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above.</p> | Extremely Unlikely ◀ | <input type="radio"/> | ▶ Extremely Likely |
| <p>4 People whose opinions I value would encourage me to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above.</p> | Definitely False ◀ | <input type="radio"/> | ▶ Definitely True |

[Previous](#) [Next](#)



Internet Privacy Survey



PRIVACY IN E-COMMERCE
22 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

Two privacy practices are:

- Purpose* - *What information the site collects and what it is going to do with the information* and
- Security* - *Protects the information against unauthorized access and use.*

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|---|----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|--------------------|
| ● People who are close to me think that I should provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> if the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above. | Extremely Unlikely ◀ | <input type="radio"/> | ▶ Extremely Likely |
| ● I am going to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above. | Extremely Unlikely ◀ | <input type="radio"/> | ▶ Extremely Likely |
| ● Providing my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above is an idea I _____. | Extremely Dislike ◀ | <input type="radio"/> | ▶ Extremely Like |
| ● I have complete control over whether or not to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> if the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above. | Definitely False ◀ | <input type="radio"/> | ▶ Definitely True |

Previous
Next



Internet Privacy Survey



PRIVACY IN E-COMMERCE
23 / 23 PAGE

A **privacy policy** refers to the set of practices that determine whether and how a Web site collects, uses, and transfers personal information. Such a policy is usually stated in the **privacy policy statement**.

Privacy seals are third-party enforcement programs that award an identifiable symbol to express that the Web site's information practices meet program standards.

Two privacy practices are:

- *Purpose* - What information the site collects and what it is going to do with the information and
- *Security* - Protects the information against unauthorized access and use.

When a **Web site has a privacy seal**, please indicate your level of agreement with the following statements.

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|--|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|------------------|
| 1 I plan to provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT address <i>Purpose</i> and <i>Security</i> as defined above. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |
| 2 If the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above, providing my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> is _____ . | Extremely Bad ◀ | <input type="radio"/> | ▶ Extremely Good |
| 3 People who influence my behaviour would think I should provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> if the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above. | Definitely False ◀ | <input type="radio"/> | ▶ Extremely True |
| 4 It is completely up to me whether or not I provide my <i>SIN(Social Insurance Number)</i> and <i>Student ID</i> when the Web site's privacy policy does NOT state <i>Purpose</i> and <i>Security</i> as defined above. | Strongly Disagree ◀ | <input type="radio"/> | ▶ Strongly Agree |

Previous
Next



Internet Privacy Survey



INTERNET PRIVACY SURVEY

Thank you for your submission.

Please write down the following gift card number.

Your gift card number is **uw87817**

Please press the continue button below to redeem a free gift from Gift4U.

Once you complete your order, you will be return to the survey.

[CONTINUE](#)

Please note that Gift4U is not part of the Internet privacy survey site and the responsibility for using Gift4U rests with you.

Appendix III: Online Experimental Site

Online Experimental Site Main Page

The screenshot shows the Gift4U website interface. At the top, the logo "Gift4U" is displayed with the tagline "YOUR CHOICE... It's Fast. It's Fun. It's FREE!". Below the logo, a banner reads "Order Your Free Gift at Gift4U". The main content area is titled "Music" and features a sidebar with "CATEGORIES" including Books, Gift Tickets, and Music. Three music items are listed:

- 1. Most Relaxing Classical Album**
In stock
Regular Price: \$14.99
Our Price: FREE with GIFT CARD
Add to cart
- 2. Let It Be [Soundtrack]**
In stock
Regular Price: \$14.99
Our Price: FREE with GIFT CARD
Add to cart
- 3. Trumpet: Greatest Hits**
In stock
Regular Price: \$14.99
Our Price: FREE with GIFT CARD
Add to cart

Additional elements include a "FREE shipping!" icon, a "PRIVACY VALIDATED TRUSTWEB" badge, and a footer with navigation links: Home | About Us | Privacy Policy | Contact Us. The copyright notice at the bottom reads "Copyright © 2006 Gift4U All Rights Reserved."

Product Information Page



Let It Be [Soundtrack]
 Producer: Phil Spector BACK

CATEGORIES

- ▶ Books
- ▶ Gift Tickets
- ▶ Music

FREE shipping!





[See large image](#)

Regular Price: ~~\$14.99~~

Our Price: **FREE with GIFT CARD**

Availability: Usually ships within 15 days. Ships from Gift4U.

Description: The Beatles: Paul McCartney (vocals, guitar, piano, bass instrument); John Lennon, George Harrison (vocals, guitar); Ringo Starr (drums). Additional personnel: Billy Preston (keyboards). Generally regarded as the Beatles' last album, LET IT BE was actually recorded in 1969, before the recording and release of ABBEY ROAD.

[Add to cart](#)

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U All Rights Reserved.

Shopping Cart Page



Shopping Cart BACK

| Shopping Cart Items--To Buy Now | Quantity | Price |
|---|----------|----------------------------|
| Item added on 2006-10-19 21:30 Let It Be [Soundtrack] Producer: Phil Spector Free shipping! | 1 | FREE with GIFT CARD |

[Proceed to Checkout](#)

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U All Rights Reserved.

Checkout Page



YOUR CHOICE...
It's Fast. It's Fun. It's FREE!



Order Your Free Gift at Gift4U



SIGN IN SHIPPING INFORMATION ADDITIONAL INFORMATION COMPLETE ORDER **BACK**

Ordering from Gift4U is quick and easy

Enter Your Gift Card Number: (If you forgot your gift card number, click [HERE.](#))

The secure server will encrypt your information.
You are ordering this item from Gift4U.

[▶ Sign in using our secure server](#)

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U All Rights Reserved.

Shipping Address Page



YOUR CHOICE...
It's Fast. It's Fun. It's FREE!

Order Your Free Gift at Gift4U





[SIGN IN](#) [SHIPPING INFORMATION](#) [ADDITIONAL INFORMATION](#) [COMPLETE ORDER](#)

[Privacy Policy](#)



Enter the shipping address for this order

Please enter a shipping address for this order. When finished, click the "Continue" button.

First Name:

Last Name:

Street Address:

City:

Province:

Postal Code:

Phone Number:

[BACK](#) [Continue](#)

Address Accuracy

Make sure you get your stuff! If the address is not entered correctly, your package may be returned as undeliverable. You would then have to place a new order. Save time and avoid frustration by entering the address information in the appropriate boxes and double-checking for typos and other errors.

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U All Rights Reserved.

Additional Information Page



Gift4U *YOUR CHOICE...*
It's fast. It's fun. It's FREE!

Order Your Free Gift at Gift4U





[SIGN IN](#) [SHIPPING INFORMATION](#) [ADDITIONAL INFORMATION](#) [COMPLETE ORDER](#)

[Privacy Policy](#)



Enter the additional information

Please enter additional information. When finished, click the "Continue" button.

Which Web browser do you usually use? (Click [HERE](#) for more information.)

Internet Explorer Mozilla/Netscape Firefox Opera
 Safari Lynx/Text Don't know Other

Please enter your Social Insurance Number to enter three draws for \$100 each. (Click [HERE](#) for more information.)

If you have, or plan to purchase goods on the Internet, what kinds of goods would you be most interested in? (Please check all that apply.) (Click [HERE](#) for more information.)

Computers Equipment Software/Video Games Books/Music CDs/DVD
 Consumer Electronics Travel (Hotel, Air, etc) Ticket (Concert, Sport, etc)
 I never purchase goods on the Internet.

What is your student ID? (Click [HERE](#) for more information.)

Would you like to be added to the mailing list and receive information about any FREE gift offers?

YES NO

[BACK](#)[Continue](#) 

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U All Rights Reserved.

Complete Order Page



YOUR CHOICE...
It's fast. It's fun. It's FREE!

Order Your Free Gift at Gift4U





[SIGN IN](#) [SHIPPING INFORMATION](#) [ADDITIONAL INFORMATION](#) [COMPLETE ORDER](#) [BACK](#)

Please review and complete your order.

Important Notice for Internet Privacy Survey Participants!

Please click [HERE](#) to COMPLETE your order and to ENTER a draw of three additional \$100 prizes.

Items:

 **Let It Be [Soundtrack]**
Regular Price: ~~\$14.99~~
Our Price: **FREE with GIFT CARD**

Shipping to:

Harry Collin
50 Mooregate Crescent
Kitchener, Ontario N2M5G6

[Home](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#)

Copyright © 2006 Gift4U. All Rights Reserved.

Giff4U Privacy Policy

Thank you for visiting this website and reviewing privacy policy.



- [Accountability - Who is responsible for this site's policies and practices?](#)
- [Collection Limitation - Does this site collect only necessary information and obtains consent before the collection?](#)
- [Data Quality - Does this site make sure that collected data is accurate, complete, and kept up-to-date?](#)
- [Openness - Does this site make available to you specific information about its privacy policies and practices?](#)
- [Participation - Does this site allow you to challenge the accuracy of the information and have it amended?](#)
- [Use Limitation - Does this site use the information only for purposes for which it was collected?](#)

Accountability - Who is responsible for this site's policies and practices?

[Go to Top](#)

We are responsible for all personal information under our control, including any personal information that is transferred to third parties for processing, storage or other purposes. We have a person, Won Gyun No, who is accountable for compliance with these privacy and security principles.

Collection Limitation - Does this site collect only necessary information and obtains consent before the collection?

[Go to Top](#)

We collect only the information required to process your order. If we require your personal information for other reasons, we will ask your consent before or at the time the information is collected.

Data Quality - Does this site make sure that collected data is accurate, complete, and kept up-to-date?

[Go to Top](#)

We keep your personal information up to date, accurate and relevant for its intended use. You may request access to the personal information we have on record in order to review and amend the information, as appropriate.

Openness - Does this site make available to you specific information about its privacy policies and practices?

[Go to Top](#)

We provide you with understandable and easily available information about our policy and practices related to management of your personal information. This policy and any related information is available at all times on this site, under Privacy Policy or on request. You can contact us by email to wgno@engmail.uwaterloo.ca or phone at (519)888-4567 x3422.

Participation - Does this site allow you to challenge the accuracy of the information and have it amended?

[Go to Top](#)

You can request access or change to your personal information. You can contact us by email to wgno@engmail.uwaterloo.ca or phone at (519)888-4567 x3422. Upon receiving your request, we will provide you with access to your information so you can review and verify the accuracy and completeness and request changes to the information and also make any necessary updates to your personal information.

Use Limitation - Does this site use the information only for purposes for which it was collected?

[Go to Top](#)

We use and disclose your personal information only for the purposes it was collected. We do not sell or share personal information to any organization or person for any reason.



