A Gap in Perceived Importance of Privacy Policies between Individuals and Companies

A Gap in Perceived Importance of Privacy Policies between Individuals and Companies

Efrim Boritz
School of Accounting & Finance
University of Waterloo
Waterloo, Canada
jeboritz@uwaterloo.ca

Won Gyun No
Department of Accounting
Iowa State University
Ames, U.S.A
wgno@iastate.edu

***Abstract*—Although several studies have examined individuals' privacy concerns and companies' privacy policy disclosures, only a few studies examined whether customers' privacy concerns are adequately addressed in companies' privacy policy disclosures. This study investigates companies' privacy policy statements and important privacy policies that individuals want to know. We examine the privacy policy statements of 136 companies from the U.S. and Canada and relate them to the results of a Web-based user survey of 210 respondents. Our findings reveal a difference in companies' privacy policies between the U.S. and Canada and a gap between what privacy policies individuals value and what companies emphasize in their privacy policy statements.**

Privacy; Fair Information Practics; Privacy Policies

I. INTRODUCTION

The growing privacy concerns of customers are resulting in companies paying increased attention to privacy [1, 2]. A number of studies have shown that companies' privacy policy disclosures are signals to individuals about their fair information practices and thus help build trust and promote the disclosure of personal information [e.g., 2, 3, 4]. However, only a few studies have examined whether customers' privacy concerns are adequately addressed in companies' privacy policy disclosures. For instance, based on findings from prior literature, Sheehan and Hoy [5] came up with five influences that might reflect the underlying dimensions of customers' privacy concerns and examined whether FTC Fair Information Practice (FIP) principles reflect these five influences. They found that the FTC FIP principles reflect three influences on customers' privacy concerns (i.e., awareness of information collection, information usage, and information sensitivity), but not the other two influences (i.e., the exchange of information for appropriate compensation and the relationships between entities and online users). Earp et al. [6] studied a difference 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. That is, the three most frequently addressed information items in privacy statements were 1) security over data collection and transfer 2) how data is collected, and 3) consent about information collection. However, users were mainly 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.

Although the studies conducted by Sheehan and Hoy [5] and Earp et al. [6] examine the question of whether FTC principles sufficiently encompass 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 covered in the OECD principles; 2) whether companies' privacy policy statements include OECD principles that are most central to consumers; and 3) whether customers and companies perceive each OECD principle differently depending on the nature of personal information involved (e.g., sensitive versus non-sensitive information). The aforementioned three unanswered questions are investigated in this study.

The study differs from the study conducted by Sheehan and Hoy [5] which focuses on the U.S. FTC's core principles by investigating whether customers' concerns are addressed in companies' privacy policy statements using a more universal set of FIP principles (i.e., OECD principles). The OECD guidelines are the global standard for privacy protection and are the recommended model for legislation in number of countries [6-8]. The FTC principles only reflect a subset of the privacy principles stated in the OECD guidelines. This study also differs from Earp et al. [6]. Earp and his colleagues examined the difference between users' privacy concerns and companies' privacy policies in health care industries. Earp et al. used a qualitative approach to identify differences between their content analyses of the Web site data and the survey data from users. In contrast, we examine Web sites from a variety of industries and conduct a quantitative analysis of the gap between individuals' perceived importance ratings of companies' privacy policies and privacy policies disclosed in companies' privacy policy statements. Also, in contrast with Earp et al. who used a mixture of FTC principles and their own categories of privacy policies, we use OECD principles as a benchmark for comparing company disclosures. In addition, we investigate whether there are differences in companies'

978-0-7695-3805-1/09 $26.00 © 2009 IEEE
DOI 10.1109/CONGRESS.2009.32

privacy policy disclosures between the U.S. and Canadian companies and whether such differences exist due to the nature of personal information (e.g., sensitive versus non-sensitive information).

A Web-based survey of 210 Internet users was conducted to identify FIP principles that are most important to consumers. Next, the disclosure of these principles in companies' privacy policy statements was examined by assessing a total of 136 Web sites' privacy policies from the U.S. and Canada. We find a difference in companies' privacy policies between the U.S. and Canada. In addition, there is a gap between individuals' importance ratings of companies' privacy policies and the privacy policies that companies emphasize in their privacy policy disclosures. The results of this research are particularly important for regulators since the findings provide information as to whether individuals' privacy concerns are adequately addressed in companies' privacy policy disclosures. This information may used to promote privacy laws and educate the public about privacy issues to protect customer privacy. It also can help companies to reduce their customers' privacy concerns by emphasizing matters that customers consider most important and thus help to build strong trusting relationships with their customers.

The remainder of the paper is organized as follows. Following this brief introduction, the next section reviews the background literature and addresses hypotheses to be investigated in this study. This is followed by details of the research methodology. Next, the results of the study are presented, and their implications are discussed. Finally, this paper concludes with a brief summary of findings and the limitations of the study.

II. RATURE REVIEW

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. One stream of previous research has investigated the relationship between privacy concerns and customer behavior [e.g., 4, 9-11]. For instance, Earp and Baumer [4] studied consumers' behavior and online privacy and 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. Phelps, Nowak, and Ferrell [11] examined the relationship between customers' privacy concerns and their behavior as well as factors affecting their privacy concerns. They found 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.

Another stream of previous research has examined companies' practices with respect to the privacy policy disclosures on their Web sites [e.g., 12, 13, 14]. For example, Desai, Richards, and Desai [12] examined Internet policies posted on 40 U.S. companies' Web sites from 1999 to 2001 and found that privacy-related policies were the most frequently posted policies on companies' Web sites. Similarly, by analyzing four Web surveys conducted between 1998 and 2001, Milne and Culnan [14] found that the number of privacy disclosure statements increased over time, and also that most popular sites had posted more privacy disclosures than their counterparts.

