The Value of Online Information Privacy: Evidence from the USA and Singapore

Il-Horn Hann*, Kai-Lung Hui, Tom S. Lee**, and I.P.L. Png****

October 2002

Abstract

Concern over online information privacy is widespread and rising. However, prior research is silent about the value of information privacy in the presence of potential benefits from sharing personally identifiable information. We analyzed individuals' trade-offs between the benefits and costs of providing personal information to websites. We found that benefits – monetary reward and future convenience – significantly affect individuals' preferences over websites with differing privacy policies. We also quantified the value of website privacy protection. Among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62. Finally, we identified three distinct segments of Internet consumers – privacy guardians, information sellers, and convenience seekers.

* Marshall School of Business, University of Southern California; ** Department of Information Systems, National University of Singapore. We acknowledge financial support from the Carnegie Bosch Foundation, GSIA, Carnegie Mellon University. We thank Teck H. Ho, and 2002 International Conference on Information Systems referees for valuable comments.

Introduction

Privacy has been identified to be a major, if not the most critical, impediment to e-commerce: "In our view, the single, overwhelming barrier to rapid growth of e-commerce is a lack of consumer trust that consumer protection and privacy laws will apply in cyberspace. Consumers … worry, deservedly, that supposedly legitimate companies will take advantage of them by invading their privacy to capture information about them for marketing and other secondary purposes without their informed consent" (U.S. Public Interest Research Group 2000).

Even before the advent of e-commerce, there was broad concern about collection of personal information in various contexts, including employment, retailing and direct marketing, and government. These concerns prompted government action. In 1974, the U.S. Congress passed the Privacy Act to regulate government collection and use of personal information.[1] In 1980, the Organization for Economic Co-operation and Development published guidelines for the collection and use of personal information by government and private organizations (OECD 1980). Further, in 1995, the European Union adopted a data protection directive that regulates information within and beyond the Union (European Union 1995). The directive disallows transfer of information to other countries that do not provide adequate protection.

Rapid improvements in computing technologies and the advent of e-commerce have amplified public concern about privacy, especially on electronic networks. With every website visit, a browser leaves an electronic trace which can later be retrieved and analyzed. Combined with technology to store identifying information (cookies), website operators can profile browsers to an unprecedented degree and subsequently merge these profiles with other demographic data. Such an enriched data set can then

[1] Specifically, the Privacy Act of 1974 prohibits unauthorized disclosures of records and gives individuals the right to review records about themselves to check whether records have been disclosed and to request corrections or amendments.

be used by the company or sold to other parties.[2] This information could benefit the customer by more precisely identifying her need. However, it could also be used to her detriment. For example, Amazon.com was suspected of engaging in differential pricing based on prior shopping information and other customer demographics for the sales of DVDs.[3] Westin (2001) concludes: "There has been a well-documented transformation in consumer privacy attitudes over the past decade, moving concerns from a modest matter for a minority of consumers in the 1980s to an issue of high intensity expressed by more than three-fourth of American consumers in 2001".

Despite the passage of new legislation, including the 1998 Children's Online Privacy Protection Act, which regulates the online collection and use of children's personal information, there continues to be public pressure for increased regulation. Over fifty bills to regulate online privacy were introduced in the first session of the 107th Congress. Industry, however, is resisting the proposals to tighten regulation. The national cost of complying with these legislative proposals has been estimated to be US$9-36 billion (Hahn 2001). For just catalog and Internet clothing retailers, a study sponsored by the Direct Marketing Association estimated that opt-in restrictions to use of demographic information by third parties would raise costs by US$1 billion (Turner 2001).

The conflict between privacy advocates and industry motivates our research objective: Exactly how much do individuals perceive to be the cost of releasing personal information online? The real policy issue is not whether consumers value online privacy. It is obvious that people value online privacy. What is not known is how *much* people value online privacy and the extent to which people *differ* in their valuations. Despite tremendous debate and policy interest, there has, to date, been no research

[2] *New York Times*, "Giving the Web a Memory Cost Its Users Privacy," September 4, 2001.

[3] Amazon has subsequently apologized for charging different prices and refunded an average of $3.10 to each of 6,896 customers who bought a DVD. These consumers paid between 25-66 percent more than the lowest available price. While it has been speculated that Amazon engaged in price discrimination, Amazon claimed that these were 'random' tests. (http://www.internetnews.com/ec-news/article.php/4_471541, September 28, 2000)

into this question (Hahn 2001). Indeed, it has been conjectured that "measuring the value of consumer privacy may prove to be intractable" (Ward 2001).

Businesses need to know the value of privacy in deciding whether to invest in privacy seals and what incentives to offer consumers for their personal information. Governments need this information to decide on public policy towards information privacy. For instance, Laudon (1996) and Varian (1997) have proposed to regulate privacy through markets in personal information. But the economic viability of such markets depends on individuals' perceived value of privacy.

In this study, we applied conjoint analysis, which is the standard way of measuring consumer trade-offs (Green and Srinivasan 1990; Wittink and Cattin 1989), to subjects' rankings of alternative combinations of benefits and privacy protection in an online setting. The benefits were monetary reward and future convenience, while the privacy protection applies to errors in storing or processing personal information, unauthorized secondary use of information, and improper access to information.[4] This allows us to make the following contributions:

First, the conjoint analysis showed that the benefits had a significant effect on our subjects' preferences.

Second, by comparing the value of protection on the three privacy concerns with the value of monetary reward, we provide first- estimates of the monetary value of privacy protection in the United States.

Last, by applying cluster analysis to the subjects' marginal rankings of the various benefits and concerns, we found that our subjects could be categorized into three distinct segments – privacy guardians, information sellers, and convenience

[4] The objective of this research certainly fits within Wittink's (2001) "Encapsulation Model" in which business school research must have real-world relevance.

seekers. The majority of subjects were relatively sensitive to online information privacy concerns (“privacy guardians”). By contrast, a smaller proportion were relatively willing to provide information in exchange for money (“information sellers”), and an even smaller proportion were relatively willing to provide information in exchange for convenience (“convenience seekers”).

All of the preceding results were robust in the sense that they held in both the U.S. and Singapore samples. Our results contribute directly to the public policy debate over whether online privacy protection is worth its cost to industry. They also inform businesses whether to invest in privacy seals and what incentives to offer consumers for their personal information.