Verified

Gift4U

Validated Privacy Statement

For www.Gift4U.ca

License Agreement Version 6.1

Gift4U is a certified licensee of the TrustWeb Privacy Seal Program. The privacy statement and practices of www.Gift4U.ca have been reviewed by TrustWeb for compliance with our strict program requirements.

Make Informed Choices for Your Personal Information

Appendix IV: Debriefing Questionnaire

Debriefing Page 1

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

DEBRIEFING 1 / 5 PAGE

1 How satisfied are you with your experience with Giff4U Web site?

| | | | | | | | | |
|---------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|------------------|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
| Very Dissatisfied ◀ | <input type="radio"/> | ▶ Very Satisfied |

2 Did Giff4U Web site collect your personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*)?

YES NO

3 Did you read the privacy policy of Giff4U?

YES NO

Next

If Q2 is YES, go to Debriefing Page 2. If NO, go to Debriefing Page 4.

Debriefing Page 2

The screenshot shows the 'Debriefing' section of the 'Internet Privacy Survey' on page 2 of 5. The header includes the University of Waterloo logo and the Department of Management Sciences. The question asks: 'Did you know why Gift4U asked for your personal information (e.g., SIN(Social Insurance Number) and Student ID)?'. There are two radio button options: 'YES' and 'NO'. Navigation buttons for 'Previous' and 'Next' are located at the bottom right.

If YES, go to Debriefing Page 2a. If NO, go to Debriefing Page 3.

Debriefing Page 2a

The screenshot shows the 'Debriefing' section of the 'Internet Privacy Survey' on page 2 of 5. The question asks: 'What are the reasons that Gift4U Web site collected your personal information (e.g., SIN(Social Insurance Number) and Student ID)?'. Below the question is a large, empty text input field with a vertical scrollbar on the right side. Navigation buttons for 'Previous' and 'Next' are located at the bottom right.

Debriefing Page 3

The screenshot shows the 'Debriefing' section of the 'Internet Privacy Survey' on page 3 of 5. The question asks: 'Did you question Gift4U's need for your personal information (e.g., SIN(Social Insurance Number) and Student ID)?'. There are two radio button options: 'YES' and 'NO'. Navigation buttons for 'Previous' and 'Next' are located at the bottom right.

If YES, go to Debriefing Page 3a. If NO, go to Debriefing Page 4.

Debriefing Page 3a

University of Waterloo
Internet Privacy Survey Department of Management Sciences

DEBRIEFING 3 / 5 PAGE

What led you to question Gift4U's need for your personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*)?

Previous Next

Debriefing Page 3b

University of Waterloo
Internet Privacy Survey Department of Management Sciences

DEBRIEFING 3 / 5 PAGE

Did you provide your personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*) even though you questioned Gift4U's need for your information?

YES NO

Previous Next

If YES, go to Debriefing Page 3c. If NO, go to Debriefing Page 4.

Debriefing Page 3c

University of Waterloo
Internet Privacy Survey Department of Management Sciences

DEBRIEFING 3 / 5 PAGE

What are the reasons that you provided (or did not provide) your personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*).

Previous Next

Debriefing Page 4

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

DEBRIEFING 4 / 5 PAGE

Did Gift4U have a privacy seal on its Web site?

YES NO

Previous Next

If YES, go to Debriefing Page 4a. If NO, go to Debriefing Page 5.

Debriefing Page 4a

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

DEBRIEFING 4 / 5 PAGE

Which privacy seal did you see on Gift4U site?















Other

Previous Next



Internet Privacy Survey



DEBRIEFING
5 / 5 PAGE

Please indicate your level of **AGREEMENT**.

NOTE:

Make each item a separate and independent judgment. Work at fairly high speed through this questionnaire. Do not worry or puzzle over individual items. It is your first impressions, the immediate feelings about the items, that we want. On the other hand, please do not be careless, because we want your true impressions.

While I was providing personal information (e.g., *SIN(Social Insurance Number)* and *Student ID*) at Gift4U, to me privacy was

| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | |
|-----------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|---------------------|
| Important ◀ | <input type="radio"/> | ▶ Unimportant |
| Relevant ◀ | <input type="radio"/> | ▶ Irrelevant |
| Means nothing ◀ | <input type="radio"/> | ▶ Means a lot to me |
| Involving ◀ | <input type="radio"/> | ▶ Uninvolving |
| Not needed ◀ | <input type="radio"/> | ▶ Needed |

Previous
Next

Debriefing Consent Page

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

INTERNET PRIVACY SURVEY

Thank you for your participation in Internet privacy survey.

We appreciate your participation in our study, and thank you for spending the time helping us with our research. Since the study was more complicated than what we explained to you at the start, we could not give you complete information about the study at that time, because it may have influenced your behaviour during the study. We apologize for this omission, and hope that you understand the need for it once the purpose of the study has been fully explained to you.

We are interested in how individuals react when they are asked to provide sensitive or less sensitive personal information on a Web site as well as how the existence of privacy policy statement and privacy seal influences an individual's behaviour. When you redeemed a gift from the Gift4U, you were

During the debriefing session, I was given an explanation as to why it was necessary for the researchers to disguise the real purpose of this study. I was informed that having full information about the actual purpose of the study might have influenced the way in which I responded to the tasks and this would have invalidated the results. Thus, to ensure that this did not happen, some of the details about the purpose of the study initially were not provided. However, I have now received a complete written explanation as to the actual purpose of the study. In addition, I have had an opportunity to ask any questions about this and to receive acceptable answers to my questions. I give permission for the researchers to use information I provided in their study, and agree to this request. I am aware that I may withdraw this consent by notifying the Principal Investigator of this decision.

I am aware that I may contact Dr. Susan Sykes, Director of the Office of Research Ethics at 519-888-4567 ext. 6005 or by email at ssykes@uwaterloo.ca if I have any concerns or comments resulting from my involvement in this study.

Please check if you are interested in obtaining the results of this survey.
The result will be sent to you by email before December 31, 2006.

If you have any general comments or questions related to this study, please contact Won Gyun No at 519-888-4567 ext. 3422 or by email at wgn0@engmail.uwaterloo.ca.

We would like to assure you that this study has been reviewed by, and received ethics clearance through, the Office of Research Ethics. If you have any concerns regarding your participation in this study, please contact Dr. Susan Sykes, Director, Office of Research Ethics at ssykes@uwaterloo.ca or (519) 888-4567 Ext. 6005.

Debriefing End Page

University of Waterloo **Internet Privacy Survey** Department of Management Sciences

INTERNET PRIVACY SURVEY

Appendix V: List of 420 Web Sites

United States

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|---|----------------------|--|----------------------------|
| Albertsons, Inc. | www.albertsons.com | Aetna Inc. (New) | www.aetna.com |
| Alcoa, Inc. | www.alcoa.com | Allstate Corp. (The) (United States) | www.allstate.com |
| Altria Group Inc | www.philipmorris.com | American Express Co. (United States) | www.americanexpress.com |
| Boeing Co. (The) | www.boeing.com | American International Group Inc | www.aig.com |
| Darden Restaurants, Inc. (United States) | www.darden.com | Aon Corp. (United States) | www.aon.com |
| Delphi Corp. (United States) | www.delphi.com | Bank of America Corp. (United States) | www.bankofamerica.com |
| Disney (Walt) Co. (The) | www.disney.com | CIGNA Corp. | www.cigna.com |
| Electronic Data Systems Corp. (New) (United States) | www.eds.com | Citigroup Global Markets Holdings Inc | www.salomonsmithbarney.com |
| FedEx Corp | www.fedex.com | Citigroup Inc | www.citigroup.com |
| Ford Motor Co. (DE) | www.ford.com | Countrywide Financial Corp | www.countrywide.com |
| General Electric Co. (United States) | www.ge.com | Fidelity National Financial, Inc. | www.fnf.com |
| General Motors Corp | www.gm.com | First American Corp (The) | www.firstam.com |
| Hewlett-Packard Co. (DE) (United States) | www.hp.com | General Motors Acceptance Corp | www.gmacfs.com |
| Home Depot, Inc. (United States) | www.homedepot.com | Hartford Financial Services Group Inc. (United States) | www.thehartford.com |
| International Business Machines Corp. | www.ibm.com | HCA, Inc. | www.hcahealthcare.com |
| Kmart Holding Corp | www.bluelight.com | HealthSouth Corp. | www.healthsouth.com |
| Kroger Co. | www.kroger.com | JPMorgan Chase & Co. | www.jpmorganchase.com |
| Marriott International, Inc. (New) | www.marriott.com | Kindred Healthcare Inc | www.kindredhealthcare.com |
| McDonald Corp (United States) | www.mcdonalds.com | Liberty Mutual Insurance Co. (Boston) | www.libertymutual.com |

| | | | |
|---|--|--|--|
| Northrop Grumman Corp | www.northropgrumman.com | MBNA Corp. | www.mbna.com |
| Penney (J.C.) Co.,Inc. (Holding Co.) | www.jcpenney.net | Merrill Lynch & Co Inc | www.ml.com |
| PepsiCo Inc. | www.pepsico.com | Metlife Inc | www.metlife.com |
| Pfizer Inc (United States) | www.pfizer.com | Morgan Stanley | www.morganstanley.com |
| Safeway Inc. (United States) | www.safeway.com | National City Bank (Cleveland, OH) | www.national-city.com |
| Sara Lee Corp. | www.saralee.com | Prudential Financial, Inc. (United States) | www.prudential.com |
| SBC Communications, Inc. | www.sbc.com | Quest Diagnostics, Inc. | www.questdiagnostics.com |
| Sears, Roebuck & Co. | www.sears.com | Res-Care, Inc. | www.rescare.com |
| Target Corp | www.targetcorp.com | SunTrust Banks, Inc. | www.suntrust.com |
| The Gap, Inc. | www.gapinc.com | Tenet Healthcare Corp. (United States) | www.tenethealth.com |
| United Parcel Service, Inc. (United States) | www.ups.com | U.S. Bancorp (DE) | www.usbank.com |
| United Technologies Corp. | www.utc.com | UnitedHealth Group Inc | www.unitedhealthgroup.com |
| Verizon Communications Inc (United States) | www.verizon.com | Universal Corp. | www.universalcorp.com |
| Viacom Inc | www.viacom.com | Wachovia Corp (New) | www.wachovia.com |
| Walgreen Co. | www.walgreens.com | Washington Mutual Inc. (United States) | www.wamu.com |
| Wal-Mart Stores, Inc. | www.wal-mart.com | Wells Fargo & Co. (New) | www.wellsfargo.com |