In addition, several studies have examined the relationship between customers' privacy concerns and companies' privacy policies [e.g., 6, 15-18]. For instance, Palmer, Bailey, and Faraj [18] examined how firms use trusted third parties (i.e., privacy seals) and privacy policy statements to build trust on their Web sites. They found that by posting a privacy policy statement on their Web sites, companies can reduce their customers' perceived privacy concerns about providing personal information. On the contrary, Hui, Teo, and Lee [15] found that the existence of a privacy statement encouraged individuals to provide their personal information, but a privacy seal did not. They also showed a positive effect of monetary incentives and a negative effect of the amount of information requested on individuals' information disclosure.

III. RESEARCH HYPOTHESES

Each country adopts different regulatory approaches for dealing with Internet privacy. For instance, Canada has enacted privacy legislation that plays an important role in protecting privacy while the United States has taken a more liberal industry self-regulation approach [for more details see 7, 19, 20]. According to Sarathy and Robertson [21], for a number of companies, existing and pending legislations are likely to form the basis for developing their privacy policies. Hence, companies' privacy policy disclosures can be different between the U.S. and Canada due to their different regulatory approaches.

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 [8]. A variety of governments has developed their own FIPs and encourages or requires companies to use a specific FIP for creating privacy policy statements [22]. The U.S. uses FTC fair information practices as a guideline for creating privacy policy statements, and Canada uses PIPEDA (Personal Information Protection and Electronic Documents Act). Although FTC fair information practices and PIPEDA are similar, they differ in their specific requirements with respect to a number of key principles [7]. Hence, it is possible that some principles commonly addressed in the privacy policy statements of the U.S. companies may not be addressed in the privacy statements of Canadian companies. Therefore, the following hypothesis is suggested.

H1: FIP principles addressed in companies' privacy policy statements vary between the U.S. and Canada.

It is also possible that companies' privacy statements differ due to the type of industry in which a company operates its business. Prior literature has shown that companies in a particular industry tend to perceive the importance of privacy risks (e.g., lawsuit from customers) differently compared to companies in other industries [23].

Since individuals have different privacy concerns and preferences depending on the type of information a company collects and uses [11, 24], it is expected that the type of industry in which the company operates its business might influence the company's risk recognition and thus impact on its privacy policies. Prior studies have shown that medical and financial information is considered to be more sensitive than other types of information [25, 26]. Hence, companies in more information-sensitive industries (i.e., industries holding more sensitive information) such as financial and health industries may develop more comprehensive privacy policies by stating related FIP principles in their privacy policy disclosures than those in less information-sensitive industries (i.e., industries holding less sensitive information) such as manufacturing and retail industries. This leads to the following hypothesis.

H2: Companies in more information-sensitive industries incorporate more FIP principles in their privacy policy disclosures than do companies in less information-sensitive industries.

Prior studies have shown that companies' privacy policies stated in privacy policy statements help build trust and promote the disclosure of personal information by signaling customers about their fair information practices [3, 27]. Since companies in more information-sensitive industries collect and use personal information that leads to 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.

H3: Companies in more information-sensitive industries perceive FIP principles as having a different importance when compared to less information-sensitive industries.

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 how individuals perceive companies' privacy policies and whether companies' privacy policy disclosures address privacy policies that individuals want to know. 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 [5, 11, 28]. 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, they may be more willing to disclose their purchasing preferences, and in that context 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 for 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.

H4: 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., more information-sensitive industries) when compared to manufacturing or retail Web sites (i.e., less information-sensitive industries). Accordingly, this study proposes the following hypothesis.

H5: Individuals' perceived importance of FIP principles differs depending on the type of Web site.

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

H6: Companies incorporate more FIP principles that individuals perceive as important principles in their privacy policy disclosures than FIP principles that individuals perceived as less important.

IV. RESEARCH METHODOLOGY

A Web-based user survey was conducted to assess how individuals perceive FIP principles (presented below under the heading *Internet Privacy User Survey*). In addition, for companies' privacy policy disclosures, 136 companies' Web sites were examined to assess the content of privacy policy statements (presented below under the heading *Privacy Policy Disclosure Survey*).

A. Internet privacy user survey

A survey was conducted to gather information about individuals' importance ratings of OECD based principles. A Web-based survey was employed because it provides the ability to skip questions on previous answers and allows greater design flexibility and data control. Research participants were first provided general information about the study. Then, they were asked to complete the Internet privacy questionnaire.

A questionnaire was developed to probe participants' concerns regarding various aspects of Internet privacy. The questionnaire consisted of three sections. The first section was designed to gather demographic information. The

second section was developed as part of the manipulation. 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 wanted to know. The third section measured individuals' privacy concerns. A scale developed by Chellappa and Sin [29] was adapted to assess individuals' privacy concerns.

A pre-test and a pilot test were conducted. A total of 16 questions were finally developed.[1] Except for demographic questions such as age, gender, and ethnicity, most questions were measured using a seven-point scale. A total of 210 students participated in the study, and the response rate was 38 percent. 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. Over a month, 267 students visited the survey site. Among 267 participants, 11 did not provide any information, 56 did not finish the Internet privacy user survey. Accordingly, the final sample consisted of 210 valid responses. On average, it took 29 minutes for participants to complete the survey.

B. Privacy Policy Disclosure Survey

A questionnaire was developed to capture whether companies' privacy policies stated in privacy policy statements address FIP. Since the U.S. and Canada have adopted different FIP, companies may develop their privacy policy statements based on their country's FIP. For comparison purposes, OECD privacy guidelines were used because FIPs developed by both countries were based on OECD guidelines [30, 31]. The OECD privacy guidelines offer fundamental guidelines for privacy protection and establish eight principles that could be used as the benchmark for assessing organizations' privacy policies. The eight principles in the OECD guideline include *Accountability*, *Collection Limitation*, *Data Quality*, *Individual Participation*, *Openness*, *Purpose Specification*, *Security Safeguards*, and *Use Limitation*.

We first carefully examined the guidelines and detailed comments of the OECD guideline principles (henceforth, OECD principles) in 'OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' [8]. Next, the major requirements of each OECD principle were identified. Based on the identified requirements, survey items for each OECD principle were developed.

