Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach

IL-HORN HANN, KAI-LUNG HUI, SANG-YONG TOM LEE, AND IVAN P.L. PNG

IL-HORN HANN is an Assistant Professor at the Marshall School of Business at the University of Southern California. He received his Ph.D. from the University of Pennsylvania in 2000. His primary research interests focus on the intersection of information technology and markets. He has investigated issues regarding competition and pricing in electronic markets and online privacy. His second research interest is in the area of open source software. His research has been published in *Journal of Management Information Systems* and *Management Science.*

KAI-LUNG HUI is an Associate Professor in the Department of Information Systems, Faculty of Business, City University of Hong Kong, while he is on leave from the National University of Singapore. He received his Ph.D. from the Hong Kong University of Science and Technology. His research interests include information privacy, product line design and pricing, and intellectual property. His research has been published in *American Economic Review: Papers and Proceedings, Journal of Management Information Systems, Management Science,* and *MIS Quarterly,* among others.

SANG-YONG TOM LEE is an Associate Professor in the College of Information and Communications, Hanyang University, Seoul, Korea. He received his Ph.D. from Texas A&M University (1999), and taught at the Department of Information Systems, National University of Singapore, before joining Hanyang University. His research interests are economics of information systems, information privacy, and value of IT investments. His papers have been published in *MIS Quarterly, Decision Support Systems, Information & Management, Communications of the ACM,* and others.

IVAN P.L. PNG is Kwan Im Thong Hood Cho Temple Professor and Professor of Business Policy and Economics at the National University of Singapore. His research focuses on the economics of intellectual property, information privacy, and pricing. Dr. Png is the author of *Managerial Economics,* which has been translated into Chinese (traditional and simplified characters) and Korean. He is a Professorial Fellow of the IP Academy of Singapore, and an Associate Editor of *Management Science.* He was a nominated Member of Parliament (10th Parliament of Singapore), 2005–6.

ABSTRACT: The advent of the Internet has made the transmission of personally identifiable information more common and often unintended by the user. As personal information becomes more accessible, individuals worry that businesses misuse the information that is collected while they are online. Organizations have tried to mitigate this concern in two ways: (1) by offering privacy policies regarding the handling and

Journal of Management Information Systems / Fall 2007, Vol. 24, No. 2, pp. 13–42.

0742–1222 / 2007 $9.50 + 0.00.
DOI 10.2753/MIS0742-1222240202

use of personal information and (2) by offering benefits such as financial gains or convenience. In this paper, we interpret these actions in the context of the information-processing theory of motivation. Information-processing theories, also known as expectancy theories in the context of motivated behavior, are built on the premise that people process information about behavior–outcome relationships. By doing so, they are forming expectations and making decisions about what behavior to choose. Using an experimental setting, we empirically validate predictions that the means to mitigate privacy concerns are associated with positive valences resulting in an increase in motivational score. In a conjoint analysis exercise, 268 participants from the United States and Singapore face trade-off situations, where an organization may only offer incomplete privacy protection or some benefits. While privacy protections (against secondary use, improper access, and error) are associated with positive valences, we also find that financial gains and convenience can significantly increase individuals' motivational score of registering with a Web site. We find that benefits—monetary reward and future convenience—significantly affect individuals' preferences over Web sites with differing privacy policies. We also quantify the value of Web site privacy protection. Among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth \$30.49–\$44.62. Finally, our approach also allows us to identify three distinct segments of Internet users—privacy guardians, information sellers, and convenience seekers.

Key words and phrases: conjoint analysis, expectancy theory, financial reward, information privacy, online privacy, segmentation.

Privacy problems have been identified to be a major impediment to e-commerce. According to the U.S. Public Interest Research Group, "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" [2].

Even before the proliferation 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 Cooperation and Development published guidelines for the collection and use of personal information by government and private organizations [51]. Further, in 1995, the European Union adopted a data protection directive that regulates information within and beyond the Union [18]. The directive disallows transfer of information to other countries that do not provide adequate protection. Continued public pressure has led to increased regulation specifically of online privacy. Recent examples include the 1998 Children's Online Privacy Protection Act and the 2003 California Online Privacy Protection Act, which regulate the online collection and use of personal information regarding children under the age of 13 and California residents.[2] Additional legislation, such as disclosure requirements of security breaches of data, is currently under consideration.

Rapid improvements in computing technologies and the advent of e-commerce have amplified public concern about privacy, especially on electronic networks. With every Web site visit, a visitor leaves an electronic trace that can later be retrieved and analyzed. Combined with technology to store identifying information (cookies), Web site operators can profile visitors to an unprecedented degree and subsequently merge these profiles with other demographic data. Such an enriched data set can then be used by the company or sold to other parties [54]. This information could benefit the customer by more precisely identifying his or her needs. However, it could also be used to his or her detriment. For example, Amazon.com was suspected of engaging in differential pricing based on prior shopping information and other customer demographics for the sale of DVDs; more precisely, some customers were deliberately overcharged.[3] In general, Westin observes that 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-fourths of American consumers in 2001" [68].

Violation of privacy occurs when an organization, in its efforts to pursue the organization's objectives, collects, stores, manipulates, or transmits personal information unbeknownst to the individual. Not all of these activities surrounding personal information are necessarily perceived as invading privacy. A person submitting his or her name, e-mail address, residential address, and credit card information online for a purchase may not perceive the payment procedure as invasive, but as a necessity to obtain the benefits of the product or service (Simmons made similar arguments regarding disclosure of intimate personal information [55]). However, the person may feel that his or her privacy is invaded if that information is then linked to other primary and secondary data such as browsing behavior on the Web site and demographic information. Yet other people might welcome these efforts if this leads to price and product promotions. In general, perceptions of privacy infringements vary individually.

Privacy research has shown that this perception can be influenced by the firm's actions. Naming the disclosure targets—that is, the person to whom private information is disclosed and the purpose of the relationship—influences perception of privacy violations [37, 62]. Fusilier and Hoyer [21] show that granting permission of disclosure greatly reduces the perception of privacy invasion. Culnan and Armstrong [9] find that privacy concerns can be addressed by explicitly stating that fair procedures for managing private information will be employed. In addition, Spiekermann et al. [58] show that in order to reduce product complexity, many participants, even some privacy fundamentalists, willingly share private information with a Web site. Even though their study does not measure the cost–benefit trade-off directly, it indicates that perceptions of privacy are context dependent. One important contribution of our study is to analyze such considerations.

Some actions of Internet businesses can certainly be interpreted as strategies to mitigate privacy concerns. An organization's promise to adhere to privacy policies regarding the handling and use of personal information may reduce perceptions of privacy violations. Perhaps the most common way of reducing privacy concerns has been to offer incentives. Many online organizations have offered prizes (such as participation in raffles or free shipping) in exchange for submitting personal information. Even more pervasive is the facility of "customizing" a Web site according to a customer's preferences, thereby increasing his or her convenience. For example, Amazon's "1-click ordering" technology greatly reduces the inconvenience of the payment process for repeat customers.

Previous privacy research has, perhaps due to the nature of the subject, mostly focused on privacy concerns [8, 9, 45, 56, 60]. We extend this discussion by introducing additional dimensions that the information-seeking organization has to offer—namely, financial incentives and convenience. In this paper, we are interested in analyzing these means of mitigating privacy concerns. Our research objectives are as follows: first, we analyze privacy mitigation strategies from the viewpoint of information-processing theories of motivation. Specifically, we apply the *expectancy theory of motivation* (from now on "expectancy theory"), which assumes that an individual's choice is determined by his or her expectations about attaining desired outcomes. After processing information about behavior–outcome relationships, people are considered to form expectations and make decisions about what alternatives to choose. Based on this theory, we hypothesize that efforts to mitigate privacy concerns effectively lead to an increase in motivational score.