Canada

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|--|--|--|--|
| Ace Aviation Holdings Inc | www.aircanada.ca | AGF Management Ltd | www.agf.com |
| Alcan Inc. (Canada) | www.alcan.com | Amica Mature Lifestyles Inc./ Style de Vie Amica Inc. | www.amica.ca |
| Aliant, Inc. (Canada) | www.aliant.ca | B2B Trust (Canada) | www.b2b-trust.com |
| Atco Ltd. (Canada) | www.atco.com | Bank of Canada (Ottawa) | www.bankofcanada.ca |
| Bell Canada (Canada) | www.bell.ca | Bank of Montreal (Canada) | www.bmo.com |
| Bombardier Inc. | www.bombardier.com | Bank of Nova Scotia (Toronto, Canada) | www.scotiabank.com |
| Brascan Corp | www.brascan.com | Boardwalk Real Estate Investment Trust | www.bwalk.com |
| Canadian National Railway Co. (Canada) | www.cn.ca | Business Development Bank of Canada | www.bdc.ca |
| Canadian Pacific Railway Ltd. | www.cpr.ca | Caisse de Depot et Placement du Quebec (Canada) | www.cdpcapital.com |
| Canadian Tire Corp., Ltd | www.canadiantire.ca | Canadian Hotel Income Properties Real Estate Investment Trust (Canada) | www.chipreit.com |
| CanWest Global Communications Corp. (Canada) | www.canwestglobal.com | Canadian Imperial Bank of Commerce | www.cibc.com |
| Celestica, Inc. | www.celestica.com | Canadian Western Bank (Canada) | www.cwbank.com |
| CGI Group, Inc. (Canada) | www.cgi.com | Co-Operators General Insurance Co. (Canada) | www.cooperators.ca |
| Fairmont Hotels & Resorts, Inc. (Canada) | www.fairmont.com | Datawest Solution Inc (Canada) | www.datawestsolutions.com ; www.datawest.ca |
| FirstService Corp. | www.firstservice.com | Desjardins Financial Security Life Assurance Co. (Canada) | www.desjardinsfinancialsecurity.com |
| Forzani Group Ltd. (Canada) | www.forzanigroup.com | Desjardins Group | www.desjardins.com |
| Four Seasons Hotels Inc. (Canada) | www.fourseasons.com | Dundee Wealth Management Inc | www.dundeewealth.com |
| Hudsons Bay Co. (Canada) | www.hbc.ca | Export Development Canada | www.edc.ca |
| Intier Automotive Inc. | www.intier.com | Farm Credit Canada | www.fcc-fac.ca |

| | | | |
|--|--|--|--|
| Loblaw Cos. Ltd. | www.loblaw.com | IGM Financial Inc | www.investorsgroup.com |
| Magna International Inc. (Canada) | www.magna.com | Industrial Alliance Insurance and Financial Services Inc | www.inalco.com |
| Metro Inc | www.metro.ca | ING Insurance Company of Canada | www.ingcanada.com |
| Nortel Networks Corp (Holding Co.) | www.nortelnetworks.com | Laurentian Bank of Canada | www.laurentianbank.com |
| Onex Corp. | www.onex.com | Manulife Century (Canada) | www.manulife.ca |
| Precision Drilling Corp. (Canada) | www.precisiondrilling.com | MDS Inc. (Canada) | www.mdsintl.com |
| Rogers Communications Inc. (Canada) | www.rogers.com | Med-Emerg International, Inc. (Canada) | www.med-emerg.com |
| RONA, Inc. (Canada) | www.rona.ca | National Bank of Canada | www.nbc.ca |
| Royal Group Technologies Ltd. (Canada) | www.royalgrouptech.com | Newalta Income Fund | www.newalta.com |
| Sears Canada Inc. | www.sears.ca | Oppenheimer Holdings Inc | www.opco.com |
| Teck Cominco Ltd. | www.teckcominco.com | Royal Bank of Canada (Montreal, Quebec) | www.rbc.com |
| TELUS Corp. (Canada) (New) | www.telus.com | Sun Life Assurance Company of Canada | www.sunlife.ca |
| Tembec, Inc. (Canada) | www.tembec.com | TLC Vision Corp (Canada) | www.tlcvision.com |
| Thomson Corp. | www.thomson.com | Toronto Dominion Bank | www.td.com |
| Transcontinental Inc | www.transcontinental.com | Trizec Properties, Inc | www.trz.com |
| Weston (George) Limited | www.weston.ca | Vancouver City Savings Credit Union (Canada) | www.vancity.com |

United Kingdom

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|---|--------------------------|---|--------------------------|
| AMEC Plc (United Kingdom) | www.amec.com | AMEC Plc (United Kingdom) | www.amec.com |
| Associated British Foods Plc (United Kingdom) | www.abf.co.uk | Associated British Foods Plc (United Kingdom) | www.abf.co.uk |
| AstraZeneca Plc (United Kingdom) | www.astrazeneca.com | AstraZeneca Plc (United Kingdom) | www.astrazeneca.com |
| BHP Billiton Plc (United Kingdom) | www.bhpbilliton.com | BHP Billiton Plc (United Kingdom) | www.bhpbilliton.com |
| BOC Group Plc (United Kingdom) | www.boc.com | BOC Group Plc (United Kingdom) | www.boc.com |
| BP p.l.c. (United Kingdom) | www.bp.com | BP p.l.c. (United Kingdom) | www.bp.com |
| British Airways Plc | www.britishairways.com | British Airways Plc | www.britishairways.com |
| BT Group Plc (United Kingdom) | www.btplc.com | BT Group Plc (United Kingdom) | www.btplc.com |
| Cadbury Schweppes PLC (United Kingdom) | www.cadburyschweppes.com | Cadbury Schweppes PLC (United Kingdom) | www.cadburyschweppes.com |
| Compass Group PLC (United Kingdom) | www.compass-group.com | Compass Group PLC (United Kingdom) | www.compass-group.com |
| Consignia Holdings Plc (United Kingdom) | www.consignia.com | Consignia Holdings Plc (United Kingdom) | www.consignia.com |
| Diageo Plc (United Kingdom) | www.diageo.com | Diageo Plc (United Kingdom) | www.diageo.com |
| Exel PLC (New) (United Kingdom) | www.exel.com | Exel PLC (New) (United Kingdom) | www.exel.com |
| FirstGroup Plc (United Kingdom) | www.firstgroup.com | FirstGroup Plc (United Kingdom) | www.firstgroup.com |
| GKN Plc | www.gknplc.com | GKN Plc | www.gknplc.com |
| GlaxoSmithKline Plc (United Kingdom) | www.gsk.com | GlaxoSmithKline Plc (United Kingdom) | www.gsk.com |
| GUS Plc (United Kingdom) | www.gusplc.com | GUS Plc (United Kingdom) | www.gusplc.com |
| Hilton Group Plc (United Kingdom) | www.hiltongroup.com | Hilton Group Plc (United Kingdom) | www.hiltongroup.com |
| Intercontinental Hotels Group Plc | www.ichotelsgroup.com | Intercontinental Hotels Group Plc | www.ichotelsgroup.com |
| Invensys Plc (United Kingdom) | www.invensys.com | Invensys Plc (United Kingdom) | www.invensys.com |
| J. Sainsbury PLC | www.sainsbury.co.uk | J. Sainsbury PLC | www.sainsbury.co.uk |
| Lewis (John) Partnership Plc (United Kingdom) | www.johnlewis.co.uk | Lewis (John) Partnership Plc (United Kingdom) | www.johnlewis.co.uk |

| | | | |
|---|--|---|--|
| Kingdom) | | Kingdom) | |
| Marks & Spencer Group PLC | www.marksandspencer.com | Marks & Spencer Group PLC | www.marksandspencer.com |
| Mitchells & Butlers Plc | www.mbplc.com | Mitchells & Butlers Plc | www.mbplc.com |
| National Express Group Plc (United Kingdom) | www.nationalexpressgroup.com | National Express Group Plc (United Kingdom) | www.nationalexpressgroup.com |
| Reed Elsevier Plc (New) (United Kingdom) | www.reedelsevier.com | Reed Elsevier Plc (New) (United Kingdom) | www.reedelsevier.com |
| Rentokil Initial Plc (United Kingdom) | www.rentokil-initial.com | Rentokil Initial Plc (United Kingdom) | www.rentokil-initial.com |
| Rio Tinto Plc (United Kingdom) | www.riotinto.com | Rio Tinto Plc (United Kingdom) | www.riotinto.com |
| Rolls Royce Group Plc | www.rolls-royce.com | Rolls Royce Group Plc | www.rolls-royce.com |
| Stagecoach Group Plc. (United Kingdom) | www.stagecoachgroup.com | Stagecoach Group Plc. (United Kingdom) | www.stagecoachgroup.com |
| Tesco PLC (United Kingdom) | www.tesco.com | Tesco PLC (United Kingdom) | www.tesco.com |
| Tomkins Plc (United Kingdom) | www.tomkins.co.uk | Tomkins Plc (United Kingdom) | www.tomkins.co.uk |
| Unilever Plc (United Kingdom) | www.unilever.com | Unilever Plc (United Kingdom) | www.unilever.com |
| Vodafone Group Plc (New) (United Kingdom) | www.vodafone.com | Vodafone Group Plc (New) (United Kingdom) | www.vodafone.com |
| WPP Group Plc (United Kingdom) | www.wpp.com | WPP Group Plc (United Kingdom) | www.wpp.com |