Additionally, a panel of experts reviewed the identified requirements of each OECD principle to assure the study had adequately tapped into each OECD principle.[2] In addition, seven graduate students conducted a pilot test. 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.[3]

The study adopted procedures similar to those implemented in FTC [32]. A total of four trained graduate students (hereafter, surfers) were hired to conduct the Web site survey. Two surfers were assigned for the U.S. companies, and the other two surfers were assigned for Canadian companies. The data collection was done using a Web-based survey. First, each surfer participated in a three-hour training session that was intended to explain the entire survey procedures, skills required to visit and review Web sites, and the use of Web-based survey. Following this training session, a list of companies' Web sites was provided to a pair of assigned surfers. The sites were drawn from Mergent Online (formerly Moody's Online) [33]. For each country, the top 34 largest companies from more information-sensitive industries and another top 34 from less information-sensitive industries were selected.[4] As with literatures in the past, this study defined "large" by the number of employees. More information-sensitive industries included finance, insurance and real-estate (SIC major group 60 to 67), and health-care (SIC major group 80).

Next, each surfer in the pair independently accessed each Web site to search for its privacy policy disclosures and to print privacy policy disclosures, and then independently completed the privacy policy survey questionnaire. Once both surfers 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.

C. Measures

Based on the privacy policy disclosure survey results, eight OECD principle scores were created to measure the eight OECD principles that could be addressed in a company's privacy policy statement. All questions used to measure the eight OECD principles were True/False questions coded as '1' for True and '0' for False. The score of each OECD principle was calculated by adding the score for each question. For example, if a company's privacy policy statement explains its practice about *Purpose Specification* principle (i.e., the domain states what specific personal information it collects from consumers), one point is assigned to *Purpose Specification* score. Thus, the company will be assigned the maximum five of *Purpose Specification* score if the company's privacy policy statement addresses all five questions. On the other hand, if none of the information is described in the privacy policy statement, *Purpose Specification* score will be zero. Accordingly, the maximum scores of each OECD principle are *Accountability* (2), *Collection Limitation* (4), *Data Quality* (3), *Individual Participation* (6), *Openness* (2), *Purpose Specification* (5), *Security Safeguards* (5), and *Use Limitation* (3). The sum of each principle score represents the OECD principle score, and thus the maximum OECD principle score is 30.

[1] The survey items are available from the authors.

[2] 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).

[3] The survey items are available from the authors.

[4] The number, 34 Web sites, was arbitrarily select to ensure enough statistical power for the study.

In addition, the rank order of eight OECD principles was identified. Since the number of questions used to measure 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 *Accountability* and *Collection Limitation* principles in the U.S. were .66 and .54, and the maximum scores of both principles were 2 and 4, respectively. Each proportion score was calculated by dividing each mean score by its maximum principle score. Thus, the proportion score of *Accountability* principle was .33 (= .66/2) and that of *Collection Limitation* principle was .14 (= .54/4). Then, the rank order of proportion scores was determined.

The participants' perceived importance of OECD principles was also measured. Based on the respondents' answers about two pieces of information that they feel most reluctant to provide (e.g., SIN and student ID) and two pieces of information that they least reluctant to provide (e.g., gender and age), several questions were automatically generated to assess their perceived importance of OECD principles in an online shopping site and a banking site. 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 privacy policies from the list of privacy policies developed based on OECD principles when they are 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 the participants (i.e., 105 respondents) were requested to identify the two most important and the two least important company privacy policies when they are asked to provide two pieces of information that they feel *least* reluctant to provide in an online shopping site. The same questions were also asked of 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.

Firm size and firm age were used as control variables. Since large companies are more concerned about information privacy and tend to post more privacy policy disclosures than small companies because of customer relationship and litigation risks, it is possible that FIP principles addressed in companies' privacy policy statements are affected by the size of a company. In addition, a firm's age may influence its privacy policy disclosures since a firm's disclosure policy likely varies with the maturity of its public relations, which likely improves over time from learning. Firm size was measured with the number of employees. Firm age was measured by subtracting the year of incorporation from the study year (i.e., 2008).

V. Analysis and Results

An analysis of covariance (ANCOVA) was conducted to assess, after controlling for firm size and firm age, whether there is a difference in companies' privacy policies between the U.S. and Canada and whether companies' privacy policies in more information-sensitive industries are different from those in less information-sensitive industries. In addition, Spearman rho statistic was calculated to assess a gap in the perceived importance of OECD principles between individuals and companies.

A. Descriptive statistics

A total of 210 students participated in the Internet privacy user survey. 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. About 88 percent of the respondents was undergraduate students. Of the participants, about 92% reported that they had online transaction experiences such as ordering things, subscribing to services or registering on Web sites for online services. On average, they conducted online transactions 10 times in the past twelve months. Furthermore, 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 by type of personal information requested. 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).

A total of 136 sites, 68 Web sites for each of the U.S. and Canada, were accessed and investigated. The companies are from 7 different industries classified by SIC division structure from the U.S. Department of Labor[5]: Mining (2), Manufacturing (25), Transportation, Communications, Electric, Gas, And Sanitary Services (14), Wholesale Trade (2), Retail Trade (17), Finance, Insurance, And Real Estate (60), and Services (16). On average, the number of employees is 94,179. The mean values of net income, total assets, and total revenue are $15,145M, $142,223M, and $30,049M.

B. Differences in Web site disclosing OECD principles

The privacy policy statements of 136 Web sites were examined to measure their compliance with the eight OECD principles. Figure 1 shows a summary of Web sites disclosing OECD principles.

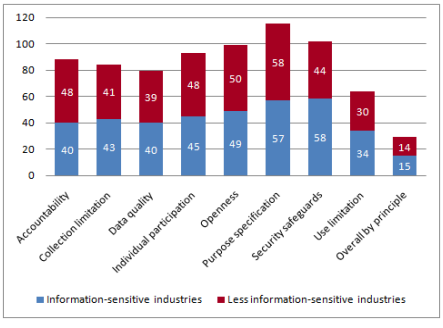


Figure 1. Summary of OECD principles

[5] See more detail at www.osha.gov/pls/imis/sic_manual.html.