A second contribution of this study is that our research design allows for heterogeneity of privacy preferences. This study differs from previous work on information privacy in that we use a within-person approach that allows us to estimate the *individual's utility* for the means to mitigate privacy concerns. We employ the technique of conjoint analysis in which each subject is asked to assess trade-off situations, where an organization may only be able to offer incomplete privacy protection and/or promotions and/or convenience. Using this method, 84 U.S. and 184 Singapore subjects ranked alternative combinations of benefits and privacy protection policies in an online setting. Based on this approach, we estimate that for U.S. subjects, protection of personal information is worth US$30.49–$44.62. For Singapore subjects, we find that privacy protection is valued at S$57.11. An additional advantage of using a within-person approach is that we can use the individual utilities as a basis to identify segments of Internet users. Our results indicate that there are three distinct segments of Internet users, which we term *privacy guardians, information sellers,* and *convenience seekers.*

Theory and Hypotheses

Information privacy has been defined as the individual's ability to control the collection and use of personal information [61, 67]. Based on the work of Goffman [22], this concept stipulates that privacy is viewed as control of information about the self. Control of personal information requires that an individual manage the outflow of information as well as the subsequent disclosure of that information to third parties. Research in psychology suggests that individuals seek privacy to maintain self-identity, establish personal boundaries, and avoid unwanted disclosure and intrusion [23, 24]. In many experimental and organizational settings, people are found to perceive privacy invasions when they are not granted sufficient control on the solicitation, storage, use, and disclosure of various types of personal information [15, 63, 69]. Such perception may deter them from taking part in transactions that involve personal information solicitation [8, 62].

Consumer research suggests that individuals face a degree of risk when they enter into marketing transactions, and their perceived risk may significantly affect their extent of information search and purchase decisions [7]. Generally, perceived risk encompasses both the uncertainty and adverse consequences of taking part in a transaction [14]. Advances in network and telecommunications technologies have fostered the growth of electronic commerce, which has added a new information dimension to marketing transactions. Increasingly, personal information is acquired, exchanged, and used by online establishments. This has expanded the risk of Internet users who now face additional uncertainty regarding how their personal information is handled. Information privacy has been found to be of utmost concern to consumers in contemporary marketing exchanges [9, 35, 53].

Previous research by Laufer and Wolfe [40] in an organizational setting suggests that individuals perform a "calculus of behavior" to assess the costs and benefits of providing personal information. On the basis of this theoretical construct, individuals explicitly consider the trade-off between the merits of interactions and potential consequences.[4] Implicitly assumed in this "privacy calculus" is that individuals behave to maximize the difference of benefits and costs. Based on this understanding, we use an information-processing theory of motivation to analyze the extent of individuals' online information privacy concerns. Like all cognitive theories, information-processing theory focuses on the cognitive process that occurs before a behavior is undertaken or a choice is made. Specifically, we employ the expectancy theory framework to give more structure to the question of how individuals make decisions regarding privacy in an online setting.[5] Originally formulated by Vroom [66], expectancy theory is a framework to explain how an individual chooses between alternative forms of behavior. The theory proposes that the individual considers the outcomes associated with various levels of performance as well as the likelihood of achieving these outcomes. When deciding among alternatives, an individual selects the option with the greatest *motivational score.*[6]

The motivational force for a behavior or action is a function of three distinct perceptions: expectancy, instrumentality, and valence—that is, Motivational Score = f(Expectancy, Instrumentality, Valence). *Expectancy* is a probability assessment that reflects the individual's belief that a given level of effort will result in a given level of performance. *Instrumentality* refers to the subjective assessment that a given performance level will lead to one or more outcomes. *Valence* refers to the value that an individual places on a given outcome.

For illustration purposes, we discuss expectancy theory in the context of a person considering whether to register at a financial Web site to trade stocks, to stay current about the value of his or her stock holdings, to collect information about the companies that are part of his or her stock portfolio, and to receive advice on the riskiness of his or her stock portfolio. For these purposes, the financial Web site may require the person to submit an e-mail address, name, residential address, banking information, social security number, and the names of the stocks and quantities owned. *Motivation* is seen as the force that directs behavior. It deals with the question of choice among competing alternatives. As applied to online information privacy, in the case of financial Web sites, we investigate which site the individual chooses, after controlling for content and the amount of personal information that it collects and given that the individual may choose among different mixes of privacy policies, convenience, and financial benefits. *Expectancy* is the probability weight that characterizes the perceived effort–performance relationship. It is the expectancy that one's effort will lead to the desired performance. In our example, an individual may provide the requested personal and portfolio information that results in signing up with the financial Web site. *Instrumentality* is the weight that describes the perceived performance–outcome relationship. It characterizes the belief that if a person does meet performance expectations, he or she will receive a particular outcome. For the individual, signing up with the financial Web site may provide more convenience when checking the stock portfolio and becoming updated on relevant company news, and financial benefits through promotions. Regarding online privacy, an important outcome is the commitment of the financial Web site to protect personal information according to its privacy policy. Finally, *valence* refers to the value the individual personally places on the outcome. This is a function of his or her needs, goals, and values. Depending on the outcome, the valence can be positive or negative. In the financial Web site example, positive valences include the appreciation of the convenience of having all relevant information without repeated search and the financial gain from having signed up with this Web site. In the context of online privacy, positive valence includes the feeling of security due to the specifics of the privacy policy. A Web site with an incomplete privacy policy may generate negative valences such as the potential to be vulnerable to others or to be exploited by others.

In the context of privacy, a consumer who has the choice between alternative financial Web sites will take the amount of personally identifiable information collected, the privacy policy, the convenience, and the financial gains into consideration. Each of these dimensions is associated with a value for expectancy, instrumentality, and valence. An individual will rank the alternatives and choose the one with the greatest motivational force. More formally, for an alternative with *n* dimensions, the expectancy theory assumes a score that is computed as

$$\text{Motivational Score} = \sum_{i=1}^{n} \underbrace{(E \rightarrow P)_i}_{\text{Expectancy}} \times \underbrace{(P \rightarrow O)_i}_{\text{Instrumentality}} \times \underbrace{V_i}_{\text{Valence}} ,$$

where Expectancy characterizes the weight on the effort-to-performance relationship ($E \rightarrow P$) and Instrumentality characterizes the weight on the performance-to-outcome relationship ($P \rightarrow O$).

Applying this model in the context of online information privacy, we note that expectancies, instrumentalities, and valences are specific to each person. However, this model also implies that the variable outcome (O) can be influenced by the organization to increase the motivational score of a person. If the organization can effectively use outcomes that are associated with positive valences, it can increase the motivational score and effectively decrease privacy concerns. Important to our approach is that given a certain motivational score for fixed effort, performance, and a manipulated outcome, we can elicit the valences that are associated with the means to mitigate online privacy concerns.

Our first research objective addresses how organizations can mitigate privacy concerns by managing outcomes and associated valences within the expectancy model. We first have to establish the various outcomes that are associated with valences. Previous research by Smith et al. [56] identified four specific privacy concern dimensions that represent the cognitive state of consumers toward corporate use of information. These four privacy dimensions are collection, error, unauthorized secondary use, and improper access. *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*[7] refers to the concern that "information is collected for one purpose but is used for another, secondary purpose," and *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" [56, p. 172, table 2]. While Smith et al. [56] identified these dimensions through a careful instrument development and validation process using students, consumers, and professionals, Stewart and Segars [60] further validated these dimensions with a large, representative sample of consumers.[8] Therefore, we use these dimensions (collection, error, unauthorized secondary use, and improper access) as the basis for potential outcome variables, which will determine the instrumentalities. Consistent with expectancy theory, businesses can use the protection of privacy as an outcome to increase the motivational score of the Web site. Specifically, individuals link performance (successfully obtaining an account) with outcome (assurance by privacy policy). For example, a person may give a privacy policy that restricts secondary use a higher instrumentality and hence a greater motivational score than a policy that omits protection from secondary use. Therefore, we hypothesize:

> *Hypothesis 1a (Privacy Protection): Specification of privacy protection increases the motivational scores.*

Besides information privacy protection, an individual's motivational score may also be affected by extrinsic, positive reinforcements. Resource exchange theory characterizes six categories of interpersonal resources—love, status, information, money, goods, and services—and it is well demonstrated that people are willing to trade one resource for another [13, 19]. Prior research has shown that this resource framework is quite general, and it can be applied to analyze different types of marketing transactions that involve interpersonal relationships and resource exchanges [33].