The remainder of this paper is organized as follows. We provide an overview of the relevant literature and our research questions in Section 2. The experimental procedure is explained in Section 3. Section 4 describes the results of the conjoint analysis and estimates the dollar value of privacy protection. Section 5 reports the results of the cluster analysis. Section 6 discusses limitations and directions for future research. Section 7 concludes with implications for public policy and business strategy.

Literature Review and Research Questions

Information privacy has been defined as “the claim of individuals … to determine for themselves when, how, and to what extent information about them is communicated to others” (Westin 1967, page 7). Control over the communication and use of personal information is a key dimension of privacy that has been emphasized by researchers in diverse disciplines (see, e.g., Goodwin 1991; Schwartz 2000; Smith et al. 1996; Stone and Stone 1990).

Empirical research has repeatedly shown information privacy to be of utmost concern in diverse organizational and marketing contexts (Esrock and Ferre 1999;

Hoffman et al. 1999; Phelps et al. 2000; Stone et al. 1983). With rapid advances in information technology, consumer surveys report rising concern over the proper handling and usage of personal information (Cranor et al. 1999; Culnan and Milne 2001; Katz and Tassone 1990). Harper and Singleton (2001), however, argue that most surveys exaggerate privacy concerns: in unprompted surveys, information privacy did not appear to be of top priority to individuals.

What factors underlie individuals' concern over privacy? Concern has been related to cultural values and regulatory preferences (Milberg et al. 1995, 2000; Smith 2001). Further, perceptions of privacy invasion depend on information control, outcomes due to disclosures, information type and sensitivity, perceived relevancy of information use, and target of disclosures (Eddy et al. 1999; Stone et al. 1983; Tolchinsky et al. 1981; Woodman et al. 1982). More importantly, individuals' perceived degree of privacy and information control affect their subsequent attitudes, intentions, and actual behavior. Specifically, if subjects believe that their privacy interest was protected, they are more willing to disclose personal information or enter into a long-term relationship with the information collector (Culnan 1993; Culnan and Armstrong 1999; Hoffman et al. 1999; Phelps et al. 2000).

While individuals are concerned about the communication and use of their personal information, this information can be used to allocate scarce resources more efficiently (Posner 1981; Stigler 1980).[5] Specifically, in the context of e-commerce, retailers and service providers can use personally identifiable information to better meet consumer needs, increase efficiency and lower prices, provide greater convenience, and expand access to products and services (Cate and Staten 1999). Indeed, Culnan and Milberg (1999) christen consumers' exchange of information for enhanced service and

[5] An often-cited example is the labor market. Job seekers prefer to hide prior history of termination from employment, illness, or criminal behavior, but employers seek such information to make optimal employment decisions.

better deals as the "second exchange" that follows the "first exchange" of a good or service for money.

Sociological research suggests that individuals perform a privacy calculus, assessing the cost and benefit of providing information. The calculus depends on factors including self-ego, environmental stimuli, and interpersonal relationships (Laufer and Wolfe 1977; Stone and Stone 1990). Accordingly, concern over information privacy might be mitigated by sufficient positive reinforcement. Such a compensative reinforcement hypothesis is consistent with sociological and economic exchange theories, and the social penetration theory of interpersonal relationships (Taylor et al. 1969; Taylor and Altman 1975).

Anecdotal evidence suggests that people are willing to disclose personal information for gifts and catalogs (Oberndorf 1999; S. Schwartz 2000). In a recent survey, 82 percent of online consumers reported that they would provide personal information to new retail websites in exchange for a $100 drawing (Jupiter Media Metrix 2002). Further, compensation received the highest weight in a conjoint analysis of the factors influencing participation in direct mail (Milne and Gordon 1993).[6]

All the foregoing evidence supports the proposition that individuals respond to benefits in deciding whether to disclose personal information to websites.[7] This motivates our primary set of research questions: Do individuals' preferences over disclosing personal information systematically depend on benefits such as monetary reward and convenience? If so, how do the preferences vary with the benefits? Further, can we quantify the dollar value of privacy protection?

[6] Milne and Gordon's conjoint task involved trade-offs among compensation, targeting, volume, and permission. These dimensions, however, do not clearly represent positive or negative consequences of revealing personal information. Hence, their results do not address individuals' willingness to exchange personal information for positive reinforcement.

[7] Among critics of privacy protection, such as Harper and Singleton (2001), the rapid adoption of B2C commerce suggests that privacy concerns are either overstated or outweighed by countervailing benefits.

Prior research suggests that individuals differ in their sensitivity towards disclosure of personal information, and that their preferences vary with personal and environmental factors (Hoffman et al. 1999; Laufer and Wolfe 1977; Stone and Stone 1990). However, with the exception of opinion surveys dividing the U.S. population into a majority of "privacy pragmatists", and minorities of "privacy fundamentalists" and "privacy unconcerned" (Westin 2001), these propositions have not been verified empirically. This motivates our secondary set of research questions: Do individuals systematically *differ* in their trade-off between benefits of disclosing personal information and privacy concerns? If so, to what extent can we explain these differences?

Experimental Procedure

To address our primary set of research questions, we employed the technique of conjoint analysis. This technique presents test subjects with a set of alternatives (stimuli). Each stimulus consists of particular levels of various dimensions. The subject is asked to rank the stimuli according to her own preferences. Conjoint analysis assumes that the individual's ranking of each stimulus can be decomposed into the sum of contributions from the multiple dimensions. For each dimension, the contribution is the *part-worth* multiplied by the level of that dimension. Essentially, the part-worth is the marginal utility of the dimension in the individual's ranking of the conjoint stimuli.

To keep the conjoint tasks to a manageable size, Green and Srinivasan (1990) recommend that the number of attributes be limited to six or fewer. Following Green and Krieger (1991), we conducted focus groups prior to the conjoint study. Specifically, we conducted three focus group discussions with upper-division undergraduate and graduate students in the United States and Singapore to identify the key benefits that they expected from registration with websites and suitable attribute levels.