Germany

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|---|-------------------------|---|-------------------------|
| Adam Opel AG (Germany, Fed. Rep.) | www.opel.de | Adam Opel AG (Germany, Fed. Rep.) | www.opel.de |
| AUDI AG (Germany, Fed. Rep.) | www.audi.com | AUDI AG (Germany, Fed. Rep.) | www.audi.com |
| BASF AG (Germany) | www.basf.com | BASF AG (Germany) | www.basf.com |
| Bayer AG (Germany) | www.bayer.com | Bayer AG (Germany) | www.bayer.com |
| Bayerische Motoren Werke AG (BMW) (Germany) | www.bmwgroup.com | Bayerische Motoren Werke AG (BMW) (Germany) | www.bmwgroup.com |
| Bertelsmann AG (Germany, Fed. Rep.) | www.bertelsmann.com | Bertelsmann AG (Germany, Fed. Rep.) | www.bertelsmann.com |
| Bilfinger & Berger AG (Germany, Fed. Rep.) | www.bilfingerberger.com | Bilfinger & Berger AG (Germany, Fed. Rep.) | www.bilfingerberger.com |
| Bosch (Robert) GmbH (Germany Fed. Rep.) | www.bosch.com | Bosch (Robert) GmbH (Germany Fed. Rep.) | www.bosch.com |
| Continental AG (Germany, Fed. Rep.) | www.conti-online.com | Continental AG (Germany, Fed. Rep.) | www.conti-online.com |
| DaimlerChrysler AG (Germany) | www.daimlerchrysler.com | DaimlerChrysler AG (Germany) | www.daimlerchrysler.com |
| Degussa Ag Neu Duesseldorf Glarus (Germany) | www.degussa.com | Degussa Ag Neu Duesseldorf Glarus (Germany) | www.degussa.com |
| Deutsche Bahn AG | www.bahn.de | Deutsche Bahn AG | www.bahn.de |
| Deutsche Lufthansa AG (Germany, Fed. Rep.) | www.lufthansa.com | Deutsche Lufthansa AG (Germany, Fed. Rep.) | www.lufthansa.com |
| Deutsche Post AG (Germany) | www.dpwn.de | Deutsche Post AG (Germany) | www.dpwn.de |
| Deutsche Telekom AG (Germany) | www.telekom.de | Deutsche Telekom AG (Germany) | www.telekom.de |
| E.ON AG (Germany) | www.eon.com | E.ON AG (Germany) | www.eon.com |
| E.ON Energie AG (Germany) | www.eon-energie.com | E.ON Energie AG (Germany) | www.eon-energie.com |
| Ford-Werke AG (Germany, Fed. Rep.) | www.ford.de | Ford-Werke AG (Germany, Fed. Rep.) | www.ford.de |
| Franz Haniel & Cie. GmbH (Germany, Fed. Rep.) | www.haniel.com | Franz Haniel & Cie. GmbH (Germany, Fed. Rep.) | www.haniel.com |
| Fresenius AG (Germany) | www.fresenius-ag.com | Fresenius AG (Germany) | www.fresenius-ag.com |

| | | | |
|--|--|--|--|
| Fresenius Medical Care AG (Germany) | www.fmc-ag.com | Fresenius Medical Care AG (Germany) | www.finc-ag.com |
| Henkel KGAA (Germany, Fed. Rep.) | www.henkel.com | Henkel KGAA (Germany, Fed. Rep.) | www.henkel.com |
| Hochtief AG (Germany) | www.hochtief.de | Hochtief AG (Germany) | www.hochtief.de |
| MAN Aktiengesellschaft (Germany, Fed. Rep.) | www.man-group.com | MAN Aktiengesellschaft (Germany, Fed. Rep.) | www.man-group.com |
| Metro AG (Germany) | www.metrogroup.de | Metro AG (Germany) | www.metrogroup.de |
| Osram GmbH (Germany, Fed. Rep.) | www.osram.de | Osram GmbH (Germany, Fed. Rep.) | www.osram.de |
| Otto Versand (GmbH & Co.) (Germany, Fed. Rep.) | www.otto.de | Otto Versand (GmbH & Co.) (Germany, Fed. Rep.) | www.otto.de |
| RAG AG (Germany, Fed. Rep.) | www.rag-coalinter.de | RAG AG (Germany, Fed. Rep.) | www.rag-coalinter.de |
| RWE AG (Germany) | www.rwe.com | RWE AG (Germany) | www.rwe.com |
| Siemens AG (Germany) | www.siemens.com | Siemens AG (Germany) | www.siemens.com |
| Thyssen Industrie AG (Germany, Fed. Rep.) | www.thyssenkruppindustries.com | Thyssen Industrie AG (Germany, Fed. Rep.) | www.thyssenkruppindustries.com |
| Thyssen Krupp Steel AG (Germany) | www.thyssen-krupp-steel.com | Thyssen Krupp Steel AG (Germany) | www.thyssen-krupp-steel.com |
| TUI Ag (Germany) | www.tui.com | TUI Ag (Germany) | www.tui.com |
| Volkswagen A.G. (Germany, Fed. Rep.) | www.volkswagen-ir.de | Volkswagen A.G. (Germany, Fed. Rep.) | www.volkswagen-ir.de |
| ZF Friedrichshafen AG (Germany) | www.zf.com | ZF Friedrichshafen AG (Germany) | www.zf.com |

Japan

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|---|------------------------------|---|------------------------------|
| Aeon Co. Ltd. (Japan) | www.aeon.info | Aeon Co. Ltd. (Japan) | www.aeon.info |
| Aisin Seiki Co., Ltd. (Japan) | www.aisin.co.jp | Aisin Seiki Co., Ltd. (Japan) | www.aisin.co.jp |
| Asahi Glass Co., Ltd. (Japan) | www.agc.co.jp | Asahi Glass Co., Ltd. (Japan) | www.agc.co.jp |
| Bridgestone Corp. (Japan) | www.bridgestone.co.jp | Bridgestone Corp. (Japan) | www.bridgestone.co.jp |
| Canon, Inc. (Japan) | www.canon.co.jp | Canon, Inc. (Japan) | www.canon.co.jp |
| Denso Corp. (Japan) | www.denso.co.jp | Denso Corp. (Japan) | www.denso.co.jp |
| East Japan Railway Co. (Japan) | www.jreast.co.jp | East Japan Railway Co. (Japan) | www.jreast.co.jp |
| Fuji Photo Film Co., Ltd. (Japan) | www.fujifilm.co.jp | Fuji Photo Film Co., Ltd. (Japan) | www.fujifilm.co.jp |
| Fujitsu Ltd. | www.fujitsu.com | Fujitsu Ltd. | www.fujitsu.com |
| Hitachi, Ltd. (Japan) | www.hitachi.co.jp | Hitachi, Ltd. (Japan) | www.hitachi.co.jp |
| Honda Motor Co., Ltd.(Honda Giken Kogyo Kabushiki Kaisha) (Japan) | www.honda.co.jp | Honda Motor Co., Ltd.(Honda Giken Kogyo Kabushiki Kaisha) (Japan) | www.honda.co.jp |
| Ito-Yokado Co., Ltd. (Japan) | www.itoyokado.iyg.co.jp | Ito-Yokado Co., Ltd. (Japan) | www.itoyokado.iyg.co.jp |
| Japan Airlines Corp | www.jal.co.jp | Japan Airlines Corp | www.jal.co.jp |
| Kyocera Corp. (Japan) | www.kyocera.co.jp | Kyocera Corp. (Japan) | www.kyocera.co.jp |
| Matsushita Electric Industrial Co., Ltd. (Japan) | www.matsushita.co.jp | Matsushita Electric Industrial Co., Ltd. (Japan) | www.matsushita.co.jp |
| Matsushita Electric Works, Ltd. (Japan) | www.mew.co.jp | Matsushita Electric Works, Ltd. (Japan) | www.mew.co.jp |
| Mitsubishi Corp. (Japan) | www.mitsubishi.co.jp | Mitsubishi Corp. (Japan) | www.mitsubishi.co.jp |
| Mitsubishi Electric Corp. | www.MitsubishiElectric.co.jp | Mitsubishi Electric Corp. | www.MitsubishiElectric.co.jp |
| Mitsubishi Heavy Industries Ltd. (Japan) | www.mhi.co.jp | Mitsubishi Heavy Industries Ltd. (Japan) | www.mhi.co.jp |
| Mitsumi Electric Co., Ltd. (Japan) | www.mitsumi.co.jp | Mitsumi Electric Co., Ltd. (Japan) | www.mitsumi.co.jp |
| NEC Corp | www.nec.co.jp | NEC Corp | www.nec.co.jp |
| Nippon Express Co., Ltd. | www.nittsu.co.jp | Nippon Express Co., Ltd. | www.nittsu.co.jp |
| Nippon Steel Corp. (Japan) | www.nsc.co.jp | Nippon Steel Corp. (Japan) | www.nsc.co.jp |

| | | | |
|--|--|--|--|
| Nippon Telegraph & Telephone Corp. (Japan) | www.ntt.co.jp | Nippon Telegraph & Telephone Corp. (Japan) | www.ntt.co.jp |
| Nissan Motor Co., Ltd. (Japan) | www.nissan.co.jp | Nissan Motor Co., Ltd. (Japan) | www.nissan.co.jp |
| Ricoh Co., Ltd. (Japan) | www.ricoh.co.jp | Ricoh Co., Ltd. (Japan) | www.ricoh.co.jp |
| Sanyo Electric Co., Ltd. (Japan) | www.sanyo.co.jp | Sanyo Electric Co., Ltd. (Japan) | www.sanyo.co.jp |
| Sharp Corp. (Japan) | www.sharp.co.jp | Sharp Corp. (Japan) | www.sharp.co.jp |
| Sony Corp (Japan) | www.sony.co.jp | Sony Corp (Japan) | www.sony.co.jp |
| Sumitomo Electric Industries, Ltd. (Japan) | www.sei.co.jp | Sumitomo Electric Industries, Ltd. (Japan) | www.sei.co.jp |
| Tokyo Electric Power Co. Inc. (The Japan) | www.tepco.co.jp | Tokyo Electric Power Co. Inc. (The Japan) | www.tepco.co.jp |
| Toshiba Corp. (Japan) | www.toshiba.co.jp | Toshiba Corp. (Japan) | www.toshiba.co.jp |
| Toyota Motor Corp. (Japan) | www.toyota.co.jp | Toyota Motor Corp. (Japan) | www.toyota.co.jp |
| West Japan Railway Co (Japan) | www.westjr.co.jp | West Japan Railway Co (Japan) | www.westjr.co.jp |
| Yamato Transport Co., Ltd. (Japan) | www.kuronekoyamato.co.jp | Yamato Transport Co., Ltd. (Japan) | www.kuronekoyamato.co.jp |