Many e-commerce Web sites provide monetary reward or exclusive, convenient services that help reduce transaction time to people who disclose certain personal information.[9] Both money and service are primary elements in Foa's theory [19], and they may act as positive incentives and resources for online organizations to exchange for personal information. Applying this to the expectancy theory–based framework, this implies that an organization can offer financial gains and convenience to increase the motivational score. As in H1a, the organization influences the instrumentalities by creating outcomes (financial gain, convenience) that are desirable. Hence, we hypothesize:

> *Hypothesis 1b (Financial Gain and Convenience): Offering financial gains and convenience increases the motivational score.*

H1a and H1b describe basic individual preferences, and they may apply to general behavioral decisions, such as participation in online activities, information disclosure, or selection of Web sites for transactions. However, in many real-life situations, the organization may be able to extract substantial value from personal information. Culnan and Armstrong [9] and Culnan and Bies [10] observe that competitive pressure may make it necessary for organizations to use personal information. In the financial Web site example, the organization may be able to cross-sell additional investment services when analyzing the person's portfolio. Hence, the Web site may choose to offer financial incentives, convenience, and a privacy policy that includes error correction and protection from unauthorized access, but no protection from secondary use. One direct implication for the expectancy theory–based framework is that any method that evaluates the valences of outcomes must specifically address the possibilities of trade-offs between the outcomes.

Previous research on information privacy was mostly concerned with identifying key dimensions of privacy concerns [56, 60] and how perceptions of privacy infringements can be influenced [9, 21, 37, 62]. However, academic research has given less attention to differences in privacy preferences. Informal surveys have shown that people do not always exhibit identical preferences on privacy and that differences across the population may exist [68]. From an organizational point of view, it is important to determine which preferences exist and how prevalent they are. Such an analysis would allow an organization to take the appropriate steps to address the privacy concerns appropriately. Hence, we are interested in a characterization of the trade-offs of outcome valences. Social exchange theory posits that individuals' choice of actions (and hence their preferences toward alternative stimuli) are influenced by their personal experience; the more frequently a person was rewarded by a particular stimulus in the past, the more likely he or she would be to perform an action that leads to the stimulus [16, 35]. Further, the extent of privacy calculus posited by Laufer and Wolfe [40] depends on personal and environmental characteristics, and Stone and Stone's [61] expectancy theory–driven privacy model includes individual and social factors such as personality and previous learning.

In accordance with these models, individuals' preferences toward privacy protection and positive reinforcement may be shaped by their personal characteristics. In the context of information privacy, these theories posit that individuals may vary in their judgments toward online privacy. Inasmuch as expectations about valences across individuals are similar, groups may be identified. For example, past opinion surveys have divided the U.S. population into a majority of "privacy pragmatists" and minorities of "privacy fundamentalists" and "privacy unconcerned" [68]. Therefore, we hypothesize:

> *Hypothesis 2 (Privacy Diversity): Individuals have systematic differences in privacy preferences.*

Methodology and Experimental Procedure

Researchers in the past have used judgment models based on a within-person-based approach of expectancy theory [47, 57, 59]. They have in common that an individual is provided with a set of variables that are used to arrive at a particular decision. The within-person approach requires that multiple cases with unique combinations of variables be presented and each individually evaluated. Our approach, the *conjoint analysis* method, shares these characteristics, but is rooted in decision theory. Conjoint analysis grew out of the area of conjoint measurement, which was first developed in economics [11] and psychology [42]. The technique provides a measurement method for decision-making contexts where multiple dimensions must be taken into account.[10]

Conjoint analysis presents test subjects with a set of *alternatives* (stimuli). Each stimulus consists of particular *levels* of various *dimensions* (attributes). In the context of online privacy, *dimensions* of a Web site include the dimensions of privacy (collection, error correction, secondary use, and improper access), convenience, and monetary reward. Each *dimension* is represented by two or more *levels.* For example, "unauthorized secondary use of private information" and "no unauthorized secondary use of private information" represent two levels of the secondary use dimension. The subject is asked to rank the stimuli according to his or her preferences. An example of the conjoint analysis stimuli and the accompanying introduction is provided in the Appendix. The conjoint analysis technique decomposes ranking-scale evaluation judgments of alternatives into components based on the dimensions of the alternatives. A numerical utility, which is also called a *part-worth* (see, e.g., [28]), is computed for each level of each dimension.

To keep the conjoint tasks to a manageable size, Green and Srinivasan [27] recommend that the number of attributes be limited to six or fewer. Following the work of Green and Krieger [25], 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 Web sites 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 Web site. The focus groups identified two sources of convenience benefits—the explicit time saving per session and the expected visit frequency to the Web site. Accordingly, we operationalized convenience by "expected visit frequency/total time savings" in our conjoint experiment.[11]

As mentioned before, we considered the four privacy dimensions identified by Smith et al. [56]—collection, error, unauthorized secondary use, and improper access. For our purpose, collection is a necessary antecedent to the three other dimensions. Error, unauthorized secondary use, and improper access of information cannot 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 Web site 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 trade-offs between collection and other outcome dimensions. Accordingly, in our conjoint analysis, we controlled for the collection of information and manipulated the other three dimensions.

Taken together, our conjoint study assesses trade-offs among five dimensions—two benefit outcomes and three privacy outcomes. Based on the discussion with our focus groups, we created three outcomes for monetary reward ($5, $10, and $20, in the respective currency) and visit frequency/time savings (monthly, weekly, and daily).[12] The outcomes of the three privacy dimensions (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 × 3 × 2 × 2 × 2 = 72 conjoint stimuli. To avoid asking subjects to rank too many alternatives, we selected 18 stimuli based on an optimal orthogonal design [1].[13] For example, one particular stimulus was a Web site that provided a $5 monetary reward (in the respective currency) in return for personal information and which the subject visited once a month with a total time savings of 24 minutes per year. Further, the Web site 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 Web sites (stimuli) that represented different combinations of benefits and privacy protection.

The basic estimation procedure underlying the conjoint analysis is a main effects analysis of variance (ANOVA), which computes utilities such that the rank ordering of the sums of each alternative's set of part-worths is the same as the actual rank ordering of the alternatives. The basic building block of our conjoint analysis is built on the following model:

$$\begin{aligned} \mathit{Ranking} = \alpha + \sum_{j\in\{\$10,\$20\}} \mathit{Outcome}_{\text{Fin. Rew.}\, j} * \mathit{PW}_{\text{Fin. Rew.}\, j} \\ + \sum_{k\in\{\text{dly},\text{wkly}\}} \mathit{Outcome}_{\text{Freq.}\, k} * \mathit{PW}_{\text{Freq.}\, k} + \mathit{Outcome}_{\text{Error}} * \mathit{PW}_{\text{Error}} \\ + \mathit{Outcome}_{\text{Sec. Use}} * \mathit{PW}_{\text{Sec. Use}} + \mathit{Outcome}_{\text{Unauth. Access}} * \mathit{PW}_{\text{Unauth. Access}} + \varepsilon. \end{aligned}$$

To recall, the part-worth (*PW*) is the marginal utility of the dimension in the individual's ranking of the conjoint stimuli. To estimate the part-worths, we use 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 outcomes and three privacy protection outcomes as the independent variables.[14] Then, the coefficient of each independent variable is the part-worth corresponding to the outcome of that dimension.

In summary, the conjoint analysis proceeds by the following steps [26]:

Step 1: Selection of preference model: part-worth function model (piecewise linear).
Step 2: Data collection method: full profile experiment approach, which utilizes a full set of factors (privacy concerns, mitigating factors).
Step 3: Stimulus set construction: optimal orthogonal design [1], which is a sample of the full factorial set.
Step 4: Stimulus presentation: Web-based instructions and description.
Step 5: Measurement scale for dependent variable: nonmetric; rank order.[15]
Step 6: Estimation method: ordinary least squares.

In order to control for industry effects, we posed the conjoint stimuli in three settings—financial, health care, 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 Web sites) 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. In particular, travel Web sites requested the person's occupation, travel purpose, destination, and frequency of travel, as well as frequent flyer numbers; health-care Web sites asked for medical history, drug allergies, and prescription record; and financial Web sites asked for household income, stock portfolio, and previous stock trading experience.

Each subject was randomly assigned to one of the three industry settings and asked to rank the 18 stimuli (Web sites) according to his or her preferences. In other words, the benefit/privacy dimensions were within-subject factors whereas industry was a between-subject factor. To capture the background of the 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 United States and Singapore. The U.S. subjects were upper-division undergraduate students from a major Eastern U.S. 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.