The focus groups suggested that individuals clearly value direct monetary savings. In addition, they also identified convenience as another important benefit of providing personal information to a website. The focus groups identified two sources of convenience benefits – the explicit time saving per session and the expected visit frequency to the website. Accordingly, we operationalized convenience by "expected visit frequency/total time savings" in our conjoint experiment.[8]

Regarding the costs of privacy, we considered the four concern dimensions identified by Smith *et al.* (1996) – collection, error, unauthorized secondary use, and improper access.[9] Logically, collection is a necessary antecedent to the three other dimensions. Error, unauthorized secondary use and improper access of information can not happen without *ex ante* collection of personal information. Further, individuals' concerns on the other three dimensions are a direct function of the amount of information collected – the more information a website collects, the higher should be the concerns with error, unauthorized secondary use, and improper access of information. Therefore, it would not be appropriate to manipulate the collection of information and let subjects assess the tradeoffs between collection and other concern/benefit dimensions. Accordingly, in our conjoint analysis, we controlled for the collection of information and manipulated the other three concern dimensions.

Taken together, our conjoint study assessed trade-offs among five dimensions – two benefits and three privacy concerns. We created three treatment levels each of

[8] The subjects were told during the experiments that if they expected to visit the website daily, their average time saving over the year would be 8 hours and 20 minutes (assuming an average saving of 2 minutes per transaction, 2 minutes x 5 days a week x 50 weeks = 8 hours and 20 minutes); if they expected to visit the website weekly, the yearly saving would be 1 hour and 40 minutes; and if they expected to visit the website monthly, the yearly saving would be 24 minutes.

[9] Collection refers to the concern that "extensive amounts of personally identifiable data are being collected and stored in databases"; error refers to the concern that "protections against deliberate and accidental errors in personal data are inadequate"; unauthorized secondary use refers to the concern that "information is collected for one purpose but is used for another, secondary purpose"; improper access refers to the concern that "data about individuals are readily available to people not properly authorized to view or work with this data" (Smith et al. 1996, page 172, Table 2). These dimensions were further validated by Stewart and Segars (2002).

monetary reward ($5, $10 and $20) and visit frequency/time savings (monthly, weekly and daily).[10] The benefit levels were motivated by the focus groups. The three concerns (error, unauthorized secondary use and improper access of information) were manipulated by the presence (or absence) of proper information handling and access procedures.

Based on these five dimensions and their treatment levels, there were a maximum of 3 x 3 x 2 x 2 x 2 = 72 conjoint stimuli. To avoid asking subjects to rank too many alternatives, we selected 18 stimuli based on an optimal orthogonal design (Addelman 1962). For example, one particular stimulus was a website that provided a $5 monetary reward in return for personal information and the subject visited the website once a month with a total time savings of 24 minutes per year. Further, the website had no error correction procedure, no policies to prevent unauthorized secondary use, and no policies to prevent improper access to information. Our conjoint analysis asked subjects to rank 18 websites (stimuli), which represented different combinations of benefits and privacy protection. In order to control for industry effects, we posed the conjoint stimuli in three settings – financial, healthcare, and travel. Within each of the three industries, we controlled for the degree of information collection by telling the subjects that all 18 stimuli (that is, hypothetical websites) requested the same set of personal information from the subjects. The personal information consisted of name, home address, phone number, e-mail address, credit card information, and some industry-specific information. Specifically, travel websites requested the consumer's occupation, travel purpose, destination and frequency of travel, as well as frequent flyer numbers. Healthcare websites asked for medical history, drug allergies, and prescription record. Financial websites asked for household income, stock portfolio, and previous stock trading experience.

[10] The monetary rewards were framed in the respective local currencies. As of April 2002, one Singapore dollar = 54 US cents. Due to the currency differences, the effective ranges of monetary rewards differed between the U.S. and Singapore experiments – in US dollars, the Singapore rewards were equivalent to US$2.70, US$5.40, and US$10.80, respectively.

Each subject was randomly assigned to one of the three industry settings and asked to rank the 18 stimuli (websites) according to her own preferences. In other words, the benefit/concern dimensions were within-subject factors whereas industry was a between-subject factor. To capture the background of the experimental subjects, we also included demographic questions regarding subjects' gender, age, Internet usage and previous experience with invasion of privacy.

To strengthen the external validity of our study, we conducted the conjoint experiment in both the USA and Singapore. The U.S. subjects were upper-division undergraduate students from a major Eastern university. The Singapore sample consisted of upper-division undergraduate students enrolled in an e-commerce technologies course at a major university. Table 1 presents some descriptive statistics about our subjects.

Table 1. Descriptive Statistics

	U.S.	Singapore
Number of subjects	84	184
Percentage of females	42%	44%
Average age	24	23.1
Average Internet experience (years)	6.8	5.9
Percentage of subjects having online purchase experience	95%	61%

The experiment proceeded as follows. First, all subjects completed the demographic questions. Then, the experimental task and the meanings of the five dimensions were explained. Finally, the subjects ranked the 18 stimuli based on their personal preferences. In the U.S. sample, 84 participants completed the experiment, and, among them, 35 students received course credit, while the remainder were compensated with US$7.[11] In Singapore, 184 subjects completed the experiment and received course credit. We collected 268 responses in total.

Conjoint Analysis

The key outcome of conjoint analysis is the part-worths (marginal utilities) of the various dimensions that comprise the conjoint stimuli. To estimate the part-worths, we used least-squares regression with the subjects' rankings (from 1 to 18) as the dependent variable and indicators of the various levels of the two benefit and three privacy concern dimensions as the independent variables. Then, the coefficient of each independent variable would be the part-worth corresponding to that level of the dimension.

Further, we calculated the relative importance of each dimension as the part-worth corresponding to the maximum level of that dimension divided by the sum of the part-worths corresponding to the maximum levels of all five dimensions. We expressed relative importance as a percentage.

Table 2 reports the means of the part-worths and relative importance for the U.S. and Singapore subjects. Note that the part-worths and relative importance for the U.S. and Singapore samples are not directly comparable as the monetary rewards were framed in the respective local currencies. At the April 2002 exchange rate, the rewards specified to the Singapore subjects were equivalent to US$2.70, US$5.40, and US$10.80 respectively.

[11] We found no statistically significant difference in part-worths between those who received course credit and those compensated with US$7. Hence, we pooled both groups into a single sample.