Overall, only 29 of 136 sites (21.3%) addressed all OECD principles in their privacy policy statements. In terms of each OECD principle, *Purpose Specification* (115 sites) was the most frequently addressed principle followed by *Security Safeguards* (102 sites), *Openness* (99 sites), *Individual Participation* (93 sites), *Accountability* (88 sites), *Collection Limitation* (84 sites), *Data Quality* (79 sites), and *Use Limitation* (64 sites).

With regards to the less information-sensitive industries, 14 of 68 Web sites (20.6%) addressed all OECD principles. *Purpose Specification* (58 sites) was the most frequently addressed principle, and *Use Limitation* (30 sites) was the least commonly stated principle. In terms of the more information-sensitive industry group, 15 of 68 Web sites (22.1%) incorporated at least a piece of information about all OECD principles in their privacy policy statements. *Security Safeguards* (58 sites) was the most often addressed principle while *Use Limitation* (34 sites) was the least frequently posted principle.

The low percentage of Web sites disclosing OECD principles and the low mean values of OECD principle scores suggest that many Web sites in both countries did not address all OECD principles in their privacy policy statements.

C. *Differences in privacy policies between the U.S. and Canada*

An analysis of covariance (ANCOVA) was conducted to assess differences in companies' privacy policies between U.S. and Canada and between industries after controlling for firm size and firm age. The ANCOVA results are shown in Table I.

TABLE I. ANALYSIS OF COVARIANCE RESULTS

Source	*df*	*MS*	*F*	*P*
FIRM_SIZE	1	91.616	2.154	.145
FIRM_AGE	1	156.407	3.678	.057
COUNTRY	1	212.867	5.006	.027
INDUSTRY	1	4.778	.112	.738
COUNTRY*INDUSTRY	1	7.653	.180	.672
Error	130	42.526		

The result of overall OECD principle score indicates a significant difference between U.S. and Canada ($F_{(1, 130)}$ = 5.006 p = .027). This indicates that OECD principles disclosure varied between two countries, supporting H1. Another main effect (i.e., INDUSTRY) was not significant, suggesting that OECD principles disclosure did not differ between the less information-sensitive industry group and the more information-sensitive industry group.[6] Also, the interaction effect was not statistically significant. These results are inconsistent with H2. That is, companies in more information-sensitive industries did not incorporate more OECD principles in their privacy policy statements than companies in less information-sensitive industries.[7]

Although the analysis results of overall OECD principle show a significant difference between the two countries and no significant difference between the two industries, these results may be due to the differences in FIP adopted by each country (e.g., FTC vs. PIPEDA) and the different importance of each principle in each industry (e.g., *Security Safeguards* for financial vs. retail industries). Hence, an analysis for each OECD principle was also performed. The analysis results of each OECD principle indicate that five OECD principles (*Accountability*, *Collection Limitation*, *Individual Participation*, *Purpose Specification*, and *Use Limitation*) were significantly different between U.S. and Canada (all p < .05), but *Data Quality*, *Openness*, and *Security Safeguards* principles were not. Only the *Security Safeguards* principle was significantly different between less information-sensitive industry and more information-sensitive industry groups (p = .023).

In terms of interactions, the *Accountability*, *Data Quality*, and *Openness* principles were marginally significant (p = .093, p = .055, and p = .078, respectively). 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, with respect to *Accountability* principle, the difference between two industries in each country was examined. The results (not provided in tabular form) indicate that there was a significant difference between the less information-sensitive industry and more information-sensitive industry groups in the U.S. ($F_{(1, 64)}$ = 6.555, p = .013), but the difference was not statistically significant in Canada.

D. *Additional analysis using other FIP principles*

Since the analysis results of each OECD principle indicate a difference between the two countries for five principles as well as a difference between the two industries for the *Security Safeguards* principle, it is possible that these results are due to the differences in FIPs adopted in the U.S. and Canada to manage privacy issues. Hence, we conducted additional analyses to examine whether the differences in companies' privacy policies between the U.S. and Canada would still exist if we used different FIP principles as the benchmark for comparison: FTC fair information practice in U.S. and PIPEDA in Canada. Following the same procedure used to develop the OECD principle score, two additional variables were created based on the privacy policy disclosure survey results: FTC principle score and PIPEDA principle score.[8] Figure 2 summarizes the FIP principles score and PIPEDA principle score.

[6] It is possible that the insignificant industry effect is due to our rough industry classification. To test this explanation, we conducted another analysis using two additional industry classifications: 1) SIC division structure from U.S. Department of Labor and 2) two-digit SIC codes. The results were the same.

[7] We also conducted ANCOVAs for each country to examine the differences in industry level. The ANCOVA results indicated that OECD principles disclosure was not significantly different between two industries in two countries.

[8] The survey items are available from the authors.

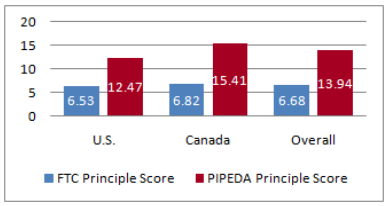


Figure 2. Summary of FTC and PIPEDA principles

On average, roughly 7 pieces of information from a maximum of 16 FTC principle score were stated in companies' privacy policy statements: the U.S. (6.53) and Canada (6.82). In terms of PIPEDA principle, companies addressed approximately 14 pieces of information from a maximum of 37 PIPEDA principle score. Companies in Canada posted more PIPEDA principles (15.41) in their privacy policy statements than those in the U.S. (12.47).

An analysis of covariance (ANCOVA) was conducted to assess differences between the U.S. and Canada and between industries after controlling for firm size and firm age. Table II shows ANCOVA results.