The experiment proceeded as follows. First, all subjects completed the demographic questions. Second, 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 other students were compensated with US$7.[16] In Singapore, 184 subjects completed the experiment and received course credit. We collected 268 responses in total.

Table 1. Descriptive Statistics

	United States	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
Subjects' country of origin (number of subjects)	United States (48), India (13), 10 other countries (each fewer than five)	Singapore (145), Malaysia (12), nine other countries (each fewer than five)

Linking the Theoretical Framework to the Methodology: Expectancy-Based Theory of Motivation and Conjoint Analysis

The expectancy-based theory can be related to the selected research methodology, the conjoint analysis. In our research design, the expectancy (the effort–performance weight) is constant across all Web site choices. Because we specify the required effort (i.e., input of the same set of personal information), as well as performance (i.e., fulfilling the information request of the Web site), we set the expectancy weight equal to one. Instrumentality, the performance–outcome weight, is affected by the outcomes offered. In our research design, the outcomes are varied in a controlled manner by the conjoint stimuli. The conjoint stimuli are determined by the orthogonal design of the set of specific outcomes of the five dimensions (error, unauthorized secondary use, improper access, monetary reward, and visit frequency/time savings). Hence, the instrumentality weights are set to either one or zero, depending on whether a specific outcome is present or not. For example, if the conjoint stimulus specifies that a financial reward of $10 (in the respective currency) be offered, then the instrumentality weight for the financial reward outcome of $10 is equal to one. Valence, the value that the person places on the outcomes, is not affected by the reward or privacy protection factors, but is inferred from his or her ranking of the stimuli.

As previously discussed, the motivational score is a function of expectancy, instrumentalities, and valences. In our research design, the expectancy weights are fixed (set to one), the instrumentality weights are set to zero or one (depending on the outcomes described by the conjoint stimuli), and the motivational score is the actual ranking of the conjoint stimuli (which motivates the person's choice given the set of specific outcomes for the five dimensions). The valences are inferred through the conjoint analysis methodology, given fixed expectancy and instrumentality weights. As noted above, the conjoint analysis regresses the subjects' rankings of the conjoint stimuli (from 1 to 18) on dummy variables, which represent the various levels of the two benefit outcomes and three privacy protection outcomes.[17] The coefficient of each independent variable would be the part-worth corresponding to the outcome of that dimension (in order to be consistent with the regression language, we will use the term *coefficient* to mean part-worth from here on). In the context of the expectancy theory–based framework, the coefficients of the dummy variables represent the valences of the outcomes.

The relationship between the expectancy-based theory of motivation framework for privacy and the conjoint analysis can be depicted as follows:

$$\begin{aligned}
\underbrace{Ranking}_{\text{Motivational Score}} &= \alpha + \sum_{j\in\{\$10,\$20\}} \underbrace{Outcome_{\text{Fin. Rew.}\,j}}_{\text{Instrumentality for Fin. Rew. } j} * \underbrace{PW_{\text{Fin. Rew.}\,j}}_{\text{Valence for Fin. Rew. } j} \\
&+ \sum_{k\in\{\text{dly},\text{wkly}\}} \underbrace{Outcome_{\text{Freq.}\,k}}_{\text{Instrumentality for Freq. } k} * \underbrace{PW_{\text{Freq.}\,k}}_{\text{Valence for Freq. } k} \\
&+ \underbrace{Outcome_{\text{Error}}}_{\text{Instrumentality for Error}} * \underbrace{PW_{\text{Error}}}_{\text{Valence for Error}} \\
&+ \underbrace{Outcome_{\text{Sec. Use}}}_{\text{Instrumentality for Sec. Use}} * \underbrace{PW_{\text{Sec. Use}}}_{\text{Valence for Sec. Use}} \\
&+ \underbrace{Outcome_{\text{Unauth. Access}}}_{\text{Instrumentality for Unauth. Access}} * \underbrace{PW_{\text{Unauth. Access}}}_{\text{Valence for Unauth. Access}} + \varepsilon.
\end{aligned}$$

Results and Discussion

Conjoint Analysis

Table 2 reports the means of the coefficients (valences) for the U.S. and Singapore subjects. Further, we calculated the relative importance of each dimension as the coefficient corresponding to the maximum level of that dimension divided by the sum of the coefficients corresponding to the maximum levels of all five dimensions. The relative importance indicates how much impact a specific outcome has relative to other outcomes. We expressed relative importance as a percentage. Note that the coefficients 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 prevailing exchange rate, the rewards specified to the Singapore subjects were equivalent to US$2.70, US$5.40, and US$10.80.[18]

We first examined whether the responses from the subjects differed across the three industries (financial, health care, and travel). Because our U.S. and Singapore samples were reasonably large, the central-limit theorem implies that the estimated coefficients for each independent variable should approximately follow a normal distribution. Based on this premise, we conducted one-way ANOVA and pairwise *t*-tests to compare the coefficients of each outcome across the industries. The results suggested that the coefficients were not statistically different across financial, health care, and travel Web sites. Accordingly, in all subsequent analyses, we pooled the data across industries.

As elaborated above, the coefficient of an outcome is its valence interpreted in the expectancy theory–based framework. By offering a specific outcome, such as protec-

Table 2. Coefficients and Relative Importance

		United States		Singapore	
Instruments	Level	Coefficient[1]	Relative importance (percent)	Coefficient[1]	Relative importance (percent)
Monetary reward	$5[2]	n.a.	26.24	n.a.	11.69
	$10[2]	1.327***		0.232	
		(0.341)		(0.165)	
	$20[2]	3.141***		1.388***	
		(0.534)		(0.281)	
Visit frequency/ time savings	Monthly	n.a.	6.13	n.a.	6.02
	Weekly	0.568**		0.432***	
		(0.260)		(0.153)	
	Daily	0.734*		0.715***	
		(0.411)		(0.254)	
Error	No review	n.a.	24.80	n.a.	15.06
	Review	2.968***		1.787***	
		(0.355)		(0.194)	
Improper access	No restriction	n.a.	25.12	n.a.	28.43
	Restriction	3.007***		3.374***	
		(0.529)		(0.349)	
Unauthorized secondary use	Allowed	n.a.	17.70	n.a.	38.80
	Not allowed	2.118***		4.605***	
		(0.324)		(0.297)	

Notes: [1] Standard errors are shown in parentheses. The lowest levels of each of the included dimensions are used as experimental control and hence are excluded from the estimation. We label all lowest-level coefficients as “n.a.” (not applicable). [2] U.S. dollars for U.S. subjects and Singapore dollars for Singapore subjects. *** Significant at the 1 percent level; ** significant at the 5 percent level; * significant at the 10 percent level.

tion from unauthorized access, an organization can benefit from the instrumentality of such an outcome. The motivational score increases if this outcome is associated with a positive valence. Hence, a positive and significant coefficient for an outcome indicates that this outcome increases the motivational score. The coefficients (valences) on the outcomes of the privacy dimensions (error, improper access, and unauthorized secondary use) show strong support for the Privacy Protection hypothesis (H1a). A positive coefficient for a specific privacy dimension that differs significantly from zero indicates that subjects, on average, prefer a Web site with this privacy protection feature.

For example, in the U.S. sample, a privacy policy that restricts improper access will raise its motivational score by 3.007 (out of 18). Referring to Table 2, the coefficients (valences) for protection against all three privacy concerns were statistically significant at the 1 percent level in both samples. Among U.S. subjects, the coefficient for review (which enabled an individual to correct errors in his or her personal information) was 2.968, whereas that for disallowing unauthorized secondary use was 2.118. Among Singapore subjects, the coefficients (valences) for error review and editing, restricting improper access, and disallowing unauthorized secondary use were 1.787, 3.374, and 4.604.

Comparing the coefficients (valences) between countries, we found that, consistent with previous research [17, 44], 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 [9].