Table 2. Part-Worths and Relative Importance

Instruments	Level	U.S.		Singapore	
		Part-Worth[+]	Relative Importance	Part-Worth[+]	Relative Importance
Monetary Reward	$5[#]	0	26.24%	0	11.69%
	$10[#]	1.327*** (0.341)		0.232 (0.165)	
	$20[#]	3.141*** (0.534)		1.388*** (0.281)	
Visit Frequency/Time Savings	Monthly	0	6.13%	0	6.02%
	Weekly	0.568** (0.260)		0.432*** (0.153)	
	Daily	0.734* (0.411)		0.715*** (0.254)	
Error	No Review	0	24.80%	0	15.06%
	Review	2.968*** (0.355)		1.787*** (0.194)	
Improper Access	No restriction	0	25.12%	0	28.43%
	Restriction	3.007*** (0.529)		3.374*** (0.349)	
Unauthorized Secondary Use	Allowed	0	17.70%	0	38.80%
	Not allowed	2.118*** (0.324)		4.605*** (0.297)	

[+] Standard errors in parentheses. The control stimulus consisted of the lowest levels of each of the included dimensions. Because the control was represented by a least squares intercept, we label all lowest level part-worths as zero. The mean intercept is not reported for brevity.

[#] US dollars for U.S. subjects and Singapore dollars for Singapore subjects.

*** significant at 1% level; ** significant at 5% level; * significant at 10% level.

We first examined whether the responses from the subjects differed across the three industries (financial, healthcare and travel). Since our U.S. and Singapore samples were relatively large, the central-limit theorem implies that the estimated part-worths for each independent variable should approximately follow a normal distribution. Based on this premise, we conducted one-way analysis of variance (ANOVA) and pairwise t-tests to compare the part-worths across the industries. The results suggested that the part-worths (or, equivalently, the subjects' preferences) were not statistically different across financial, healthcare and travel websites. Accordingly, in all subsequent analyses, we pooled the data across industries.

Next, we investigated whether the subjects' preferences over the stimuli (websites) were sensitive to monetary reward. If the part-worth for a particular level of monetary reward differs significantly from zero, then the evidence suggests that subjects are willing to trade privacy protection or convenience for that level of reward.

For the U.S. sample, the part-worth for a US$20 reward was 3.141 and was statistically significant. This means that a website offering a US$20 reward for personal information would raise its ranking by 3.141 (out of 18) as compared to an otherwise identical website offering the base level US$5 reward. Also, the part-worth for a US$10 reward was 1.327 and significant.

For the Singapore sample, the part-worth for a S$20 reward was 1.388 and was statistically significant. At the prevailing exchange rate, S$20 was equivalent to US$10.80, hence it was not surprising that the part-worth was much less than the US$20 part-worth in the U.S. sample (3.141). Interestingly, the S$20 part-worth among Singapore subjects (1.388) was very close to the US$10 part-worth among U.S. subjects (1.327). This result arose even though the base-level rewards were different in the two samples (S$5 and US$5 respectively).

The part-worth for a S$10 reward in the Singapore sample was 0.232 but not statistically significant. Apparently, the subjects were willing to trade away privacy protection or convenience only when the monetary reward exceeded a threshold, which lay between S$10-20 (US$5.40 – 10.80).

Taken together, the results from the U.S. and Singapore samples suggest that a sufficiently large monetary reward did significantly increase the relative attractiveness of a website independent of its privacy policy. Further, when the monetary reward was relatively low (as in the Singapore sample), the marginal utility of the reward was increasing, and when the monetary reward was relatively high (as in the U.S. sample), the marginal utility tended to decrease. These results indicate that the attractiveness of a monetary reward relative to privacy protection or convenience might follow the "S"-shape as shown in Figure 1. The results are consistent with economic analysis that utility functions tend to be non-concave (Friedman and Savage 1948; Hartley and Farrell 2002).

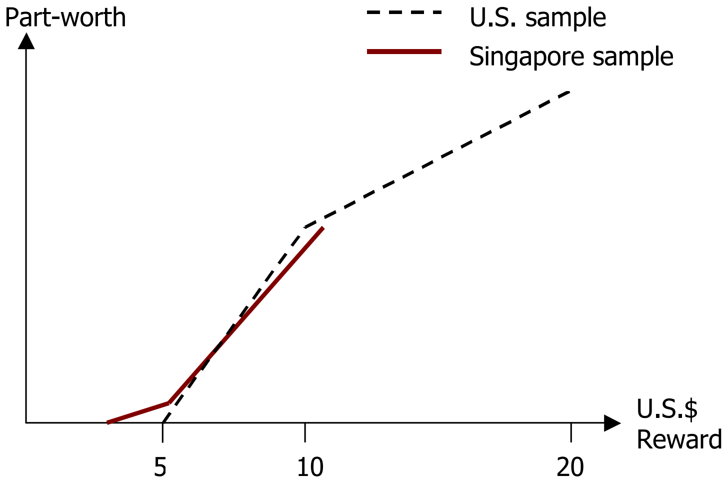

Figure 1. Part-Worths for Monetary Reward

We can use these results to calculate the marginal utility of a one-dollar reward. Referring to Table 2, in the U.S. sample, between the US$5 and US$10 rewards, the US$5 increase raised the ranking by 1.327, or 0.265 per dollar of reward. Alternatively, between the US$10 and US$20 rewards, the US$10 increase raised the ranking by 3.141 – 1.327 = 1.814, or 0.181 per dollar of reward. These two estimates provide a range of 0.181 – 0.265 per U.S. dollar of reward.[12]

[12] Between the US$20 and US$5 rewards, the US$15 increase raised the ranking by 3.141, or 0.210 per dollar of reward, which is within the range of 0.181 – 0.265 calculated using the other reward differences.

Again, referring to Table 2, in the Singapore sample, the S$10 part-worth was not significantly different from zero. Accordingly, we focus on the S$20 part-worth. Between the S$5 and S$20 rewards, the S$15 increase raised the ranking by 1.388, which amounted to 0.0925 per (Singapore) dollar of reward or 0.171 per U.S. dollar of reward. This was quite remarkably close to the range (0.181 – 0.265 per U.S. dollar of reward) that we found among U.S. subjects.