TABLE II. ANALYSIS OF COVARIANCE RESULTS

FTC principle score

Source	*df*	*MS*	*F*	*P*
FIRM_SIZE	1	20.778	1.687	.196
FIRM_AGE	1	35.854	2.911	.090
COUNTRY	1	9.975	.810	.370
INDUSTRY	1	7.133	.579	.448
COUNTRY*INDUSTRY	1	1.937	.157	.692
Error	130	12.315		

PIPEDA principle score

Source	*df*	*MS*	*F*	*P*
FIRM_SIZE	1	154.241	2.608	.109
FIRM_AGE	1	208.507	3.526	.063
COUNTRY	1	387.310	6.549	.012
INDUSTRY	1	1.588	.027	.870
COUNTRY*INDUSTRY	1	8.584	.145	.704
Error	130	59.139		

The ANCOVA results indicate an insignificant difference in overall FIP principle score between the U.S. and Canada. However, a significant difference between two countries was observed with respect to overall PIPEDA principle score, indicating that companies in Canada addressed more PIPEDA principles then those in the U.S. ($F_{(1,\ 130)}$ = 6.549, p = .012). With respect to industries, there is no significant difference between more information-sensitive industries and less information-sensitive industries with respect to both FTC principle and PIPEDA principle.

In addition, we conducted an analysis for each FTC principle as well as each PIPEDA principle.[9] The analysis results of each FTC principle indicate that two principles were significantly different between the U.S. and Canada: *Choice/Consent* (p = .001) and *Access/Participation* (p = .06). However, there were no differences between the two countries regarding the *Notice/Awareness*, *Integrity/Security*, and *Enforcement/Redress* principles. In terms of the PIPEDA principles, six principles were statistically different between the U.S. and Canada: *Accountability* (p = .039), *Consent* (p = .001), *Identifying Purposes* (p = .047), *Individual Access* (p = .03), *Limiting Collection* (p = .001), and *Limiting Use, Disclosure and Retention* (p = .001). However, there were no significant differences between two countries with respect to the *Accuracy*, *Challenging Compliance, Openness*, and *Safeguards* principles.

With respect to the differences between less information-sensitive industries and more information-sensitive industries, only the FTC principle of *Security/Integrity* was significantly different between the two industries, and this was only the case in the Canada (p = .07). Similarly, only the PIPEDA principle of *Security Safeguards* was significantly different between less information-sensitive industries and more information-sensitive industries. However, this was only the case in the U.S. (p = .043). A plausible explanation for these findings is that the major requirements of the *Security/Integrity* principle differ from those of the *Security Safeguards principle*. Therefore, companies in each country tend to comply with their countries' requirements, which, in turn, leads to the difference between the two industries in each country.

In summary, the results of our analyses indicate that there is no apparent difference between the U.S. and Canada regarding privacy policies addressed in companies' privacy policy statements when we analyze the statements using the less comprehensive FIP principle (i.e., FTC fair information practice principle). Only two FTC principles were significantly different between the U.S. and Canada: *Choice/Consent* and *Access/Participation*. In contrast, when we analyze the statements based on the more comprehensive FIP principles (i.e., PIPEDA principle), a significant difference was found between two countries with respect to the six PIPEDA principles: *Accountability*, *Consent*, *Identifying Purposes*, *Individual Access*, *Limiting Collection*, and *Limiting Use, Disclosure and Retention*

E. Frequently addressed OECD principles in companies' privacy policy disclosures

To examine which OECD principles are frequently disclosed in companies' privacy policy statements, the rank order of each OECD principle was identified based on the

[9] FTC fair information practice consists of five core principles: *Notice/Awareness*, *Choice/Consent*, *Access/Participation*, *Integrity/Security*, and *Enforcement/Redress*. On the other hand, PIPEDA consists of ten core principles: *Accountability*, *Identifying Purposes*, *Consent*, *Limiting Collection*, *Limiting Use*, *Disclosure*, *Retention*, *Accuracy*, *Safeguards*, *Openness*, *Individual Access*, and *Challenging Compliance*.

proportion score of each OECD principle. Figure 3 shows the rank order of OECD principles.

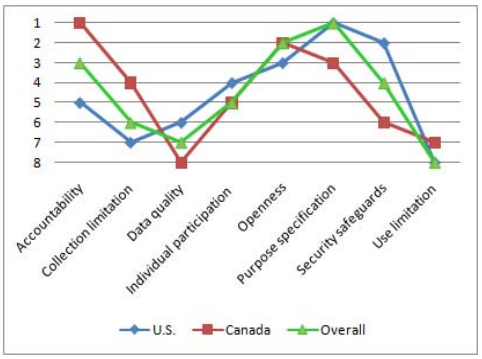


Figure 3. Rank order of OECD principles

The results reveal that the two most frequently addressed principles in the U.S. were the *Purpose Specification* and *Security Safeguards* principles. The *Accountability* and *Openness* principles were the two most frequently addressed OECD principles in Canada. On the other hand, the least frequently addressed principle in Canada was the *Data Quality* principle whereas the *Use Limitation* was the least frequently addressed principle in the U.S. Spearman's rho was calculated to examine if there was a difference among the mean ranks of the OECD principles between the U.S. and Canada. The result of the Spearman rho statistic was statistically insignificant ($\gamma_s(8) = .381$, $p = .352$), indicating that companies perceived each OECD principle as having different importance in the U.S. and Canada. The differences among countries with respect to each industry were also examined. The Spearman rho statistics showed that in both information-sensitive and less information-sensitive industries, the companies' perceived importance of OECD principles was different between the U.S. and Canada ($\gamma_s(8) = .19$, $p = .651$), and also there was difference between the two countries in less information-sensitive industries ($\gamma_s(8) = .571$, $p = .139$).

The difference between two industries with respect to OECD principles was also examined. The result of the Spearman rho statistic indicates that there was no difference in frequently addressed OECD principles between two industries ($\gamma_s(8) = .814$, $p = .014$). In addition, this study 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 be significant: the U.S. ($\gamma_s(8) = .881$, $p = .004$), Canada ($\gamma_s(8) = .929$, $p = .001$). This indicates that in the two countries, the companies' perceived importance of OECD principles was not different between the two industries. Hence, H3 is not supported.

F. *Important companies' privacy policies that individuals want to know*

Figure 4 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 *Security Safeguards* and *Use Limitation* principles as the two most important privacy policies that they wanted to know about. On the other hand, the *Data Quality* and *Individual Participation* principles were the two least important privacy policies.