Our results also indicate support for the Financial Gain and Convenience hypothesis (H1b), that outcomes such as monetary rewards are associated with positive valences and hence increase the motivational score. For the U.S. sample, the coefficient (valence) for a US$20 reward was 3.141 and was statistically significant. This means that a Web site offering a US$20 reward for personal information could increase the motivational score by 3.141 (out of 18) as compared to an otherwise identical Web site offering the base-level US$5 reward. Also, the coefficient for a US$10 reward was 1.327 and significant. For the Singapore sample, the coefficient 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 coefficient was much less than the US$20 coefficient in the U.S. sample (3.141). Interestingly, the S$20 coefficient among Singapore subjects (1.388) was very close to the US$10 coefficient 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). The coefficient 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 of 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 significantly increased the relative attractiveness of

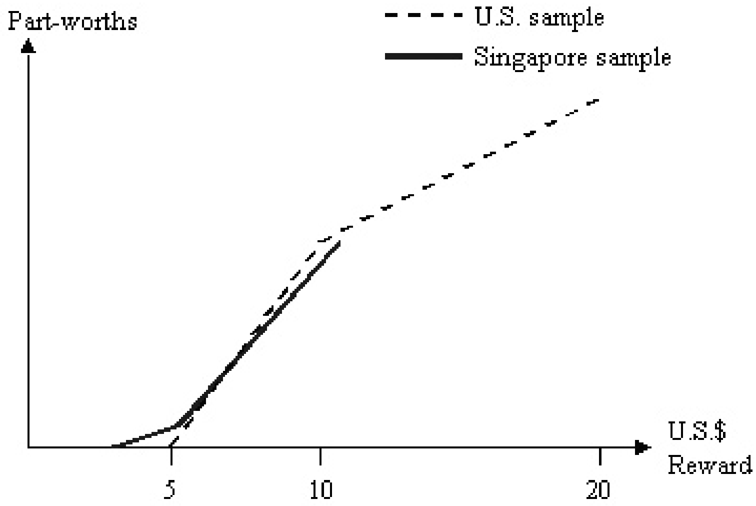

Figure 1. Part-Worths Associated with the Monetary Rewards

a Web site 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 nonconcave [20, 31].

We also find support for the second part of the Financial Gain and Convenience hypothesis (H1b), that outcomes such as time-saving services, operationalized by visit frequency/time savings, are associated with positive valences and hence increase the motivational score. Referring to Table 2, in the U.S. sample, the coefficient (valence) for weekly visits was significant at the 5 percent level, but the coefficient for daily visits was significant only at the 10 percent level. Even though the coefficients for weekly visits were smaller than for daily visits, they were not significantly different. In the Singapore sample, the coefficients for visit frequency/time savings were generally more significant. However, as with the U.S. subjects, the effect due to weekly visits was not significantly different from that due to daily visits.

From the results of both samples, we conclude that there is some evidence that subjects value convenience. The evidence is stronger among Singapore subjects than U.S. subjects. Further, once the subjects expected to visit a certain Web site sufficiently frequently (at least once a week), more frequent visits did not seem to affect subjects' preferences. This is consistent with the notion of a "convenience threshold," which is reached with a weekly visit frequency. The coefficients 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 coefficients and relative importance for the other dimensions. Apparently, among our subjects, convenience was only a minor factor when evaluating Web sites. By contrast, monetary reward and privacy protection were perceived to be much more important.

The coefficient (valence) is the value associated with an outcome. In our setting, it represents the marginal increase in the motivational score. However, with some simple calculations, we can give the coefficients a more useful meaning. Specifically, we can interpret the coefficient (valence) of monetary reward in terms of the marginal utility of a $1 reward in the respective currency. Referring to Table 2, in the U.S. sample, between the US$5 and US$10 rewards, the US$5 increase raised the motivational score by 1.327, or 0.265 per dollar of reward. Further, between the US$10 and US$20 rewards, the US$10 increase raised the motivational score 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.[19] In the Singapore sample, the S$10 coefficient was not significantly different from zero. Accordingly, we focus on the S$20 coefficient. Between the S$5 and S$20 rewards, the S$15 increase raised the motivational score by 1.388, which amounted to 0.0925 per Singapore dollar of reward or 0.171 per U.S. dollar of reward. This was remarkably close to the range (0.181–0.265 per U.S. dollar of reward) that we found among U.S. subjects.

Finally, using the marginal utilities of a US$1 reward and the coefficients 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 coefficient 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 = US$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.

Generally, our results in Table 3 suggest that Web sites 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 between US$30.49 and US$44.62, as seen by summing the column entries for U.S. subjects. Based on the S$20 coefficient in Table 2, the comparable number for Singapore subjects is S$57.11.

Segmentation 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 [25, 65]. This technique groups subjects into distinct segments according to the similarity of their estimated coefficients for the various outcomes. In the present case, we applied cluster analysis to segment the

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

	Value	
Web site privacy policy	United States	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

subjects according to their estimated valences over the various benefits and dimensions of privacy protection.[20]

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 [29, pp. 493–498]. We used a distance measure for (dis)similarity as all the valences (the inputs to the cluster analyses) were derived from a common scale—the Web site 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. [29, p. 499]. Table 4 reports the three clusters, their sample sizes, and the respective mean coefficients.[21]

Overall, we found strong support for the Privacy Diversity hypothesis (H2). 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 percent of the U.S. subjects and 84 percent of the Singapore subjects exhibited relatively high coefficients for protection against error, improper access, and unauthorized secondary use of their personal information. By contrast, their coefficients 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 Web site privacy policies.

The smallest cluster comprised subjects who focused exclusively on convenience (operationalized by visit frequency/time savings).[22] In fact, their coefficients for visit frequency/time savings were so high that their preferences over alternative Web sites 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 Web site privacy policies.

Table 4. Clusters

Segment (number of observations)		Average coefficient Monetary reward	Visit frequency/ time savings	Error	Unauthorized secondary use	Improper access
United States	Privacy guardians	1.637***	0.027	4.040***	2.576***	5.116***
(78)[1]	(56)	(0.385)	(0.316)	(0.434)	(0.448)	(0.519)
	Information sellers	10.865***	–0.781	0.245	1.255**	–0.099
	(16)	(0.330)	(0.753)	(0.458)	(0.483)	(0.462)
	Convenience seekers	1.445	11.028***	1.500**	0.750*	0.542
	(6)	(0.781)	(0.613)	(0.348)	(0.371)	(0.945)
Number of outliers/unclassifiable observations: 6						
Singapore	Privacy guardians	0.464**	0.089	2.234***	5.734***	4.973***
(165)[1]	(138)	(0.195)	(0.166)	(0.183)	(0.318)	(0.314)
	Information sellers	11.286***	–0.714	0.107	1.768***	0.446
	(14)	(0.360)	(0.855)	(0.263)	(0.434)	(0.470)
	Convenience seekers	1.127	10.512***	0.404	1.077**	0.173
	(13)	(0.862)	(0.682)	(0.372)	(0.484)	(0.382)
Number of outliers/unclassifiable observations: 19						

Notes: Standard errors are shown in parentheses. [1] Number excluding outliers. *** Significant at the 1 percent level; ** significant at the 5 percent level;* significant at the 10 percent level.

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

Based on opinion surveys, Westin characterized 12 percent 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" [68, p. 16]. Interestingly, we found that 12.5 percent of the U.S. samples were "information sellers." However, our evidence is that information sellers demand a great deal more than "5 cents off." This point distinguishes our analysis from opinion surveys: we can estimate the dollar amount that information sellers must be paid for their personal information.

Further, our analysis revealed a cluster that Westin [68] 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 [68] differentiated between "privacy pragmatists" (63 percent) and "privacy fundamentalists" (25 percent) according to their sensitivities to privacy, whereas 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 subsegment 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 providing personal information to Web sites than privacy guardians ($t = 3.115$, $p < 0.01$). The information sellers' greater prior experience was consistent with their relatively high coefficients 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 Web sites.

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 Web sites 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 coefficients 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. This latter finding is particularly noteworthy, because cookies are useful for Web sites to provide personalized and convenient services to consumers and hence should a priori be welcomed by convenience seekers. The confirmation of this relationship provides face validity and enhances the confidence in our modeling approach and empirical findings.