Having studied the subjects' sensitivity to monetary reward, we next investigated their sensitivity to convenience, as operationalized by visit frequency/time savings. Referring to Table 2, in the U.S. sample, the part-worth for weekly visit was significant at the 5% level, but the part-worth for daily visit was significant only at the 10% level. Further, the part-worths for weekly and daily visits were not significantly different. In the Singapore sample, the part-worths for visit frequency/time savings were generally more significant. However, as with the U.S. subjects, the effect due to weekly visit was not significantly different from that due to daily visit.

From the results of both samples, we conclude that there is some evidence that subjects are sensitive to convenience. The evidence is stronger among Singapore subjects than U.S. subjects. Further, once the subjects expected to visit a certain website sufficiently frequently (at least once a week), more frequent visits did not seem to affect the subjects' preferences.

The part-worths and relative importance associated with visit frequency/time savings among U.S. and Singapore subjects were very close. In both samples, these were much lower than the part-worths and relative importance for the other dimensions. Apparently, among our subjects, convenience was only a minor factor when evaluating websites. By contrast, monetary reward and privacy protection were perceived to be much more important.

Referring to Table 2, the part-worths for protection against all three privacy concerns were statistically significant at the 1% level in both samples. Among U.S. subjects, the part-worth for review (which enabled an individual to correct errors in his/her personal information) was 2.968. This indicated that a website could raise its ranking by 2.968 (out of 18) by letting customers review and edit their personal information. The part-worth for restricting improper access was 3.007, while that for disallowing unauthorized secondary use was 2.118.

Among Singapore subjects, the part-worths for error review and editing, restricting improper access, and disallowing unauthorized secondary use were 1.787, 3.374 and 4.604 respectively.

Comparing the part-worths between countries, we found that, consistent with previous research (Esrock and Ferre 1999; Milberg et al. 1995), Singapore subjects were relatively more concerned about improper access and unauthorized secondary use than errors in storing information. However, the U.S. subjects exhibited less concern for unauthorized secondary use than errors in storing information. Despite the discrepancy in relative preferences toward the different privacy protections across the two samples, our conjoint experiment confirmed previous findings that individuals are highly concerned about information privacy, and they value protective measures (Culnan and Armstrong 1999).

Finally, using the marginal utilities of a dollar reward and the part-worths for privacy protection, we estimate the value of protection, on a per-subject basis, for each of the three privacy concerns. Recall that we estimated the marginal utility of a US$1 reward to be 0.181 – 0.265 among the U.S. subjects. By Table 2, the part-worth for review and editing of information was 2.968. Using the lower bound for the marginal utility (0.181 per dollar), the value of review and editing of information is 2.968/0.181 = US$16.40. Using the upper bound for the marginal utility (0.265 per dollar), the value is 2.968/0.265 = $11.20.

We can use the same method to derive the values of protecting against improper access and unauthorized secondary use. The results are reported in Table 3. We also computed the values for the Singapore subjects using the marginal utility of 0.171 per U.S. dollar.

Table 3. Value of Privacy (in U.S. dollars)

Website privacy policy	Value	
	U.S.	Singapore
Review for error	$ 11.18 - 16.36	$ 10.45
Restriction against improper access	$ 11.33 - 16.58	$ 19.73
Secondary use not allowed	$ 7.98 - 11.68	$ 26.93

Generally, our results in Table 3 suggest that websites might need to offer substantial monetary incentives to overcome individuals' concerns about error, improper access, and unauthorized secondary use of information. Among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62.

Cluster Analysis

To address our secondary set of research questions – whether individuals systematically *differ* in their trade-off between benefits of disclosing personal information and privacy concerns, we applied cluster analysis (Green and Krieger 1991; Vriens et al. 1996). This technique groups subjects into distinct segments according to the similarity of their estimated part-worths for the various dimensions. In the present case, we apply cluster analysis to segment the subjects according to their estimated part-worths over the various benefits and dimensions of privacy protection. [13]

[13] In the case of monetary reward and visit frequency/time savings, we used the maximum part-worths -- $20 monetary reward and daily frequency respectively.

Specifically, we applied hierarchical cluster analysis using average between-group linkage with (dis)similarity measured by the squared Euclidean distance to both the U.S. and Singapore samples. The hierarchical method was preferred because we had no *a priori* information on the number of clusters and initial cluster seeds/centers (Hair et al. 1998, pp. 493 - 498). We used a distance measure for (dis)similarity as all the part-worths (the inputs to the cluster analyses) were derived from a common scale, the website rankings.

For each sample, we began the analysis with every subject constituting a separate cluster. We then examined the percentage drops in the similarity coefficient as clusters were progressively merged. In both the U.S. and Singapore samples, we stopped at three clusters as further combination of any two clusters resulted in a sharp drop in similarity, a stopping rule recommended by Hair et al. (1998, pp. 499). Table 4 reports the three clusters and the respective mean part-worths. A small number of subjects could not be classified into any of the three clusters. We excluded these observations from subsequent analysis and discussion.[14]

Table 4. Clusters

Segment (no. of observations)		Average part-worth				
		Monetary reward	Visit Frequency/ Time Savings	Error	Unauthorized Secondary Use	Improper Access
U.S. (78) $^{+}$	Privacy guardians (56)	1.637*** (0.385)	0.027 (0.316)	4.040*** (0.434)	2.576*** (0.448)	5.116*** (0.519)
	Information sellers (16)	10.865*** (0.330)	-0.781 (0.753)	0.245 (0.458)	1.255** (0.483)	-0.099 (0.462)
	Convenience seekers (6)	1.445 (0.781)	11.028*** (0.613)	1.500** (0.348)	0.750* (0.371)	0.542 (0.945)
Number of outliers/unclassifiable observations: 6						

[14] Some of these outliers formed small (one- or two-member) clusters that we could not interpret. Several subjects exhibited unusual preferences such as preferring improper access to personal information. They possibly misunderstood the experimental tasks. The outliers constituted 7% and 10% of the U.S. and Singapore samples respectively.

Singapore (165) [+]	Privacy guardians (138)	0.464^{**} (0.195)	0.089 (0.166)	2.234^{***} (0.183)	5.734^{***} (0.318)	4.973^{***} (0.314)
	Information sellers (14)	11.286^{***} (0.360)	-0.714 (0.855)	0.107 (0.263)	1.768^{***} (0.434)	0.446 (0.470)
	Convenience seekers (13)	1.127 (0.862)	10.512^{***} (0.682)	0.404 (0.372)	1.077^{**} (0.484)	0.173 (0.382)
Number of outliers/unclassifiable observations: 19						

[+] Number excluding outliers.
*** significant at 1% level; ** significant at 5% level; * significant at 10% level.
standard errors in parentheses.