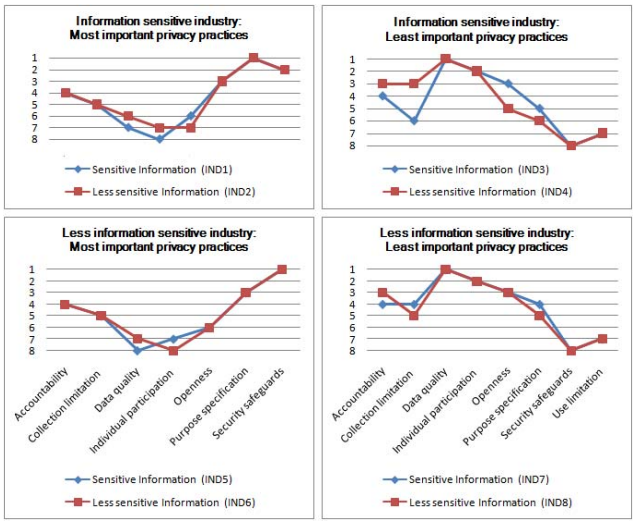


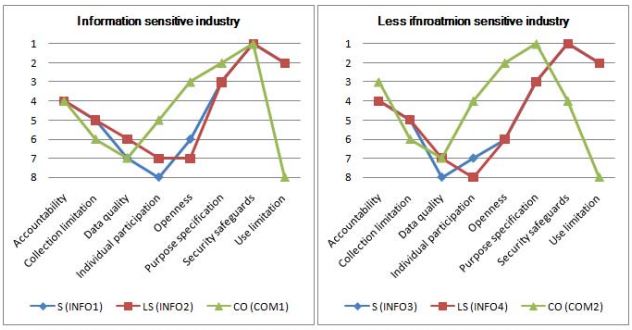
Figure 4. Individual's perceived importance of OECD principles

Spearman rho statistics were calculated to assess if there were differences in participants' importance ratings of OECD principles regarding the type of information requested. The results of Spearman rho statistics between IND1 and IND2, between IND3 and IND4, between IND5 and IND6, and between IND7 and IND8 were found to be significant ($\gamma_s(8) = .958$, $p < .001$; $\gamma_s(8) = .862$, $p = .006$; $\gamma_s(8) = .976$, $p < .001$; and $\gamma_s(8) = .963$, $p < .001$, respectively). These reveal that the participants' perceived importance of FIP principles did not differ depending on the type of information requested.

We also examined whether there were differences in the participants' importance ratings of OECD principles depending on the type of industry. Spearman rho statistics between IND1 and IND5, between IND2 and IND6, between IND3 and IND7, and between IND4 and IND8 were all statistically significant, which indicates no difference on the respondents' perceived importance of OECD principles depending on the type of industry the Web site belongs to ($\gamma_s(8) = .976$, $p < .001$; $\gamma_s(8) = .958$, $p < .001$; $\gamma_s(8) = .976$, $p < .001$; and $\gamma_s(8) = .921$, $p < .001$, respectively). Therefore, H4 and H5 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.

G. *Gap in perceived importance of OECD principles*

Figure 5 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.



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

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

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

Figure 5. Rank order of OECD principles

The rank order of each OECD principle shows a difference in the perceived importance of OECD principles between individuals and companies in both less information-sensitive industries and more information-sensitive industries. To investigate whether there is a significant gap between individuals' importance ratings of companies' privacy policies and the policies that companies emphasize in their privacy policy statements, Spearman's rho was used, and the results were not significant: INFO1 and COM1 ($\gamma_s(8) = .333$, $p = .42$), INFO2 and COM1 ($\gamma_s(8) = .216$, $p = .608$), INFO3 and COM2 ($\gamma_s(8) = .072$, $p = .866$), and INFO4 and COM2 ($\gamma_s(8) = .012$, $p = .978$). Hence, the privacy policies that individuals want to know were not addressed in companies' privacy policy statements in the same order of importance as their importance to individuals.

However, if we focus on the two most important companies' privacy policies that individuals want to know, a notable discrepancy is observed within the two industries. The *Security Safeguards* and *Use Limitation* principles were the two most important companies' privacy policies that individuals want to know in both industries. The *Security Safeguards* and *Purpose Specification* principles were the two most frequently addressed OECD principles in more information-sensitive industries while the *Purpose Specification* and *Openness* principles were the two most frequently addressed principles in less information-sensitive industries. This suggests that in more information-sensitive industries, one important OECD principle (i.e., *Security Safeguards*) that is central to customers was frequently addressed in companies' privacy policy statements. However, 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, the null hypothesis H6 is partially supported. That is, there is a gap between what privacy policies individuals value and what companies in less information-sensitive industries disclose in their privacy policy statements, but companies in more information-sensitive industries frequently disclose an important privacy policy (i.e., *Security Safeguards*) that is most central to customers.

VI. Discussion and Implications

This study investigated whether there are differences in companies' privacy policy disclosures between the U.S. and Canada and whether there is a gap between the individuals' perceived importance of OECD principles and the frequently addressed OECD principles in companies' privacy policy statements. The analyses of 136 Web sites' privacy policy statements and 210 participants' responses offer several interesting findings.

First, the results of this study indicate that there is a difference in companies' privacy policies between the U.S. and Canada. Five OECD principles (*Accountability*, *Collection Limitation*, *Individual Participation*, *Purpose Specification*, and *Use Limitation*) were significantly different between the U.S. and Canada, but *Data Quality*, *Openness*, and *Security Safeguards* principles were not. The two most frequently addressed OECD principles in the U.S. were the *Purpose Specification* and *Security Safeguards* principles while the *Accountability* and *Openness* principles were the two most frequently addressed OECD principles in Canada.

Second, only the *Security Safeguards* principle was significantly different between less information-sensitive industry and more information-sensitive industry groups, and this was only the case in the U.S.