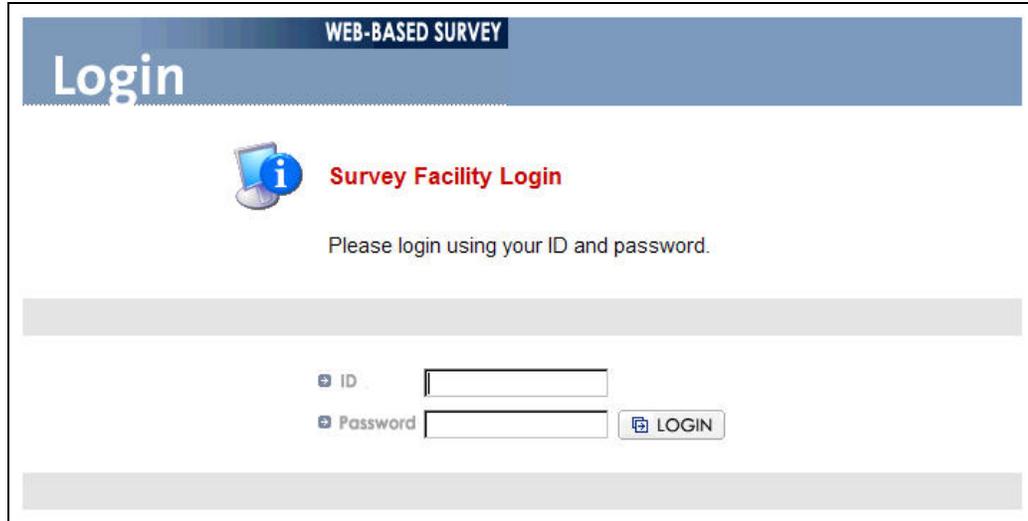
China

| Less Information-sensitive Industries | | Information-sensitive Industries | |
|--|--|--|--|
| 3M China | www.3m.com/intl/cn | 3M China | www.3m.com/intl/cn |
| Anhui Quanchai Engine Co Ltd | www.quanchai.com.cn | Anhui Quanchai Engine Co Ltd | www.quanchai.com.cn |
| Beijing Capital International Airport Co. Ltd | www.bcia.com.cn | Beijing Capital International Airport Co. Ltd | www.bcia.com.cn |
| Changsha Zoomlion Heavy Industry Science & Technology Development Co Ltd | www.zljt.com | Changsha Zoomlion Heavy Industry Science & Technology Development Co Ltd | www.zljt.com |
| Chengdu Xuguang Electronics Co. Ltd. | www.xuguang.com | Chengdu Xuguang Electronics Co. Ltd. | www.xuguang.com |
| China Eastern Airlines Corp., Ltd. | www.ce-air.com | China Eastern Airlines Corp., Ltd. | www.ce-air.com |
| Dongfeng Automobile Co Ltd | www.dfac.com | Dongfeng Automobile Co Ltd | www.dfac.com |
| GRACE Semiconductor Manufacturing Co. | www.gsmethw.com | GRACE Semiconductor Manufacturing Co. | www.gsmethw.com |
| Guangdong Goworld Co Ltd | www.gd-goworld.com | Guangdong Goworld Co Ltd | www.gd-goworld.com |
| Huaneng Power International, Inc. | www.hpi.com.cn | Huaneng Power International, Inc. | www.hpi.com.cn |
| Huawei Technologies Co Ltd | www.huawei.com | Huawei Technologies Co Ltd | www.huawei.com |
| Hunan Haili Chemical Industry Co Ltd | www.hnhlc.com | Hunan Haili Chemical Industry Co Ltd | www.hnhlc.com |
| Hunan TianYi Science & Technology Co Ltd | www.china-tianyi-pump.com | Hunan TianYi Science & Technology Co Ltd | www.china-tianyi-pump.com |
| Jiangsu Sihuan Bioengineering Co Ltd | www.shsw.com.cn | Jiangsu Sihuan Bioengineering Co Ltd | www.shsw.com.cn |
| Jilin Yatai (Group) Co Ltd | www.yatai.com | Jilin Yatai (Group) Co Ltd | www.yatai.com |
| Kweichow Moutai Co., Ltd. | www.moutaichina.com | Kweichow Moutai Co., Ltd. | www.moutaichina.com |
| Lenovo Group Ltd | www.lenovo.cn | Lenovo Group Ltd | www.lenovo.cn |
| Liaoning SG Automotive Group Co., Ltd. | www.sgautomotive.com | Liaoning SG Automotive Group Co., Ltd. | www.sgautomotive.com |
| PetroChina Co Ltd (China) | www.petrochina.com.cn | PetroChina Co Ltd (China) | www.petrochina.com.cn |
| Qingdao Aucma Co. Ltd. | www.aucma.com.cn | Qingdao Aucma Co. Ltd. | www.aucma.com.cn |

| | | | |
|---|-------------------------|---|-------------------------|
| Shanghai 3F New Material Co., Ltd. | www.sh3f.com | Shanghai 3F New Material Co., Ltd. | www.sh3f.com |
| Shanghai Feilo Co., Ltd. | www.feilo.com.cn | Shanghai Feilo Co., Ltd. | www.feilo.com.cn |
| Shanghai Jinjiang International Hotels Development Co Ltd | www.jinjianghotels.com | Shanghai Jinjiang International Hotels Development Co Ltd | www.jinjianghotels.com |
| Shanghai Online | www.online.sh.cn | Shanghai Online | www.online.sh.cn |
| Shanghai Yuansheng Biology Manufacturing Co. | www.yuanshengsh.com | Shanghai Yuansheng Biology Manufacturing Co. | www.yuanshengsh.com |
| Shenzhen Expressway Co., Ltd. | www.sz-expressway.com | Shenzhen Expressway Co., Ltd. | www.sz-expressway.com |
| Sichuan Hushan Electronic Co., Ltd. | www.china-hushan.com | Sichuan Hushan Electronic Co., Ltd. | www.china-hushan.com |
| Sinopec Yizheng Chemical Fibre Co., Ltd. | www.ycfc.com | Sinopec Yizheng Chemical Fibre Co., Ltd. | www.ycfc.com |
| Sinotex Investment & Development Co Ltd | www.sinotex-ctrc.com.cn | Sinotex Investment & Development Co Ltd | www.sinotex-ctrc.com.cn |
| Sinotrans Air Transportation Development Co Ltd | www.sinoair.com | Sinotrans Air Transportation Development Co Ltd | www.sinoair.com |
| Tibet Tianlu Communications Co. Ltd. | www.xztianlu.com | Tibet Tianlu Communications Co. Ltd. | www.xztianlu.com |
| Tongwei Co., Ltd. | www.tongwei.com.cn | Tongwei Co., Ltd. | www.tongwei.com.cn |
| Yunnan Yuntian Hua Co Ltd | www.yyth.com.cn | Yunnan Yuntian Hua Co Ltd | www.yyth.com.cn |
| Yuxi Hongta Tobacco (Group) Co., LTD. | www.hongta.com | Yuxi Hongta Tobacco (Group) Co., LTD. | www.hongta.com |
| Zte Corp, | www.zte.com.cn | Zte Corp, | www.zte.com.cn |

Appendix VI: Privacy Policy Disclosure Survey

Login Page



The screenshot shows a login page for a "WEB-BASED SURVEY". The page has a blue header with the word "Login" in white. Below the header, there is a blue information icon (a lowercase 'i' inside a circle) next to the text "Survey Facility Login". Underneath, it says "Please login using your ID and password." There are two input fields: one for "ID" and one for "Password". To the right of the "Password" field is a button labeled "LOGIN" with a small icon of a person.

WEB-BASED SURVEY

Login

 **Survey Facility Login**

Please login using your ID and password.

ID

Password

Phase I - Web Site Survey

Web Site Survey Main Page

University of Waterloo

DEPARTMENT OF MANAGEMENT SCIENCES

Web-based Survey

HELLO! USA1 What can I do for you? [Log out](#)

STAGE I

[Web Site Survey](#) *Here, you can start the survey of assigned domains.*

STAGE II

[Privacy Policy Survey](#) *Here, you can start the survey of assigned privacy policies.*



**University of
Waterloo**



**DEPARTMENT OF
MANAGEMENT SCIENCES**

SURVEY MANAGEMENT TOOL

Web-based Survey

Company List

| No. | Company Name | Survey |
|-----|--|--------------------------------------|
| 1 | Aetna Inc. (New) | DONE |
| 2 | Albertsons, Inc. | DONE |
| 3 | Alcoa, Inc. | DONE |
| 4 | Allstate Corp. (The) (United States) | DONE |
| 5 | Altria Group Inc | DONE |
| 6 | American Express Co. (United States) | DONE |
| 7 | American International Group Inc | <input type="button" value="START"/> |
| 8 | Aon Corp. (United States) | DONE |
| 9 | Bank of America Corp. (United States) | DONE |
| 10 | Bank of New York Co., Inc. | <input type="button" value="START"/> |
| ⋮ | ⋮ | ⋮ |
| 95 | Viacom Inc | DONE |
| 96 | Wachovia Corp (New) | DONE |
| 97 | Walgreen Co. | <input type="button" value="START"/> |
| 98 | Wal-Mart Stores, Inc. | <input type="button" value="START"/> |
| 99 | Washington Mutual Inc. (United States) | DONE |
| 100 | Wells Fargo & Co. (New) | DONE |

Web Site Survey Company Information Page

| | |
|--|---|
|    SURVEY Web-based Survey | |
| General Information | |
| Read general instructions and the definition of privacy disclosure carefully. | |
| Check the below information before start survey. | |
| Surfer's ID : | USA1 |
| Date : | 2007-04-13 |
| Domain Name : | General Electric Co. (United States) |
| Domain ID : | USA_008 |
| URL : | www.ge.com |
| GENERAL INSTRUCTIONS | |
| <ol style="list-style-type: none">1. Your role in the survey is to determine whether your assigned domains post disclosures about the collection and use of online users' personal information. We refer to these disclosures as "Privacy Policies."2. Surf the domain for a maximum of 10 minutes, looking for a Privacy Seal and Privacy Policy. Be sure to stay within the assigned domain as you move from Web page to Web page.3. If you have any questions, or if you are uncertain at any point as to what you should do, <i>consult a proctor.</i> | |
| "Privacy Disclosure" | |
| <input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Close"/> | |

Web Site Survey Page 1

| | |
|--|--|
|   DEPARTMENT OF MANAGEMENT SCIENCES | |
| SURVEY MANAGEMENT TOOL Web-based Survey | |
| ACCESS 1 / 6 | INSTRUCTION Select YES or NO for the question. |
| Are you able to ACCESS the domain's Web site (URL)? | Note: "Domain" A domain is the aggregation of all Web pages, sites, and servers using a particular domain name, defined as the word of letters immediately preceding the ".com". For example, the site "www.yahoo.com," the page "www.yahoo.com/news/index.asp," and "www.yahoo.com/sports" would all be included in the domain "www.yahoo.com." In this survey, we define "Web site" as a domain. |
| <input type="radio"/> YES <input type="radio"/> NO | |
| Previous Next Close | |

If YES, go to Web Site Survey Page 2.

If NO, Web Site Survey End Page.