Consistent across the two samples, the majority of the subjects formed a cluster that could be characterized by a high value on information privacy. Specifically, 72% of the U.S. subjects and 84% of the Singapore subjects exhibited relatively high part-worths for protection against error, improper access, and unauthorized secondary use of their personal information. By contrast, their part-worths on monetary reward and visit frequency/time savings were relatively low. We label this group of subjects as "privacy guardians" – people who attach a relatively high value to information privacy.

The next largest cluster consisted of subjects who attached a relatively high value to monetary reward. We call them "information sellers", as they tend to "sell" personal information with little regard for convenience (visit frequency/time savings) or website privacy policies.

The smallest cluster comprised subjects who focused exclusively on convenience (operationalized by visit frequency/time savings). In fact, their part-worths for visit frequency/time savings were so high that their preferences over alternative websites could almost be predicted by visit frequency/time savings alone. We call these subjects "convenience seekers" – people who prefer convenience with little regard for money or website privacy policies.

Across the three clusters, we observe very different attitudes toward benefits and privacy. The privacy guardians prefer protection, but they still value monetary reward (the mean part-worth for monetary reward was significantly different from zero). Only the convenience seekers value convenience; for all other clusters, the part-worths for visit frequency/time savings were insignificant.[15] Among the three privacy concerns, only unauthorized secondary use was significant in all three clusters.

Based on opinion surveys, Westin (2001, pp. 16) characterized 12% of the U.S. population as being "privacy unconcerned": "for 5 cents off, they will give you any information you want about their family, their lifestyle, their travel plans, and so forth". Interestingly, we found that 12.5% of the U.S. sample were "information sellers". However, our evidence is that information sellers demand a great deal more than "5 cents off." Indeed, this point distinguishes our analysis from opinion surveys: we can estimate the dollar amount that information sellers must be paid for their information.

Further, our analysis revealed a cluster that Westin (2001) did not identify. This cluster consisted of convenience seekers, people who would "sell" their personal information for convenience rather than money. Finally, among the remainder of the U.S. population, Westin (2001) differentiated between "privacy pragmatists" (63%) and "privacy fundamentalists" (25%) according to their sensitivities to privacy, while our cluster analysis did not find such a distinction. We did detect some evidence among the U.S. subjects that the privacy guardians could be further segmented, with each sub-segment placing relatively greater weight on one of the three privacy concerns.

Having identified three clusters, we investigated whether cluster membership depended systematically on particular demographic variables. We first sought systematic differences between information sellers and privacy guardians. Among the U.S. subjects, we found that information sellers had significantly more prior experience of

[15] Interestingly, our finding that the subjects were sensitive to convenience seems to be due solely to the convenience seekers.

providing personal information to websites than privacy guardians (t = 3.115, p < 0.01). The information sellers' greater prior experience was consistent with their relatively high part-worths for money. However, among the Singapore subjects, there was no significant difference between information sellers and privacy guardians in terms of prior experience of providing personal information to websites.

We next investigated systematic differences between convenience seekers and privacy guardians. Among the U.S. subjects, convenience seekers were much more accepting of cookies than privacy guardians (t = 4.282, p < 0.001). Specifically, the convenience seekers were less concerned about cookies, and they typically accepted all cookie manipulations from websites without warning. By contrast, the majority of the privacy guardians requested to be warned about cookies. Many of them even configured their browsers to reject all cookies. The convenience seekers' greater acceptance of cookies was consistent with their relatively high part-worths for visit frequency/time savings.

Among the Singapore subjects, the convenience seekers were also less concerned about the use of cookies than the privacy guardians (t = 6.954, p < 0.001). This result was consistent with the preferences of the U.S. sample.

Overall, we found some evidence that information sellers had more prior experience of information provision than privacy guardians, and strong evidence that convenience seekers were more accepting of cookies than privacy guardians.

Policy and Business Implications

We now address the key public policy issue – whether the benefit of increased privacy regulation justifies the cost. In the United States, the national cost of complying with various legislative proposals to increase regulation of online privacy has been estimated to be US$9-36 billion (Hahn 2001).

Referring to Table 3, we estimate that, on average, each individual values protection against errors, improper access, and secondary use of personal information at between US$30.49 – 44.62. In March 2001, an estimated 58 million Americans made a purchase over the Internet (Horrigan and Rainie 2002). Based on the number of purchasers, we estimate the benefit of privacy protection to be US$1.77 – 2.59 billion, which falls quite far short of Hahn's (2001) cost estimates.[16] This estimate is conservative, hence *understates* the value of privacy protection for several reasons. Stronger privacy legislation might raise consumer participation in Internet commerce, hence generating additional benefit. Further, our calculation assumes that each consumer provides information to just one website. To the extent that they provide information to multiple websites, the value of privacy protection would be greater.

Our results also address another public-policy issue – the viability of proposals to regulate privacy through markets (Laudon 1996; Varian 1997). Given that that individuals' concern for privacy is not absolute, but rather can be traded off against benefits such as money and convenience, we conclude that market solutions may well be viable.

As for business implications, we identified three distinct segments – privacy guardians, information sellers, and convenience seekers – in terms of individual trade-offs between the benefits of disclosing personal information and privacy concerns. The immediate implication is that e-commerce providers must differentiate their services to serve these distinct segments. Just as an auto manufacturer makes differentiated models for various segments, an e-commerce provider must differentiate its services to best meet the needs of segments with differing trade-offs among money, convenience, and privacy concerns.

[16] If each person values privacy at US$30.49, then 58 million persons would value privacy at a total of 58 x 30.49 = US$1,768 million or approximately US$ 1.77 billion. Similarly, if we use the higher estimate of the value of privacy (US$44.62), the value of privacy to the entire population is US$2.59 billion.

Convenience seekers will be the first to register with a website if it simplifies web site navigation or enables personalized content. Businesses can exploit this by offering them the opportunity to provide personal information to customize the web site and simplify the shopping experience.