Concluding Remarks

In this paper, we analyzed strategies that might mitigate online information privacy concerns. To that end, we applied the expectancy-based theory of motivation to define our research questions and hypotheses. Further, we linked the expectancy theory–based framework to the chosen methodology—the conjoint analysis. We empirically validated hypotheses based on the expectancy theory–based framework, which stipulates that individuals have positive valences for privacy protection policies, which increases the motivational score. Similarly, we confirmed the hypotheses that benefits such as financial rewards or convenience have a positive valence and increase the motivational score.

One important implication of this research is that organizations may possess means to actively manage the privacy concerns of Internet users. Our results distinctly show that privacy policies are valued by users. Hence, organizations can capitalize on this by stating their privacy policy more prominently. Often-cited benefits of increasing convenience are increased value offering through personalization [5] and lowering of frictional costs [30]. In addition, it appears that convenience also has a benefit that has been overlooked—namely, mitigating privacy concerns. Perhaps the least surprising result is that financial incentives are also a persuasive means to elicit personal information. However, this finding is consistent with anecdotal evidence that has shown that people are willing to disclose personal information for gifts and catalogs [50], and even a $100 drawing [38].

Our secondary set of research questions investigated the differences in privacy preferences. By applying cluster analysis to the subjects' marginal rankings of the various benefits and concerns (i.e., the valences), we found that our subjects can be categorized into three distinct segments—privacy guardians, information sellers, and convenience 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 personal information in exchange for money ("information sellers"), and an even smaller proportion were relatively willing to provide personal 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.

The immediate implication is that organizations with online presence must differentiate their services to serve these distinct segments to best meet the needs of segments with differing trade-offs among money, convenience, and privacy concerns.

Convenience seekers will be the first to register with a Web site 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 an individual's prior experience, they must use indirect methods to induce segmentation by self-selection [4, 49, 52]. Businesses could use monetary rewards to attract information sellers to provide personal information. Preferably, businesses would seek convenience seekers before enticing information sellers. By elimination, the individuals who do not respond to either monetary reward or convenience would be privacy guardians.

Privacy guardians represent the largest group in our study, and businesses do well to recognize their right to privacy as a necessary cost of doing business. AOL discovered this the hard way. After releasing 20 million "anonymized" search records of 658,000 users in early August 2006, AOL's search engine received 18.6 percent fewer queries. While intended for research purposes, AOL did not take into account that the search terms often contained personally identifiable information [3]. On the other hand, Google may have realized the importance of keeping its users' trust. Google successfully fended off Justice Department requests for some of its search data, whereas other companies (AOL, Microsoft, and Yahoo) complied [48]. Protecting privacy can provide Google with a competitive advantage over its competitors, while allowing Google to derive full value out of the search data.

Our findings are subject to a number of limitations that are common to many experimental settings. All of our subjects were undergraduate students. They are younger and probably more familiar with the Internet and e-commerce than the general 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. For all of these reasons, it would be important to verify our findings with a more representative sample of subjects.

We tested our hypotheses using experimental data collected from Singapore and U.S. subjects, which include students from diverse countries and cultures. Although our results are remarkably consistent across the two samples, future work could explore the possible influences of cultural values on individuals' preferences for privacy and positive reinforcements. Previously, using Hofstede's cross-cultural value indices [34], Milberg et al. [45] found that privacy concern is positively related to power distance, individualism, and masculinity, and negatively related to uncertainty avoidance. We do not have a priori information on the cultural values of our subjects. Therefore, it is infeasible for us to interpret our results in light of cultural differences. It would be interesting for future research to extend our findings and introduce cultural factors when studying decisions involving privacy trade-offs.

Further, the reported coefficients are sensitive to the specified attribute levels. For example, our conjoint stimuli specified only two levels for 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 US$1 reward. Future research may attempt to measure the impact of privacy policies and reward structures more directly.[23]

Acknowledgments: The authors thank the organizers, Eric Clemons, Rajiv Dewan, and Rob Kauffman, and the participants of the Twentieth Anniversary Symposium on Competitive Strategic, Economics, and Information Systems Research, held at the 2007 Hawaii International Conference on System Sciences, for valuable comments.

Notes

[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. See www.usdoj.gov/oip/04_7_1.html.

[2] For details of the 1998 Children's Online Privacy Protection Act, see www.ftc.gov/bcp/conline/edcams/coppa/index.html, and for the 2003 California Online Privacy Protection Act, see www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579.

[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 to 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. See www.internetnews.com/ec-news/article.php/4_471541 (September 28, 2000).

[4] In the context of online marketing, Chellappa and Sin [5] propose a conceptual model and construct several hypotheses to study Web-based personalization.

[5] For an application of the expectancy theory in organizational privacy, see Stone and Stone [61].

[6] The expectancy value approach has been successfully applied in information systems research surrounding user attitudes and satisfaction. A theoretical assessment is given by Melone [43]. Several empirical studies have applied expectancy theory to study computer usage [12, 23, 32, 36, 53, 57].

[7] For more insights on the potential detriments of unauthorized secondary use in the context of information exchanges, see Clemons and Hitt [6].

[8] Stewart and Segars [60] find that concern for information privacy is well measured by the four first-order constructs mentioned above. They also investigate and find support for a general second-order factor regarding information privacy.

[9] For instance, it is common for Web sites to offer shopping vouchers or discount coupons to first-time consumers who register as members; Amazon's "1-click ordering" facilitates quicker and easier transactions for customers who have previously provided personal information, such as delivery address and credit card profile.

[10] In the context of privacy in direct mail participation, Milne and Gordon [46] exposed subjects to a trade-off between compensation, targeting, volume, and permission.

[11] The subjects were told during the experiments that if they expected to visit the Web site 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 × 5 days a week × 50 weeks = 8 hours and 20 minutes); if they expected to visit the Web site weekly, the yearly saving would be 1 hour and 40 minutes; and if they expected to visit the Web site monthly, the yearly saving would be 24 minutes.

12. The monetary rewards were framed in the respective local currencies. At the time of the experiment, S$1 = US$0.54. Due to the currency differences, the effective ranges of monetary rewards differed between the U.S. and Singapore experiments—in U.S. dollars, the Singapore rewards were equivalent to US$2.70, US$5.40, and US$10.80, respectively.

13. The orthogonal design is a fractional factorial set, which is a sample of the full factorial set. The advantage of a fractional design is the lower cognitive burden on the participant. A full factorial design would require a ranking of 72 stimuli, which is an overwhelming task. With an orthogonal fractional design, the information on interaction effects is lost. In general, this is accepted practice. According to Louviere [41]: (1) the main effects explain the largest amount of variance in response data, often 80 percent or more; (2) two-way interactions typically account for only 3–6 percent of variance; and (3) three-way interactions or higher usually rarely account for more than 3 percent, typically between 0.5 and 1 percent.

14. We use dummy indicators instead of continuous variables to capture financial incentives ($5, $10, and $20) and convenience (monthly, weekly, and daily) in the regression because it is possible for consumers to exhibit nonlinear utilities toward these benefit outcomes [20, 31].

15. The advantage of rank ordering is that it is based on a theoretical approach to modeling decisions called *axiomatic conjoint measurement* [39, 42, 64]. Based on this theory, rank ordering can be used to derive estimates of the part-worths for each level of each attribute as originally discussed by Green and Wind [28]. From a practical point of view, the major advantage is that one does not have to assume that subjects use rating scales in an equal interval manner. Rather, one can make the weaker assumption of ordinality. It is easier for respondents to rank order stimuli than to rate them on a rating scale [26].

16. 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.

17. The lowest levels of each of the outcome variables act as experimental "controls" and hence are excluded when coding the dummy variables.

18. At the time of writing (end-April 2007), the U.S. dollar equivalents were US$3.20, US$6.59, and US$13.18, respectively.

19. 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.

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

21. We excluded a small number of subjects who could not be classified into any of the three clusters.

22. While the cluster size in an absolute sense is small, the relative size of the convenience seeker cluster to the overall U.S. sample (7.69 percent) is similar to relative size of the convenience seeker cluster to the overall Singapore sample (7.88 percent).

23. However, this may require a willingness of the businesses to share the kinds of data that they have promised not to share for secondary use.

References

1. Addelman, S. Orthogonal main-effect plans for asymmetrical factorial experiments. *Technometrics, 4,* 1 (February 1962), 21–46.