Web Site Survey Page 2

| | |
|--|---|
|   DEPARTMENT OF MANAGEMENT SCIENCES | |
| SURVEY MANAGEMENT TOOL Web-based Survey | |
| PRIVACY SEAL 2 / 6 | INSTRUCTION Select YES or NO for the question. |
| Is a PRIVACY SEAL posted on the domain? | If a PRIVACY SEAL is posted, SELECT the seal from the dropdown box. If you select " Other ", WRITE the name of the seal in the text box. |
| <input type="radio"/> YES <input type="radio"/> NO | PLACES TO LOOK FOR PRIVACY SEALS AND PRIVACY POLICIES |
| Previous Next Close | |

Web Site Survey Page 3

| | |
|--|--|
|   DEPARTMENT OF MANAGEMENT SCIENCES | |
| Web-based Survey | |
| PRIVACY POLICY 3 / 6 | INSTRUCTION Select YES or NO for the question. |
| Is a PRIVACY POLICY posted on this domain? | If YES, PRINT the entire Privacy Policy, WRITE the domain's ID Number on it, and PLACE it in domain's the folder. If you cannot print the Privacy Policy, ASK a proctor for assistance. |
| <input type="radio"/> YES <input type="radio"/> NO | Note: Increasingly, online companies are posting descriptions of their information practices. In this survey, we refer to these |
| Previous Next Close | |

Web Site Survey Page 4

| | |
|--|---|
|   DEPARTMENT OF MANAGEMENT SCIENCES | |
| Web-based Survey | |
| PRIVACY LINK 4 / 6 | INSTRUCTION Select YES or NO for the question. |
| Is there a LINK to the Privacy Policy on this domain's HOME PAGE? | Search the home page for an icon or highlighted text that allows a domain visitor to click to the Privacy Policy. Be sure to scroll all the way down to the bottom of the home page. Look for highlighted terms such as "Privacy Policy," "Privacy Statement," "Privacy," "Fair Information Practices," "Security," "Online Privacy Practices," or "Our Policies." |
| <input type="radio"/> YES <input type="radio"/> NO | |
| Previous Next Close | |



DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL

Web-based Survey

| COOKIE | 5 / 6 |
|--|---|
| Does the domain place COOKIE? | INSTRUCTION Select YES or NO for both questions. |
| <input type="radio"/> YES <input type="radio"/> NO | <ol style="list-style-type: none">1. Open the "Internet Explorer."2. Go to "Tools" → "Internet Options."3. Click "Delete cookies" and Click "OK."_____4. Click "Privacy" tab.5. Click "Advance."6. Check "Override Automatic Cookie Handling."7. Check "Prompt" under <i>First-parties Cookies</i> and Check "Prompt" under <i>Third-parties Cookies</i>8. Click "OK."_____9. Enter the assigned domain's URL in your browser.10. Check for the domain shown in the first cookie alert that appears. |
| Is a THIRD PARTY (i.e., any domain OTHER THAN the domain you are currently visiting) attempting to place a cookie at this domain? | |
| <input type="radio"/> YES <input type="radio"/> NO | |

Previous Next Close

Web Site Survey Page 6

University of Waterloo

DEPARTMENT OF MANAGEMENT SCIENCES

SURVEY Web-based Survey

PRIVACY BIRD 6 / 6

Which ICON does the AT&T "PRIVACY BIRD" show?

- GREEN BIRD
- RED BIRD
- YELLOW BIRD

INSTRUCTION

Select ONE of three choices for the question.

Note: When the AT&T Privacy Bird is disabled, the grey sleeping bird icon will appear.

1. Click on the bird icon and select "Enable Privacy Bird".
2. Enter the assigned domain's URL in your browser.
3. Look at the AT&T "Privacy Bird" icon in the top right of your browser's title bar.
4. Select one.

Previous Next Close

Web Site Survey End Page

University of Waterloo

DEPARTMENT OF MANAGEMENT SCIENCES

SURVEY Web-based Survey

Company Web Site Survey

Thank you for your submission.

Click "**Company List**" go to next assignment company.

Click "**Survey Main**" go to the survey main page.

Survey Main Company List Close

Phase II - Company Privacy Policy Survey

Company Privacy Policy Survey Main Page

University of Waterloo

DEPARTMENT OF MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL

Web-based Survey

Hello! USA1 What can I do for you? [Log out](#)

STAGE I

- [Web Site Survey](#) *Here, you can start the survey of assigned domains.*

STAGE II

- [Privacy Policy Survey](#) *Here, you can start the survey of assigned privacy policies.*
- [Privacy Policy Survey Finalization](#) *Here, you can reconcile your answers with your partner.*





Web-based Survey

Company List

| No. | Company Name | Survey |
|-----|--|--------------------------------------|
| 1 | Aetna Inc. (New) | DONE |
| 2 | Albertsons, Inc. | DONE |
| 3 | Alcoa, Inc. | DONE |
| 4 | Allstate Corp. (The) (United States) | <input type="button" value="START"/> |
| 5 | Altria Group Inc | DONE |
| 6 | American Express Co. (United States) | DONE |
| 7 | American International Group Inc | <input type="button" value="START"/> |
| 8 | Aon Corp. (United States) | DONE |
| 9 | Bank of America Corp. (United States) | <input type="button" value="START"/> |
| 10 | Boeing Co. (The) | DONE |
| ⋮ | ⋮ | ⋮ |
| 65 | Viacom Inc | <input type="button" value="START"/> |
| 66 | Wachovia Corp (New) | DONE |
| 67 | Walgreen Co. | DONE |
| 68 | Wal-Mart Stores, Inc. | DONE |
| 69 | Washington Mutual Inc. (United States) | DONE |
| 70 | Wells Fargo & Co. (New) | DONE |

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

General Information

Read **general instructions** carefully and the definition of key terms.

Check the below information before start survey.

| | |
|---------------|--------------------------------------|
| Surfer's ID : | USA1 |
| Date : | 2007-04-13 |
| Domain Name : | General Electric Co. (United States) |
| Domain ID : | USA_008 |
| URL : | www.ge.com |

GENERAL INSTRUCTIONS

1. Your role in the survey is to answer questions about the content of the **privacy policies** of the assigned domains.
2. You should answer the questions based on a **careful reading of all the privacy policy disclosures** in your folder.
3. You must work **independently** at this stage.

DEFINITION OF KEY TERMS

1. "Privacy Disclosure"
Privacy disclosures refer to any statement on a domain regarding that domain's privacy practices i.e., what information they collect, what they do with it, and how they treat it. Privacy disclosures include "fair information practices" and "privacy policies." A privacy policy is a detailed, specified description of

Previous Next Close

University of Waterloo DEPARTMENT OF MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

DATA COLLECTION 1 / 50

Does the Privacy Policy contain a declaration that the domain does **NOT** collect any personal information from consumers?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find an **express** statement that the domain does **NOT** collect any personal information from consumers.

Example:

- We do not collect any information about you when you visit our site.

Previous Next Close

If YES, go to Company Privacy Policy Survey Page 46.

If NO, go to Company Privacy Policy Survey Page 2.

University of Waterloo DEPARTMENT OF MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

DATA COLLECTION 2 / 50

Does the Privacy Policy state **anything about what specific personal information the domain collects** from consumers?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement about what specific personal information the domain collects or does not collect from consumers.

Examples:

- We collect your name and address when you register for this site.
- We collect only demographic information, such as your gender, age, and ZIP code.

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

DATA COLLECTION

3 / 50

Does the Privacy Policy state the **specific purposes** for the collection of personal information?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement about why specific personal information the domain collects.

Example:

- We collect email address to contact customers for marketing purposes.

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

DATA COLLECTION

4 / 50

Does the Privacy Policy state anything about **what personal information** is necessary to **fulfill the purposes specified**?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement about the personal information that the domain needs to fulfill the purposes specified.

Example:

- When you send a question to "Ask Us," you must provide us an email address. We use this address to answer your question.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

DATA COLLECTION

5 / 50

Does the Privacy Policy state anything about whether the domain **limits** its **collection** of personal information to what is necessary for **specified purposes**?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says regarding the **limiting** collection of personal information.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain limit both the type and amount of personal information it collects to only that which is necessary for the identified purposes.

Example:

- We only collect personal information that

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

DATA COLLECTION

6 / 50

Does the Privacy Policy state anything about whether the domain does **NOT** collect any personal information for **unspecified purposes**?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says regarding the **collection** of personal information for **unspecified purposes**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain does not collect personal information without specifying purposes.

Examples:

- We do not collect personal information

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

DATA COLLECTION

7 / 50

Does the Privacy Policy state anything about whether the domain will specify **NEW** (i.e., **previously unspecified**) **purposes**, prior to the use or disclosure of the collected information?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain informs customers a **new purpose** not identified at the time of initial collection, prior to the use of personal information.

Example:

- Whenever we use your personal information for a previously unidentified purpose, we will notify you the new purpose.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

CONSENT

8 / 50

Does the Privacy Policy contain a declaration that the domain collects any personal information from customers **with their consent**?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says with respect to obtaining **consent** when it collects personal information.

Select YES or NO for the question.

Answer YES: If you find an **express** statement that the domain obtains **consent** when it collects personal information from consumers.

Example:

- With your consent, we will collect your email address to contact you later.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

CONSENT

9 / 50

Does the Privacy Policy state anything about whether the domain will obtain **consent** from customers if personal information is to be used or disclosed for **a new purpose** not previously specified?

YES

NO

INSTRUCTION

This question requires you to characterize whether or not the domain obtains **consent before the use** of information for a **previously unspecified purpose**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain obtains **consent** before the use or disclosure of personal information for a **new purpose** not identified at the time of initial collection.

Example:

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

CONSENT

10 / 50

Does the Privacy Policy state anything about whether the domain does **NOT use or disclose** the collected personal information for a new (i.e., not previously specified) purpose **without customers' consent**?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says with respect to obtaining **consent for the use** of personal information for a **new purpose**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain does not use personal information without customers' consent for a previously unspecified purpose.

Example:

- We do not use any of your personal

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

CONSENT

11 / 50

Does the Privacy Policy state anything about whether the domain allows a customer to **withdraw consent** at any time?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says regarding the **withdrawal** of consent.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain allows customers to withdraw consent at any time.

Example:

- If you do not want us to keep your email address, please send an email to the

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION

12 / 50

Does the Privacy Policy state anything about whether personal information is **used ONLY for the purpose** for which the information was obtained or compiled?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says regarding the **use of personal information**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain uses personal information only for the identified purposes.

Examples:

- We use and disclose your personal information only for the purpose for which

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION

13 / 50

Does the Privacy Policy state **anything about how the domain may use** personal information it collects **for internal purposes**?

YES

NO

INSTRUCTION

"Internal purposes" include, but are not limited to, processing orders or requests for information, improving a site's performance, keeping track of which pages on a site are visited, and sending consumers future communications (such as emails, newsletters, updates, and marketing or promotional material).

Note: Internal purposes do **not** include the disclosure of information to third parties, for any purpose.