Third, no apparent difference was found between the U.S. and Canada when companies' privacy policy statements were examined using the less comprehensive FIP principle (i.e., FTC fair information practices). Only two principles (i.e., *Choice/Consent* and *Access/Participation*) were significantly different between the U.S. and Canada, but there were no differences between two counties regarding the *Notice/Awareness*, *Integrity/Security*, and *Enforcement/Redress* principles. In contrast, the significant difference was observed when the statements analyzed based on the more comprehensive FIP principles (i.e., OECD and PIPEDA). The six PIPEDA principles were statistically different between the U.S. and Canada: *Accountability*, *Consent*, *Identifying Purposes*, *Individual Access*, *Limiting Collection*, and *Limiting Use, Disclosure and Retention*. However, there were no significant differences between two countries with respect to the *Accuracy*, *Challenging Compliance, Openness*, and *Safeguards* principles. Furthermore, only the *Security Safeguards* principle was significantly different between less information-sensitive industries and more information-sensitive industries. Interestingly, while the difference with the *Security/Integrity* principle in the FTC was only observed in the Canada, the difference with the *Safeguards* principle in the PIPEDA was found in the U.S.

Fourth, the analysis of the individuals' importance ratings of OECD principles reveals that respondents indicated *Security Safeguards* and *Use Limitation* as the two most important OECD principles whereas *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.

Finally, partly consistent with Earp et al. [6], we found a difference in the perceived importance of OECD principles

between individuals and companies. OECD principles that respondents perceived as the most important were not incorporated in companies' privacy policy statements in less information-sensitive industries, but an important OECD principle (i.e., *Security Safeguards*) that is the most central to customers was frequently addressed in companies' privacy policy statements in more information-sensitive industries.

The growing concerns of customers are resulting in companies paying increased attention to privacy. 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 are also required to make a considerable effort to satisfy customers' privacy concerns. The results of this study show that many Web sites in the U.S. and Canada were not covering all the OECD principles in their privacy policy statements. In a global marketplace, the flow of computerized information goes beyond borders and creates individuals' privacy concerns connected with this transborder data flow. Therefore, companies need to take a proactive approach toward developing more comprehensive privacy policy statements beyond their locations, and thus build consumer trust.

The results of this study also indicate that companies' privacy policy disclosures differ between the U.S. and Canada. Companies in Canada addressed more OECD principles in their privacy policy statements than those in the U.S. As mentioned previously, Canada has enacted privacy legislation (i.e., PIPEDA) that plays an important role in protecting privacy whereas the U.S. has taken a more liberal industry self-regulation approach. Our results suggest that government intervention (e.g., privacy legislation) may lead to reasonably high privacy policies without regulatory intervention. Furthermore, our additional analyses using two other FIPs (i.e., FTC fair information practices and PIPEDA) support the role of government intervention, indicating that the more comprehensive FIPs (i.e., OECD and PIPEDA) lead more privacy policy disclosures than the less comprehensive FIP (i.e., FTC fair information practice). However, caution must be exercised when interpreting this finding since it is based on 136 large Web sites from two countries. Additional research should be conducted to confirm this finding by analyzing various companies from several countries.

Prior research has shown that by posting a privacy policy statement on their Web sites, companies can reduce customers' privacy concerns about providing personal information [18, 34]. However, the results of this study reveal that important companies' privacy practices that individuals want to know are not sufficiently addressed in companies' privacy policy statements. It is consistent with prior studies suggesting that privacy policy statements are often written in such a way to protect companies from privacy litigations because companies, in general, desire to be legally protected from potential lawsuits [6, 35, 36]. In other word, privacy policy disclosures serve as legal protection for companies more than they protect customer privacy, and thus their privacy policy statements do not adequately address individuals' privacy concerns. If companies' privacy policy statements fail to provide information that individuals want to know, it likely leads to customers' privacy concerns and reduces consumer trust in online transactions, and may eventually jeopardize the proliferation of e-commerce. Therefore, companies need to respond effectively to customers' privacy concerns.

According to the results, individuals' perceived important privacy policies 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 behavior. 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 their privacy policy statements, and thus they can reduce their customers' privacy concerns and build customer trust.

Furthermore, companies must be able to ensure that they not only has implemented effective privacy policies, but is also abiding by those policies. For companies, it is relatively easy to address the FIP principles in their privacy policy statements. However, for individuals, it is difficult to detect whether companies provide appropriate privacy policies and whether companies' privacy practices comply with their privacy policies. Hence, to satisfy customers' privacy concerns, it is important for companies not only to establish an effective approach designing appropriate and accurate privacy policies, but also to provide a means that individuals feel confident of companies' privacy practices.

VII. Conclusions and Limitations

As with any study, there are several limitations in this study. First, the 136 sample Web sites consist of top 68 Web sites each from the U.S. and Canada. Since 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. Future research should include medium and small companies. Furthermore, 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.

Second, the results of the study indicate the difference in companies' privacy policy disclosures between the U.S. and Canada. However, the study did not provide an answer to the question of why this difference is present. Is it due to cultural factors or risks such as legal risk (e.g., lawsuit from customers) and government intervention? Additional research is needed to address this matter. In addition, OECD principles were used to compare companies' privacy policies between the U.S. and Canada, and additional analyses were conducted using two other FIPs (i.e., FTC fair information practice and PIPEDA). Nevertheless, the results of this study cannot be used for generalizing to other FIPs. Future research

could verify the findings of this study by using various FIPs such as EU Directive (EU) and GAPP (AICPA/CICA).

Third, the respondents of the Internet privacy user survey were all college students and from one 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 higher level 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 the adequate 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.

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 present. A thorough investigation of this matter is needed.

Despite the limitations mentioned earlier, we believe that the results of this study broaden our understanding of companies' privacy policy disclosures and what privacy practices individuals want to see in companies' privacy policy disclosures. 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.

REFERENCES

[1] M. J. Culnan, "Protecting privacy online: Is self-regulation working?," *Journal of Public Policy & Marketing,* vol. 19, no. 1, pp. 20-26, Spring, 2000.

[2] B. Shapiro, and C. R. Baker, "Information technology and the social construction of information privacy," *Journal of Accounting and Public Policy,* vol. 20, no. 4, pp. 295-322, Winter, 2001.

[3] M. J. Culnan, and P. K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science,* vol. 10, no. 1, pp. 104-115, January, 1999.