2. Andrews, S., and Shen, A. Public comment on barriers to electronic commerce. Response to call by U.S. Department of Commerce (65 Federal Register 15898). Electronic Privacy Information Center, U.S. Department of Commerce, Washington, DC, March 17, 2000 (available at www.epic.org/privacy/internet/Barriers_to_E-commerce.html).

3. Barbaro, M., and Zeller, T., Jr. A face is exposed for AOL searcher 4417749. *New York Times* (August 9, 2006) (available at www.freepress.net/news/16973).

4. Bhargava, H.K., and Choudhary, V. One size fits all? Optimality conditions for versioning and second-degree price discrimination. Working Paper, Pennsylvania State University, College Park, March 2002.

5. Chellappa, R., and Sin, R. Personalization versus privacy: New exchange relationships on the Web. Working Paper, ebizlab, Marshall School of Business, University of Southern California, Los Angeles, May 2002.

6. Clemons, E.K., and Hitt, L.M. Poaching and the misappropriation of information: Transaction risks of information exchange. *Journal of Management Information Systems, 21,* 2 (Fall 2004), 87–107.

7. Cox, D.F., and Rich, S.U. Perceived risk and consumer decision-making: The case of telephone shopping. *Journal of Marketing Research, 1,* 4 (November 1964), 32–39.

8. Culnan, M.J. How did they get my name? An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quarterly, 17,* 3 (September 1993), 341–363.

9. Culnan, M.J., and Armstrong, P.K. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10,* 1 (January–February 1999), 104–115.

10. Culnan, M.J., and Bies, R.J. Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59,* 2 (2003), 323–342.

11. Debreu, G. Topological methods in cardinal utility theory. In S. Karlin, K.J. Arrow, and P. Suppes (eds.), *Mathematical Methods in the Social Sciences.* Palo Alto, CA: Stanford University Press, 1960, pp. 16–26.

12. DeSanctis, G. Expectancy theory as explanation of voluntary use of a decision support system. *Psychological Reports, 52,* 1 (1983), 247–260.

13. Donnenwerth, G.V., and Foa, U.G. Effect of resource class on retaliation to injustice in interpersonal exchange. *Journal of Personality and Social Psychology, 29,* 6 (1974), 785–793.

14. Dowling, G.R., and Staelin, R. A model of perceived risk and intended risk-handling activity. *Journal of Consumer Research, 21,* 1 (June 1994), 119–134.

15. Eddy, E.R.; Stone, D.L.; and Stone-Romero, E.F. The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology, 52,* 2 (Summer 1999), 335–358.

16. Emerson, R.M. Exchange theory, Part II: Exchange relations and network structures. In J. Berger, M. Zelditch Jr., and B. Anderson (eds.), *Social Theories in Progress.* Boston: Houghton Mifflin, 1972, pp. 58–87.

17. Esrock, S.L., and Ferre, J.P. A dichotomy of privacy: Personal and professional attitudes of marketers. *Business and Society Review, 104,* 1 (Spring 1999), 107–120.

18. 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). Brussels, 1995.

19. Foa, U.G. Interpersonal and economic resources. *Science, 171* (January 29, 1971), 345–351.

20. Friedman, M., and Savage, L.J. The utility analysis of choices involving risk. *Journal of Political Economy, 56,* 4 (August 1948), 279–304.

21. Fusilier, M.R., and Hoyer, W.D. Variables affecting perceptions of invasion of privacy in a personnel selection situation. *Journal of Applied Psychology, 65,* 5 (1980), 623–626.

22. Goffman, E. *The Presentation of Self in Everyday Life.* Garden City, NY: Doubleday, 1959.

23. Goodhue, D. Supporting users of corporate data: The effect of IS policy choices. Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 1988.

24. Goodwin, C. Privacy: Recognition of a consumer right. *Journal of Public Policy and Marketing, 10,* 1 (Spring 1991), 149–166.

25. Green, P.E., and Krieger, A.M. Segmenting markets with conjoint analysis. *Journal of Marketing, 55,* 4 (October 1991), 20–31.

26. Green, P.E., and Srinivasan, V. Conjoint analysis in consumer research: Issues and outlook. *Journal of Consumer Research, 5,* 2 (1978), 103–123.

27. Green, P.E., and Srinivasan, V. Conjoint analysis in marketing: New developments with implications for research and practice. *Journal of Marketing, 54,* 4 (1990), 3–19.

28. Green, P.E., and Wind, Y. New ways to measure consumer judgments. *Harvard Business Review, 53,* 4 (July–August 1975), 107–117.

29. Hair, J.F.; Tatham, R.L.; Anderson, R.E.; and Black, W.C. *Multivariate Data Analysis with Readings.* Englewood Cliffs, NJ: Prentice Hall, 1998.

30. Hann, I.H., and Terwiesch, C. Measuring the frictional costs of online transactions: The case of a name-your-own-price-channel. *Management Science, 49,* 11 (November 2003), 1563–1579.

31. Hartley, R., and Farrell, L. Can expected utility theory explain gambling? *American Economic Review, 92,* 2 (June 2002), 613–624.

32. Hill, T.; Smith, N.D.; and Mann, M.F. Role of efficacy expectations in predicting the decision to use advanced technologies: The case of computers. *Journal of Applied Psychology, 72,* 2 (1987), 307–313.

33. Hirschman, E.C. People as products: Analysis of a complex marketing exchange. *Journal of Marketing, 51,* 1 (January 1987), 98–108.

34. Hofstede, G.H. *Cultures and Organizations.* Berkshire, UK: McGraw-Hill, 1991.

35. Homans, G.C. *Social Behavior: Its Elementary Forms.* New York: Harcourt Brace Jovanovich, 1974.

36. Howard, G.S., and Mendelow, A.L. Discretionary use of computers: An empirically derived explanatory model. *Decision Sciences, 22,* 2 (1991), 241–265.

37. Jourard, S.M. Some psychological aspects of privacy. *Law and Contemporary Problems, 31* (Winter 1966), 307–318.

38. Jupiter Media Metrix. Seventy percent of U.S. consumers worry about online privacy, but few take protective action. Press Release, June 3, 2002.

39. Krantz, D.H., and Tversky, A. Conjoint measurement analysis of composition rules in psychology. *Psychology Review, 78,* 2 (March 1971), 151–169.

40. Laufer, R.S., and Wolfe, M. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33,* 3 (1977), 22–42.

41. Louviere, J.L. *Analyzing Decision Making: Metric Conjoint Analysis.* Newbury Park, CA: Sage, 1988.

42. Luce, R.D., and Tukey, J.W. Simultaneous conjoint measurement: A new type of fundamental measurement. *Journal of Mathematical Psychology, 1,* 1 (January 1964), 1–27.

43. Melone, N.P. A theoretical assessment of the user-satisfaction construct in information systems research. *Management Science, 36,* 1 (1990), 76–91.

44. Milberg, S.J.; Burke, S.J.; and Smith, H.J. Values, personal information privacy, and regulatory approaches. *Communications of the ACM, 38,* 12 (1995), 65–74.

45. Milberg, S.J.; Smith, H.J.; and Burke, S.J. Information privacy: Corporate management and national regulation. *Organization Science, 11,* 1 (2000), 35–57.

46. Milne, G.R., and Gordon, M.E. Direct mail privacy–efficiency trade-offs within an implied social contract. *Journal of Public Policy and Marketing, 12,* 2 (Fall 1993), 206–215.

47. Mitchell, T., and Beach, L. Expectancy theory, decision theory, and occupational preference and choice. In M.F. Kapalan and S. Schwartz (eds.), *Human Judgment and Decision Processes in Applied Settings.* New York: Academic Press, 1977, pp. 203–226.

48. Mohammed, A. Google refuses demand for search information. *Washington Post* (January 20, 2006), A1.

49. Moorthy, K.S. Market segmentation, self-selection, and product line design. *Marketing Science, 3,* 4 (Fall 1984), 288–307.

50. Oberndorf, S. Registering for success. *Catalog Age, 16,* 13 (1999), 47–48.

51. Organization for Economic Cooperation and Development. Guidelines on the protection of privacy and transborder flows of personal data. Paris, September 23, 1980 (available at www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).

52. Png, I. *Managerial Economics.* Malden, MA: Blackwell, 2002.

53. Robey, D. User attitudes and management information systems use. *Academy of Management Journal, 22,* 3 (1979), 527–538.