Select YES or NO for the question.

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION

14 / 50

Does the Privacy Policy state **anything about whether** the **domain uses** personal information it collects **to send communications to the consumer**?

YES

NO

INSTRUCTION

This question deals with one particular use of personal information for internal purposes - namely, the **use of personal information by the domain to send communications to the consumer**. The question asks if there is **any** statement (positive or negative) about this type of use.

Note: The term "**communications to the consumer**" includes, but is not limited to, putting the consumer on a mailing list, or sending the consumer marketing or promotional messages, newsletters, or updates. It also includes sending the consumer information about his/her order.

[Previous](#) [Next](#) [Close](#)

If YES, go to Company Privacy Policy Survey Page 15.

If NO, go to Company Privacy Policy Survey Page 17.



DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

USE OF PERSONAL INFORMATION

15 / 50

Choose **ONE** of the following options.

The Privacy Policy

- states that the **domain does or may** use personal information to **send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question)**.
- states that the **domain does not** use personal information to **send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question)**.

INSTRUCTION

This question requires you to characterize what the domain says regarding the use of personal information to send communications to the consumer.

Note: The term "**communications to the consumer**" includes, but is not limited to, putting the consumer on a mailing list, or sending the consumer marketing or promotional messages, newsletters, or updates. It also includes sending the consumer information about his/her order.

Select **ONE** for the question.

Option 1 ("does or may"): If you find a statement that the domain **does or may** use personal information to send communications to the consumer (**other than those directly related to processing an order or responding to a consumer's question**).

Examples:

- We use your email address to send you newsletters that may be of interest to you.

Previous Next Close

If OPTION 1, go to Company Privacy Policy Survey Page 16.

If OPTION 2, go to Company Privacy Policy Survey Page 17.




DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION
16 / 50

Choose **ONE** of the following options.

The Privacy Policy

- says that the **domain** provides consumers an opportunity to **opt in** to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).
- says that the **domain** provides consumers an opportunity to **opt out** of receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question).
- says that the **domain** requires **consent or offers a choice** with respect to receiving future communications from the domain (other than those directly related to processing an order or responding to a consumer's question), but **does not make clear** whether the choice is opt-in or opt-out.
- does not say anything about** offering consumers **choice** with respect to receiving future communications from the **domain** (other than those directly related to processing an order or responding to a consumer's question).

INSTRUCTION

This question requires you to characterize whether or not the domain offers consumers a **choice** regarding the use of their personal information to send communications to the consumer (other than those directly related to processing an order or responding to a consumer's question), and, if so, to determine the nature of that choice.

Note: The term "**communications to the consumer**" includes, but is not limited to, putting the consumer on a mailing list, or sending the consumer marketing or promotional messages, newsletters, or updates. It also includes sending the consumer information about his/her order.

Select **ONE** of four options for the question.

We ask about two types of choice - "**opt-in**" and "**opt-out**":

- "**Opt-in**" choice requires an affirmative act by the consumer (such as checking a click-box or sending an email or a letter) before the information can be used in a particular manner; i.e., the default is that the information **will not** be used.
- "**Opt-out**" choice allows the consumer to take an action (such as checking a click-box or sending an email or a letter) to prevent the information from being used in a particular manner; i.e., the default is that, absent action by the consumer, the information **will be** used.

If the domain provides choice with respect to sending **at least some** communications to the consumer (other than those directly related to processing an order or responding to a consumer's question), then answer this question based on that choice. Thus, for example, if the domain provides consumers choice with respect to being on the domain's mailing list, but does

Previous Next Close

| | |
|---|----------------|
|    Web-based Survey | |
| USE OF PERSONAL INFORMATION | 17 / 50 |
| <p>INSTRUCTION</p> <p>This question deals with whether or not the privacy policy makes any statement about the domain's disclosure of personal information to third parties.</p> <p>Domains often use verbs other than "disclose." Look for statements about "sharing," "renting," "selling," "providing" or "giving" information to third parties.</p> <p>Note: Remember, "third parties" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.</p> | |
| <p>Does the Privacy Policy state anything about whether the domain discloses personal information it collects to third parties ?</p> | |
| <p><input type="radio"/> YES</p> <p><input type="radio"/> NO</p> | |
| <p>Previous Next Close</p> | |

If YES, go to Company Privacy Policy Survey Page 18.

If NO, go to Company Privacy Policy Survey Page 21.



Web-based Survey

USE OF PERSONAL INFORMATION

18 / 50

Choose **ONE** of the following options.

The Privacy Policy

- states that the domain **does or may** disclose **personal identifying information to third parties**.

- states that the domain **does NOT disclose personal identifying information to third parties, or does so only:**
 - (a) as required by law,
 - (b) as necessary to process an order, and/or
 - (c) in aggregate or non-identifying form.

INSTRUCTION

This question requires you to characterize what the domain says regarding the disclosure of **personal identifying information** to third parties.

Note: This question refers to **personal identifying information**. You must read the privacy policies carefully to see whether the domain does or may disclose such information, as opposed to non-identifying information.

If the domain speaks *generally* about disclosure of personal information - *without distinguishing between identifying or non-identifying information* - **YOU SHOULD TREAT THE STATEMENT AS REFERRING TO PERSONAL IDENTIFYING INFORMATION.**

Select ONE for the question.

Option 1 ("does or may"): If you find a statement that the domain **does or may** disclose **personal identifying information** to third parties

Previous Next Close

If OPTION 1, go to Company Privacy Policy Survey Page 19.

If OPTION 2, go to Company Privacy Policy Survey Page 21.



DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY **Web-based Survey**

DATA COLLECTION
19 / 50

Choose **ONE** of the following options.

The Privacy Policy

- says that the domain provides consumers an opportunity to **opt in** to the disclosure of **personal identifying information** to third parties.
- says that the domain provides consumers an opportunity to **opt out** of the disclosure of **personal identifying information** to third parties.
- says that the domain requires **consent or offers a choice** with respect to the disclosure of **personal identifying information** to third parties, but does not make clear whether the choice is opt-in or opt-out.
- does not say anything about** offering consumers **choice** with respect to disclosure of personal identifying information to third parties.

INSTRUCTION

This question requires you to characterize whether or not the domain offers consumers a **choice** regarding the disclosure of their personal information to third parties

Select **ONE** for the question.

We ask about two types of choice - "opt-in" and "opt-out":

- "Opt-in" choice requires an affirmative action by the consumer (such as checking a click-box or sending an email or a letter) before the information can be used in a particular manner; i.e., the default is that the information will not be used.
- "Opt-out" choice allows the consumer to take an action (such as checking a click-box or sending an email or a letter) to prevent the information from being used in a particular manner; i.e., the default is that, absent action by the consumer, the information will be used.

If the domain provides choice with respect to the disclosure of **at least some** personal identifying information to **at least some** third parties, answer this question based on that choice. Thus, for example, if the domain says that it provides consumers choice with respect to the disclosure of personal identifying information to advertisers, but does not say that it provides choice with respect to the disclosure of personal identifying

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION

20 / 50

Does the Privacy Policy state anything about whether the domain does **NOT** disclose any personal information to **third parties without customers' consent** (except where required by law or other regulations)?

YES

NO

INSTRUCTION

This question requires you to characterize whether or not the domain discloses personal information to **third parties, without customer consent**.

Note: Remember, "**third parties**" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain does not disclose personal information to third parties without consent.

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION

21 / 50

Does the Privacy Policy state that if the domain gathers and combines personal information from more than one source, it ensures that the **original purposes** of collections have **NOT** changed?

YES

NO

INSTRUCTION

This question requires you to characterize what the domain says regarding the **gathering and combination** of personal information from **several sources**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that if the domain **gathers and combines** personal information from **several sources**, the domain ensures that the **original purposes** of collections have not changed.

Example:

When we combine personal information from several sources, we ensure that the original purposes of collection have not changed.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

USE OF PERSONAL INFORMATION 22 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about whether the **domain has guidelines and implements procedures** with respect to the **retention** of personal information?

YES

NO

Answer YES: If you find **at least one** statement that if the domain has **guidelines or procedures** with respect to the **retention** of personal information.

Example:

- We have a policy about the retention of personal information and have a timetable for retaining and disposing of personal information. Click here to see the policy and the timetable.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

ACCESS TO PERSONAL INFORMATION 23 / 50

INSTRUCTION
This question requires you to characterize what the domain says regarding the customers' **rights to obtain information** from the domain about the **retention of their personal information**.

Does the Privacy Policy state anything about the **customer's rights to obtain information** as to whether or not the domain holds personal information about them?

YES

NO

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that consumers have a right to request whether or not the domain has their personal information.

Example:

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

ACCESS TO PERSONAL INFORMATION 24 / 50

INSTRUCTION
To answer **YES** to this question, you **must** find a statement that the domain allows consumers to see or review at least some of the personal information about them.
Select YES or NO for the question.

Answer YES: If you find a **statement** that the domain allows consumers to review at least some personal information about them.
Example:

The domain allows consumers to review at least some of the personal information about them.

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

ACCESS TO PERSONAL INFORMATION 25 / 50

INSTRUCTION
This question requires you to characterize what the domain says regarding the **means of accessing personal information**.
Select YES or NO for the question.

Answer YES: If you find **at least one** statement about how customers can get access to their personal information held by the domain.
Example:

- Please visit 'My Profile' to access and

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

ACCESS TO PERSONAL INFORMATION 26 / 50

INSTRUCTION
Privacy policies may use terms such as "edit" or "update" rather than "correct."
Select YES or NO for the question.

Does the Privacy Policy state that the domain allows consumers to **have inaccuracies corrected in at least some personal information** about them?

YES

NO

INSTRUCTION
Privacy policies may use terms such as "edit" or "update" rather than "correct."
Select YES or NO for the question.

Answer YES: If you find a **statement** that the domain allows consumers to have inaccuracies corrected in at least some personal information about them.
Examples:

- To correct your account information,

Previous Next Close

Next

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

ACCESS TO PERSONAL INFORMATION 27 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state that the domain allows consumers to **have at least some personal information about them deleted** from the domain's records?

YES

NO

INSTRUCTION
Select YES or NO for the question.

Answer YES: If you find a **statement** that the domain allows consumers to have at least some personal information about them deleted.
Examples:

- You may also delete information.
- To have your name and address deleted from our database, send us an email.

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

ACCESS TO PERSONAL INFORMATION 28 / 50

INSTRUCTION
This question requires you to characterize what the domain says regarding the customers' **rights** to be informed a reason when their **requests for information** have been **refused**.
Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain will provide a reason if it refuses to process customers' requests for information.
Example:

Does the Privacy Policy state anything about the **customer's rights to be given a reason**, if requests for information have been **refused**?