Information sellers are distinguished from privacy guardians by prior experience of information provision. This customer type cannot be lured to provide personal information by offering them convenience. To the extent that businesses cannot observe a consumer's prior experience, they must use *indirect* methods to induce segmentation by self-selection (Bhargava and Choudhary 2002; Moorthy 1984; Png 2002, Chapter 9). Businesses could use monetary rewards to attract information sellers to provide personal information. Preferably, businesses would seek convenience seekers first before enticing information sellers.

By elimination, the consumers who do not respond to either monetary reward or convenience would be privacy guardians.   Businesses would need to use other strategies, such as privacy seals (Benassi 1999) or procedural fairness (Culnan and Armstrong 1999), to persuade these consumers to provide their personal information.

Concluding Remarks

By applying conjoint analysis, we have shown that individuals' preferences over disclosing personal information to websites do systematically vary with monetary reward and convenience. Further, we provided the first analysis of the benefit vis-à-vis cost of increased privacy regulation in the United States.   In addition, we identified three distinct segments in terms of individual trade-off between the benefits of disclosing personal information and privacy concerns – privacy guardians, information sellers, and convenience seekers. Finally, we made some headway in characterizing these segments.

Our findings are subject to a number of limitations which are common to many experimental settings. All of our subjects were undergraduate students. They would be younger and probably be more familiar with the Internet and e-commerce than the general consumer population. Further, they may have had relatively little experience of medical problems, relatively little travel experience, and had too little wealth to be familiar with investment opportunities and risks. This might explain why we found no systematic industry differences in subjects' preferences.[17] For all these reasons, it would be important to verify our findings with a more representative sample of subjects.

Further, the reported part-worths are sensitive to the specified attribute levels. For example, our conjoint stimuli specified only two levels of each privacy concern – no protection and protection. In reality, however, businesses have more flexibility. For example, they may state that personal information is currently not used for secondary purposes, but that such a practice cannot be ruled out in the future. Similarly, rewards may range from cash or vouchers to lottery drawings. Different reward structures may imply different estimates for the marginal utility of a one-dollar reward. Future research may attempt to measure the impact of privacy policies and reward structures more directly.[18]

[17] By contrast, Westin (2001) reported that Americans were particularly sensitive to privacy over financial and health information.

[18] However, this may require a willingness of the businesses to share the kind of data that they have promised not to share for secondary use.

Bibliography

Addelman, Sidney "Orthogonal Main-Effect Plans for Asymmetrical Factorial Experiments," *Technometrics*, vol.4, no.1, February 1962.

Benassi, Paola "Truste: An Online Privacy Seal Program," *Communications of the ACM*, vol. 42, no. 2, February 1999, pp. 56-59.

Bhargava, H.K. and V. Choudhary "One Size Fits All? Optimality Conditions for Versioning and Second-degree Price Discrimination," Pennsylvania State University, March 2002.

Cate, Fred H. and Michael E. Staten, *Putting People First: Consumer Benefits of Information Sharing*, Washington, DC: Online Privacy Alliance, 1999. http://www.privacyalliance.org/resources/research.shtml

Cranor, Lorrie Faith, Joseph Reagle and Mark S. Ackerman "Beyond Concern: Understanding Net Users' Attitudes About Online Privacy," *AT&T Labs-Research Technical Report* TR 99.4.3, 1999. http://www.research.att.com/library/trs/TRs/99/99.4/

Culnan, Mary J. "How Did They Get My Name? An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," *MIS Quarterly*, vol. 17, no. 3, September 1993, pp. 341-363.

Culnan, Mary J. and George R. Milne "The Culnan-Milne Survey on Consumers and Online Privacy Notices: Summary of Responses," December 2001. http://www.ftc.gov/bcp/workshops/glb/supporting/culnan-milne.pdf

Culnan, Mary J. and Pamela K. Armstrong "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science*, vol. 10, no. 1, January-February 1999, pp. 104-115.

Culnan, Mary J. and Sanda J. Milberg "Consumer Privacy," in Mary J. Culnan, Robert J. Bies, and Michael B. Levy, Eds., *Information Privacy: Looking Forward, Looking Back*, Georgetown University Press, 1999, forthcoming.

Eddy, Erik R., Dianna L. Stone and Eugene F. Stone-Romero "The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology*, vol. 52, 1999, pp. 335-358.

Esrock, Stuart L. and John P. Ferre "A dichotomy of privacy: Personal and professional attitudes of marketers," *Business and Society Review*, vol. 104, no. 1, Spring 1999, pp. 107-120.

European Union, *Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data* (95/46/EC), 1995.

Friedman, M. and L.J. Savage "The utility analysis of choices involving risk," *Journal of Political Economy*, vol. 56, no. 4, August 1948, pp. 279-304.

Goodwin, Cathy "Privacy: Recognition of a Consumer Right," *Journal of Public Policy and Marketing*, vol. 10, no. 1, Spring 1991, pp. 149-166.

Green, Paul E. and Abba M. Krieger "Segmenting Markets with Conjoint Analysis," *Journal of Marketing*, vol. 55, no. 4, October 1991, pp. 20-31.

Green, Paul E. and V. Srinivasan "Conjoint Analysis in Marketing: New Developments With Implications for Research and Practice," *Journal of Marketing*, vol. 54, no. 4, 1990, pp.3-19.

Hahn, Robert "An Assessment of the Costs of Proposed Online Privacy Legislation," AEI-Brookings Joint Center for Regulatory Studies, May 2001.

Hair, Joseph F., Ronald L. Tatham, Rolph E. Anderson and William C. Black. *Multivariate Data Analysis with Readings*. Prentice Hall, 1998.

Harper, Jim and Solveig Singleton "With a Grain of Salt: What Consumer Privacy Surveys Don't Tell us," Competitive Enterprise Institute, June 2001.

Hartley, Roger, and Lisa Farrell "Can Expected Utility Theory Explain Gambling?" *American Economic Review*, vol. 92, no. 2, June 2002, pp. 613-624.

Hoffman, Donna L., Novak, Thomas P. and Peralta, Marcos A. "Building Consumer Trust Online," *Communications of the ACM*, vol. 42, no. 4, April 1999, pp. 80-85.