54. Schwartz, J. Giving the Web a memory cost its users privacy. *New York Times* (September 4, 2001) (available at www.taborcommunications.com/dsstar/01/0911/103486.html).

55. Simmons, D.D. Invasion of privacy and judged benefit of personality-test inquiry. *Journal of General Psychology, 79* (1965), 77–81.

56. Smith, H.J.; Milberg, S.J.; and Burke, S.J. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly, 20,* 2 (June 1996), 167–196.

57. Snead, K.C., and Harrell, A.M. An application of expectancy theory to explain a manager's intention to use a decision support system. *Decision Sciences, 25,* 4 (1994), 499–513.

58. Spiekermann, S.; Grossklags, J.; and Berendt, B. E-privacy in 2nd generation e-commerce: Privacy preferences vs. actual behavior. In M.P. Wellman and Y. Shoham (eds.), *Proceedings of the Third ACM Conference on Electronic Commerce.* New York: ACM Press, pp. 38–47.

59. Stahl, M.J., and Harrell, A.M. Modeling effort decisions with behavioral decision theory: Toward an individual differences model of expectancy theory. *Organizational Behavior and Human Performance, 27,* 3 (1981), 303–325.

60. Stewart, K.A., and Segars, A.S. An empirical examination of the concern for information privacy instrument. *Information Systems Research, 13,* 1 (March 2002), 36–49.

61. Stone, E.F., and Stone, D.L. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. In K.M. Rowland and G. Ferris (eds.), *Research in Personnel and Human Resources Management,* vol. 8. Greenwich, CT: JAI Press, (1990), pp. 349–411.

62. Stone, E.F.; Gueutal, H.G.; Gardner, D.G.; and McClure, S. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology, 68,* 3 (1983), 459–468.

63. Tolchinsky, P.D.; McCuddy, M.K.; Adams, J.; Ganster, D.C.; Woodman, R.W.; and Fromkin, H.L. Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology, 66,* 3 (1981), 308–313.

64. Tversky, A. A general theory of polynomial conjoint measurement. *Journal of Mathematical Psychology, 4,* 1 (February 1967), 1–20.

65. Vriens, M.; Wedel, M.; and Wilms, T. Metric conjoint segmentation methods: A Monte Carlo comparison. *Journal of Marketing Research, 33,* 1 (1996), 73–85.

66. Vroom, V.H. *Work and Motivation.* New York: Wiley, 1964.

67. Westin, A. *Privacy and Freedom.* New York: Atheneum, 1967.

68. Westin, A. Opinion Surveys: What Consumers Have to Say About Information Privacy. Testimony before U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, Washington, DC, May 8, 2001 (available at http://energycommerce.house.gov/reparchives/107/hearings/05082001Hearing209/Westin309.htm).

69. Woodman, R.W.; Ganster, D.C.; Adams, J.; McCuddy, M.K.; Tolchinsky, P.D.; and Fromkin, H. A survey of employee perceptions of information privacy in organizations. *Academy of Management Journal, 25,* 3 (1982), 647–663.

Appendix: Stimuli Example for Conjoint Analysis—Financial Portal

Subjects were given the following introduction:

Financial portals offer online, real-time stock trading and price quotation services. Their services for members include up-to-the-minute stock price quotations, stock order placements and executions, and professional advice on portfolio management. In order to use their services, you need to create an account by providing personal information as well as a login and password.

The account record can save time for members when they request stock price quotations and market analyses. Further, portfolio management is faster and easier when the portals store members' stock portfolios and preferences. Financial portal members may also receive discounts on commission fees (for stock transactions) and service fees (for stock price quotations).

By providing personal information to a financial portal, you gain potential benefits but lose some extent of privacy. The impact on your privacy depends on the portal's policy. Since the portal retains all member information, there is a chance that member information may be stored with errors or, after a certain period of time, become outdated. Further, the portal may use member information for other purposes, such as analyzing the member's Web usage patterns. Finally, it is possible that unauthorized persons (intentionally or unintentionally) get access to the personal information stored in a portal.

All of the portals ask members for the following personal information during registration:

- name
- home address
- phone number
- e-mail address
- credit card information
- household income
- current stock portfolio
- previous stock trading experience

Consider a selection of financial portals that differ in their privacy policies and the benefits that they possibly provide. For the purpose of this exercise, assume that all financial portals offer the features that you value. In the following screens, we describe the various dimensions that you may regard as important when deciding which financial portal to sign up with.

First Dimension: Promotion

Promotions are often offered to provide customers an incentive to try out a new product or service. Financial portals typically offer a discount on the commission fee for the first stock transaction. For our scenarios, the financial portals offer a discount of $5, $10, or $20. This is a one-time promotion.

Second Dimension: Time Savings

Consumers vary in their visit frequency. For our scenarios, we ask you to think of yourself as a customer that visits the financial portal either once a day, once a week, or once a month. The financial portal will keep a record of your stock portfolio and will list the current stock prices after you log on to the Web site.

While this requires giving up some personal information, registering saves you time when inquiring about stock prices. For example, assume that it would take you 3 minutes to find and key in all stock symbols manually (without registration) and that it would take 1 minute to log in to the financial portal. If you visit the financial portal daily, it takes 2 minutes longer to key in all stock symbols than logging in to the Web site, so you will save 8 hours and 20 minutes in a year (2 minutes × 5 days a week × 50 weeks) when you register with the financial portal. If you visit the financial portal weekly, you will save 1 hour and 40 minutes per year when registering over typing it in manually. If your visit frequency is monthly, you will save 24 minutes per year.

Third Dimension: Secondary Use

Web sites may state in their privacy policy what they intend to do with your personal information and your interaction with the Web site. For example, the financial portal may analyze your Web usage data to optimize the Web site design or to learn about your preferences for products or services. These types of analyses are called "secondary use," as they do not facilitate the primary purpose of the financial portal, which is providing financial information and executing transactions. For our scenarios, the financial portal will state either that your information will not be used for any purpose other than facilitating stock quotations and transactions (i.e., no secondary use) or that your information may be analyzed for other purposes, such as revealing your Web usage preferences.

Fourth Dimension: Error

Web sites often allow customers to review their personal information after it is saved. This option is often provided to correct mistakes or update personal information. However, many Web sites do not offer this option at this point. For our purpose, the scenarios will state that the financial portal will either provide no opportunity to review your personal information for mistakes or provide the option to review your personal information and correct mistakes.

Fifth Dimension: Improper Access

Web sites typically guard the data from intrusion from the outside. However, within a company, the data is often accessible to many people in various departments. For example, the personal data may be accessed by the information technology department, which stores the data, as well as by the marketing and sales department, which may use the data to tailor their offerings. Some online retailers restrict access to the data internally to authorized personnel. These people often have training in privacy issues. For our purpose, the scenarios will state that the financial portal will either have no policy on access to personal information or provide access to personal information only to authorized personnel.

The following scenarios describe portals that differ in the privacy policy and your anticipated usage of the portal. Here is a summary of the portal characteristics:

1. *Promotion.* For signing up you obtain a discount on commission fees from the financial portal for your first stock transaction. The financial portal offers a discount of

- $5
- $10
- $20

2. *Time savings.* You anticipate to be a repeat visitor of the portal to obtain stock price information or place stock orders and sign up to save time. You estimate that you will return to the financial portal either:

- once a day, realizing time savings of 8 hours and 20 minutes per year
- once a week, realizing time savings of 1 hour and 40 minutes per year
- once a month, realizing time savings of 24 minutes per year

3. *Secondary use.* Regarding the use of your personal information, the portal will state either:

- your information will not be used for any purpose other than facilitating stock quotations or transactions
- your information may be analyzed for other purposes, such as revealing your Web usage preferences

4. *Error.* The financial portal will provide either:

- no option to review your personal information for mistakes
- option to review your personal information and correct mistakes

5. *Improper access.* Regarding the access to your personal information, the portal will state either:

- no policy on access to personal information
- access to personal information only by authorized personnel from within the company, who have been trained in privacy issues

Below you should see a list of 18 choices that are described by various combinations of the above five attributes.

Sort the following 18 descriptions of financial portals from “most preferred” to “least preferred” by clicking on a choice and dragging it up or down in the list.