YES

NO

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

SECURITY 29 / 50

INSTRUCTION
In answering these questions, be especially careful to check all the print-outs in your folder; sometimes information about security is included in its own section, often called "**Security**" or "**About Security**."

These questions ask about the **steps taken by domains** to provide security. Statements about a domain's **efforts** to provide security are sufficient, even if the domain does not guarantee security. Thus, terms such as "**best efforts**," "**attempt**," "**make an effort**," "**strive**" and "**try**" - when used to describe a domain's security efforts - all qualify as statements regarding **steps taken by domains** with respect to providing

Does the Privacy Policy state that the domain **takes any steps to provide security**?

YES

NO

[Previous](#) [Next](#) [Close](#)

[Next](#)

If YES, go to Company Privacy Policy Survey Page 30.

If NO, go to Company Privacy Policy Survey Page 34.

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

SECURITY

30 / 50

Does the Privacy Policy state that the domain takes steps to provide **security**, for personal information the domain collects, **during transmission** of the information from the consumer to the domain?

INSTRUCTION

Secured Socket Layer or "SSL" refers to security during **transmission**.

Select YES or NO for the question.

Answer YES: If you find a statement that the domain takes steps to provide security **during transmission** of the information from the consumer to the domain.

Examples:

- We use SSL to protect your credit card information.
- We encrypt your information when you

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

SECURITY

31 / 50

Does the Privacy Policy state that the domain takes steps to provide **security**, for personal information the domain collects, **after the domain has received the information** (i.e., not during transmission, but after collection)?

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find a statement that the domain takes steps to provide security for personal information **after the domain has received the information**.

Examples:

- We store all our customer information on a secure server.
- We use firewalls to prevent unauthorized access to our databases and servers.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

SECURITY

32 / 50

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find a statement that the domain takes steps to provide security by **organization measures** such as security clearances and authority levels with regard to access to data.

Examples:

- We have a information security policy which includes specific requirements for the identification and authorization of personnel with access to personal information.
- All staffs are authenticated in order to gain

Does the Privacy Policy state anything about whether the domain takes steps to provide **security**, for personal information the domain collects, by **organizational measures** (e.g., limited to access to data and security clearances)?

YES **NO**

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

SECURITY

33 / 50

INSTRUCTION

This question requires you to characterize what the domain says regarding **physical security protections**.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain takes a step to provide security by **physical measures** such as identification card and restricted access to offices.

Examples:

- All personnel have unique identification cards, which are used to access personal

Does the Privacy Policy state anything about whether the domain takes steps to provide **security**, for personal information the domain collects, by **physical measures** (e.g., restricted access to offices and identification cards)?

YES **NO**

Previous Next Close



Web-based Survey

ACCURACY

34 / 50

Does the Privacy Policy state anything about **how the domain handles the inaccuracies** personal information it has collected?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement concerning the **way** by which the domain handles **inaccuracies** of personal information held by it.

Examples:

- We will provide reasonable access to your personal information, and allow you to correct the inaccuracy and incompleteness of the information.

[Previous](#) [Next](#) [Close](#)



Web-based Survey

ACCURACY

35 / 50

Does the Privacy Policy state that the domain **destroys, erases, or makes anonymous** personal information that is **no longer required** to fulfill the identified purposes?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain destroys or makes anonymous personal information if the information is not longer required to fulfill the identified purposes.

Example:

- We destroy your personal information when it is no longer needed.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

ACCURACY 36 / 50

INSTRUCTION

This question requires you to characterize whether or not the domain informs the **third parties of correction to personal information**.

Note: Remember, "**third parties**" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain notifies the **change or correction** of personal information to **third parties** that the information has been transferred.

Does the Privacy Policy state anything about whether the domain provides **notices of correction of information to third parties** to whom personal information has been previously disclosed?

YES

NO

Previous Next Close

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

Privacy Compliance and Accountability 37 / 50

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find **at least one** statement about whether the domain has a person or group of people who is responsible for its privacy policies and practices.

Example:

- We have 'Privacy Manager' who is responsible for activities with respect to the collection, use, and transfer of personal information.

Does the Privacy Policy state anything about whether the domain has **a person or group of people** who are **accountable** for the domain's privacy policies and practices?

YES

NO

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 38 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about the **identity and contact information** of the person or group of people who is accountable for compliance with the domain's privacy policies and practices?

YES

NO

Answer YES: If you find **at least one** statement about the **identity and contact information** of the person or group of people in the domain who are accountable for compliance with established privacy policies.

Example:

- If you have any questions or concerns about the privacy policies please contact the person below:

Position: Privacy Manager

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 39 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about the **whom customers may contact for complaints**, and for **general inquires** regarding their personal information?

YES

NO

Answer YES: If you find **at least one** statement about **whom** customers **contact** if they have questions or complaints regarding their personal information.

Example:

- If you have any questions or complaints about your personal information, please contact our representatives (customerrep@privacy.com).

Previous Next Close



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 40 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about **how** the domain **responds to a customer's general inquires and complaints**?

Answer YES: If you find **at least one** statement about whether the domain responds properly to a customer's complaints and inquires (i.e., in a reasonable time, at minimal or preferably no cost, and in a form that is generally understandable).

YES

NO

Example:

- We will respond to your request by email within a week. If your request involves extensive costs, we may request you to

[Previous](#) [Next](#) [Close](#)



DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 41 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about **mechanisms** which ensure the consistent **implementation of privacy policies and practices**?

Answer YES: If you find **at least one** statement about whether the domain has **procedures** which ensure the consistent implementation of privacy policies and practices (e.g., regularly scheduled audits and compliance checks on the privacy requirements of all involved parties, training staff, or communicating information to staff about the domain's policies and practices).

YES

NO

Examples:

- We regularly review our privacy policies

[Previous](#) [Next](#) [Close](#)




DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 42 / 50

INSTRUCTION

Note: Remember, "third parties" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement that the domain is responsible for personal information in its custody including the information that has been transferred to third parties.

Example:

- We hold our responsibility regarding

Does the Privacy Policy state anything about the domain being **responsible for personal information in its custody**, including information that has been transferred to **third parties** for processing?

YES

NO




DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Compliance and Accountability 43 / 50

INSTRUCTION

Note: Remember, "third parties" include any entity other than the domain, such as advertisers, affiliates, business partners, or other companies.

Select YES or NO for the question.

Answer YES: If you find **at least one** statement about whether the domain ensures that third parties maintain a comparable level of privacy protection.

Example:

- We have specific audit and enforcement mechanism (e.g., contracts) to ensure

Does the Privacy Policy state anything about whether the domain ensures that when third parties process personal information, the parties **maintain a level of privacy protection** comparable to the domain's practices?

YES

NO

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

Privacy Compliance and Accountability 44 / 50

INSTRUCTION
This question requires you to characterize what the domain says regarding **compliant procedures**.
Select YES or NO for the question.

Does the Privacy Policy state anything about **complaint procedures** such as those of the company, the industry associations, or the regulatory bodies?

YES

NO

Answer YES: If you find **at least one** statement about the existence of relevant compliant procedures.
Example:

- If you have any complaints about our privacy practices, please contact our

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY MANAGEMENT TOOL Web-based Survey

Privacy Compliance and Accountability 45 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about when the domain finds **a compliant to be justified**, the domain **takes appropriate measures to rectify the situation** (including, if necessary, amending its policies and practices)?

YES

NO

Answer YES: If you find **at least one** statement about whether the domain takes appropriate corrective actions such as amending its policies and advising staffs.
Example:

- If we find your complaint to be justified, we will change our privacy policies and practices, if necessary.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

Privacy Compliance and Accountability 46 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state anything about providing **appropriate means of recourse** to injured parties?

YES

NO

Answer YES: If you find **at least one** statement about the appropriate **means of recourse** to injured parties.

Example:

- If you suffered due to our inappropriate privacy practices, we will provide a remedy for the violation such as correction of any misinformation, cessation of unfair practices, and compensation for any harm.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

SURVEY Web-based Survey

COOKIES 47 / 50

INSTRUCTION
Select YES or NO for the question.

Does the Privacy Policy state **anything about whether the domain places cookies**?

YES

NO

Answer YES: If you find a statement that the domain places cookies. Also answer YES if you find a statement that the domain **does not** place cookies.

Examples:

- We use cookies on this site.
- We also collect certain information through cookies.

[Previous](#) [Next](#) [Close](#)

If YES, go to Company Privacy Policy Survey Page 48.

If NO, go to Company Privacy Policy Survey Page 49.

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

COOKIES

48 / 50

Choose **ONE** of the following options.

The Privacy Policy

says that the domain **does or may** place cookies.

says that the domain **does not** place cookies.

INSTRUCTION

This question requires you to characterize what the domain says its **use of cookies**.

Select ONE for the question.

Option 1 ("does or may"): If the domain says that the domain **does or may** place cookies.

Examples:

- We use cookies on this site.
- We also collect certain information through cookies. We might in the future use cookies.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

COOKIES

49 / 50

Does the Privacy Policy state **anything about whether THIRD PARTIES may place cookies** and/or collect personal information on the domain?

YES

NO

INSTRUCTION

Select YES or NO for the question.

Answer YES: If you find a statement that third parties may place cookies and/or collect personal information on the domain. Also answer YES if you find a statement that third parties do not place cookies and/or collect personal information on the domain.

Examples:

- Advertisers whose ads appear on our site may use cookies.

[Previous](#) [Next](#) [Close](#)

If YES, go to Company Privacy Policy Survey Page 50.

If NO, go to Company Privacy Policy Survey End Page.

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

COOKIES

50 / 50

Choose **ONE** of the following options.

The Privacy Policy

- says that third parties **do or may** place cookies and/or collect personal information on the domain.
- says that third parties **do not** place cookies and/or collect personal information on the domain.

INSTRUCTION

This question requires you to characterize what the domain says about **third parties' use of cookies** on the domain.

Select **ONE** for the question.

Option 1 ("does or may"): If the domain says that third parties **do or may** place cookies and/or collect personal information on the domain.

Examples:

- Advertisers whose ads appear on our site may use cookies.
- We cannot control the use of cookies by advertisers or partners on our site.

[Previous](#) [Next](#) [Close](#)

DEPARTMENT OF
MANAGEMENT SCIENCES

Web-based Survey

Privacy Policy Survey

Thank you for your submission.

Click "**Company List**" go to next assigned company.

Click "**Survey Main**" go to the survey main page.

[Survey Main](#) [Company List](#) [Close](#)