[4] J. B. Earp, and D. Baumer, "Innovative Web use to learn about consumer behavior and online privacy," *Communications of the ACM,* vol. 46, no. 4, pp. 81-83, April, 2003.

[5] K. B. Sheehan, and M. G. Hoy, "Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing,* vol. 19, no. 1, pp. 62-73, Spring, 2000.

[6] J. B. Earp, A. I. Anton, L. Aiman-Smith *et al.*, "Examining Internet privacy policies within the context of user privacy values," *IEEE Transactions on Engineering Management,* vol. 52, no. 2, pp. 227-237, May, 2005.

[7] AICPA/CICA. "Generally accepted privacy principles: A global privacy framework," April 3, 2007; http://infotech.aicpa.org/NR/rdonlyres/49B27EE4-4A2A-4EAF-A2A5-83067F32CE43/0/GAPP_Business_092006.pdf.

[8] Organization for Economic Cooperation and Development (OECD). "OECD guidelines on the protection of privacy and transborder flows of personal data," April 20, 2005; http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[9] J. F. George, "The theory of planned behavior and Internet purchasing," *Internet Research-Electronic Networking Applications and Policy,* vol. 14, no. 3, pp. 198-212, July, 2004.

[10] T. R. Graeff, and S. Harmon, "Collecting and using personal data: Consumers' awareness and concerns," *The Journal of Consumer Marketing,* vol. 19, no. 4, pp. 302-318, July, 2002.

[11] J. Phelps, G. Nowak, and E. Ferrell, "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing,* vol. 19, no. 1, pp. 27-41, Spring, 2000.

[12] M. S. Desai, T. C. Richards, and K. J. Desai, "E-commerce policies and customer privacy," *Information Management & Computer Security,* vol. 11, no. 1, pp. 19-27, March, 2003.

[13] C. Liu, and K. P. Arnett, "An examination of privacy policies in fortune 500 web sites," *Mid-American Journal of Business,* vol. 17, no. 1, pp. 13-21, Spring, 2002.

[14] G. R. Milne, and M. J. Culnan, "Using the content of online privacy notices to inform public policy: A longitudinal analysis of the 1998-2001 U.S. web surveys" *Information Society,* vol. 18, no. 5, pp. 345-359, October-December, 2002.

[15] K. L. Hui, H. H. Teo, and S. Y. Lee, "The value of privacy assurance: An exploratory field experiment," *MIS Quarterly,* vol. 31, no. 1, pp. 19-33, March, 2007.

[16] A. D. Miyazaki, and S. Krishnamurthy, "Internet seals of approval: Effects on online privacy policies and consumer perceptions," *Journal of Consumer Affairs,* vol. 36, no. 1, pp. 28-49, June, 2002.

[17] T. T. Moores, "Do consumers understand the role of privacy seals in e-commerce?," *Communications of the ACM,* vol. 48, no. 3, pp. 86-91 March, 2005.

[18] J. W. Palmer, J. P. Bailey, and S. Faraj, "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,* vol. 5, no. 3, March, 2000.

[19] N. E. Bowie, and K. Jamal, "Privacy rights on the Internet: Self-regulation or government regulation?," *Business Ethics Quarterly,* vol. 16, no. 3, pp. 323-342, July, 2006.

[20] D. O. Stephens, "Protecting personal privacy in the global business environment," *Information Management Journal,* vol. 41, no. 3, pp. 56-59, May/June, 2007.

[21] R. Sarathy, and C. J. Robertson, "Strategic and ethical considerations in managing digital privacy," *Journal of Business Ethics,* vol. 46, no. 2, pp. 111-126, August, 2003.

[22] Federal Trade Commission (FTC), *Self-Regulation and Privacy Online: A Report to Congress* Washington, DC, 1999.

[23] D. Schoder, and P. L. Yin, "Building firm trust online," *Communications of the ACM,* vol. 43, no. 12, pp. 73-79, December, 2000.

[24] M. S. Ackerman, L. F. Cranor, and J. Reagle, "Privacy in e-commerce: Examining user scenarios and privacy preferences." pp. 1-8.

[25] H. J. Smith, *Managing Privacy: Information Technology and Corporate America*, Chapel Hill: University of North Carolina Press, 1994.

[26] S. J. Milberg, H. J. Smith, and S. J. Burke, "Information privacy: Corporate management and national regulation," *Organization Science,* vol. 11, no. 1, pp. 35-57, January-February, 2000.

[27] G. R. Milne, and M.-E. Boza, "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of Interactive Marketing,* vol. 13, no. 1, pp. 5-24, Winter, 1999.

[28] R. D. Petty, "Marketing without consent: Consumer choice and costs, privacy, and public policy," *Journal of Public Policy & Marketing,* vol. 19, no. 1, pp. 42-53, Spring, 2000.

[29] R. K. Chellappa, and R. G. Sin, “Personalization versus privacy: An empirical examination of the online consumer's dilemma,” *Information Technology and Management,* vol. 6, no. 2-3, pp. 181-202, April, 2005.

[30] AICPA/CICA. "AICPA/CICA privacy framework," April 10, 2005; http://www.cica.ca/multimedia/Download_Library/Research_Guidance/Privacy/English/PrivacyFramework0304.pdf.

[31] P. Ashley, C. Powers, and M. Schunter, "From privacy promises to privacy management: A new approach for enforcing privacy throughout an enterprise." pp. 43-50.

[32] Federal Trade Commission (FTC), *Privacy online: Fair information practices in the electronic marketplace - A report to Congress*, Washington, DC, 2000.

[33] Mergent Online. "About mergent online," May 29, 2008; http://www.mergentonline.com/noticesCM.asp?contentscode=About.

[34] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior." pp. 38-47.

[35] Z. Papacharissi, and J. Fernback, “Online privacy and consumer protection: An analysis of portal privacy statements,” *Journal of Broadcasting & Electronic Media,* vol. 49, no. 3, pp. 259-281, September, 2005.

[36] I. Pollach, “What's wrong with online privacy policies?,” *Communications of the ACM* vol. 50, no. 9, pp. 103-108, September, 2007.