Horrigan, John B. and Lee Rainie "Getting Serious Online," Pew Internet & American Life Project, Washington, DC, March 2002. http://www.pewinternet.org/reports/pdfs/PIP_Getting_Serious_Online3ng.pdf

Jupiter Media Metrix "Seventy Percent of US Consumers Worry About Online Privacy, But Few Take Protective Action," *Press Release*, June 3, 2002.

Katz, James E. and Annette R. Tassone "Public Opinion Trends: Privacy and Information Technology," *Public Opinion Quarterly*, vol. 54, 1990, pp. 125-143.

Laudon, Kenneth C. "Markets and privacy," *Communications of the ACM*, vol. 39, no. 9, 1996, pp. 92-104.

Laufer, Robert S. and Maxine Wolfe "Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory," *Journal of Social Issues*, vol. 33, no. 3, 1977, pp. 22-42.

Milberg, Sandra J., Sandra J. Burke and H. Jeff Smith "Values, Personal Information Privacy, and Regulatory Approaches," *Communications of the ACM*, vol. 38, no. 12, 1995, pp. 65-74.

Milberg, Sandra J., H. Jeff Smith and Sandra J. Burke "Information Privacy: Corporate Management and National Regulation," *Organization Science*, vol. 11, no. 1, January-February 2000, pp. 35-57.

Milne, George R. and Mary Ellen Gordon "Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract," *Journal of Public Policy and Marketing*, vol. 12, no. 2, Fall 1993, pp. 206-215.

Moorthy, K. Sridhar "Market Segmentation, Self-Selection, and Product Line Design," *Marketing Science*, vol. 3, no. 4, Fall 1984, pp. 288–307.

New York Times "Giving the Web a Memory Cost Its Users Privacy," September 4, 2001.

Oberndorf, Shannon "Registering for Success," *Catalog Age*, vol. 16, no. 13, 1999, pp. 47-48.

OECD. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Privacy Guidelines), 23 September 1980. http://www1.oecd.org/dsti/sti/it/secur/prod/privacyguide.htm

Phelps, Joseph, Glen Nowak and Elizabeth Ferrell "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing*, vol. 19, no. 1, Spring 2000, pp. 27-41.

Png, Ivan. *Managerial Economics*, Malden, MA: Blackwell, 2002.

Posner, Richard A. "The Economics of Privacy," *American Economic Review: Papers and Proceedings*, vol. 71, no. 2, May 1981, pp. 405-409.

Schwartz, Paul M. "Beyond Lessig's CODE for Internet Privacy: Cyberspace Filters, Privacy-control, and Fair Information Practices," *Wisconsin Law Review*, no. 4, 2000, pp. 743-788.

Schwartz, Susana "It's Privacy, Stupid," *Intelligent Enterprise*, vol. 3, no. 6, 2000, pp. 10-12.

Smith, H. Jeff "Information Privacy and Marketing: What the U.S. should (and shouldn't) Learn from Europe," *California Management Review*, vol. 43, no. 2, Winter 2001, pp. 8-33.

Smith, H. Jeff, Sandra J. Milberg and Sandra J. Burke "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly*, vol. 20, no. 2, June 1996, pp. 167-196.

Stewart, Kathy A. and Albert H. Segars "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research*, vol. 13, no. 1, March 2002, pp. 36-49.

Stigler, George J. "An introduction to privacy in economics and politics," *Journal of Legal Studies*, vol. 9, no. 4, 1980, pp. 623-644.

Stone, Eugene F. and Dianna L. Stone "Privacy in organizations: theoretical issues, research findings, and protection mechanisms," *Research in Personnel and Human Resources Management*, vol. 8, 1990, pp. 349-411.

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner and Stepherd McClure "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology*, vol. 68, no. 3, 1983, pp. 459-468.

Taylor, Dalmas A. and Irwin Altman "Self-Disclosure as a Function of Reward-Cost Outcomes," *Sociometry*, vol. 38, no. 1, 1975, pp.18-31.

Taylor, Dalmas A., Irwin Altman and Richard Sorrentino "Interpersonal Exchange as a Function of Rewards and Costs and Situational Factors: Expectancy Confirmation-Disconfirmation," *Journal of Experimental Social Psychology*, vol. 5, 1969, pp. 324-339.

Tolchinsky, Paul D., Michael K. McCuddy, Jerome Adams, Daniel C. Ganster, Richard W. Woodman and Howard L. Fromkin "Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment," *Journal of Applied Psychology*, vol. 66, no. 3, 1981, pp. 308-313.

Turner, Michael A. "The Impact of Data Restrictions On Consumer Distance Shopping," Direct Marketing Association, 2001. http://www.the-dma.org/isec/9.pdf

U.S. Public Interest Research Group "Public Comment on Barriers to Electronic Commerce," Response to call by U.S. Department of Commerce (65 Federal Register 15898), April 25, 2000.

Varian, Hal "Economic Aspects of Personal Privacy," in U.S. Department of Commerce, *Privacy and Self-Regulation in the Information Age*, June 1997.

Vriens, Marco, Michel Wedel and Tom Wilms "Metric Conjoint Segmentation Methods: A Monte Carlo Comparison," *Journal of Marketing Research*, vol. 33, no. 1, 1996, pp. 73-85.

Ward, Michael R. "The Economics of Online Retail Markets," in Gary Madden and Scott Savage, Eds., *The International Handbook on Emerging Telecommunications Networks*, Edward Elgar Publishers, 2001.

Westin, Alan. Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Hearing on "Opinion Surveys: What Consumers Have To Say About Information Privacy," May 8, 2001.

Westin, Alan F. *Privacy and Freedom*, New York, NY: Atheneum, 1967.

Wittink, Dick R. "Market Measurement and Analysis: The First 'Marketing Science' Conference," *Marketing Science*, vol. 20, no. 4, Fall 2001, pp. 349-356.

Wittink, Dick R. and Philippe Cattin "Commercial Use of Conjoint Analysis: An Update," *Journal of Marketing*, vol. 53, no. 3, July 1989, pp. 91-96.

Woodman, Richard W., Daniel C. Ganster, Jerome Adams, Michael K. McCuddy, Paul D. Tolchinsky and Howard Fromkin "A Survey of Employee Perceptions of Information Privacy in Organizations," *Academy of Management Journal*, vol. 25, no. 3, 1982, pp. 647-663.