The Value of Privacy Assurance: An Exploratory Field Experiment

Kai-Lung Hui [‡], Hock Hai Teo[*], Sang-Yong Tom Lee[**]

Revised, July 2006

Abstract

This paper reports the results of an exploratory field experiment in Singapore that assessed the values of two types of privacy assurance – privacy statements and privacy seals. We collaborated with a local firm to host the experiment on its website with its real domain name, and the subjects were not informed of the experiment. Hence, it provided a field observation of the subjects' behavioral responses toward the privacy assurances. We found that: (1) the existence of a privacy statement induced more subjects to disclose their personal information but that of a privacy seal did not; (2) monetary incentive had a positive influence on disclosure; and (3) information request had a negative influence on disclosure. These results were robust in other specifications that used alternative measures for some of our model variables. We discuss this study in relation to the extant privacy literature, most of which employs surveys and laboratory experiments for data collection, and draw related managerial implications.

Key words: Privacy assurance, field experiment, privacy statement, privacy seal, monetary incentive, information request

Forthcoming, MIS Quarterly

[‡] Department of Information Systems, City University of Hong Kong, and Department of Information Systems, National University of Singapore.
[*] Department of Information Systems, National University of Singapore
[**] College of Information and Communications, Hanyang University

We gratefully thank all seminar participants at the City University of Hong Kong, the senior and associate editors, and the reviewers for their helpful comments and suggestions.

1. Introduction

The collection of personal information from consumers is to-date an unavoidable element of electronic commerce. Internet merchants need consumer information to deliver products, study customer profiles, and offer personalized services. For consumers, such information collection by Internet merchants has both benefit and risk implications. In terms of benefits, it is now possible for consumers to access more convenient services and save transaction time and search costs (Amazon's 1-click shopping and personalized recommendations are good examples of such services). In terms of risk, unlike conventional retailing, consumers cannot remain anonymous in Internet transactions: Their data are revealed to Internet merchants, and they hence face a new spectrum of risks of information misuse, such as transfer of their data to third parties, or use of their data in unintended ways (price discrimination, marketing solicitations, etc.).[1] The decision of whether to provide personal information to Internet merchants relies largely on an assessment of these benefits and risks (Laufer and Wolfe 1977).

The risks of information misuse for consumers are lower if firms adopt fair information practices (FIP) (Culnan and Bies 2003). The scope of FIP varies across governments, but most FIP guidelines highlight basic features including limiting collection to data relevant to a transaction, providing sufficient notice, choice, and access mechanisms, and protecting consumer data with adequate security measures.[2] To inform consumers that FIP are followed, many

[1] The provision of personal information to facilitate marketing transactions is called "second exchange" (cf. first exchange between money, goods, and services) (Culnan and Milberg 1998). Smith et al. (1996) classify information risks and hence consumers' privacy concerns into four dimensions – collection, error, unauthorized secondary use, and improper access.

[2] In Singapore (where this study was conducted), an industry consortium called the National Trust Council (NTC) leads the development and promotion of FIP, with support from the Infocomm Development Authority of Singapore, a statutory board of the Singapore government. The Singapore version of FIP comprises 10 principles: (1) accountability; (2) specifying purposes; (3) consent; (4) limiting collection; (5) limiting use, disclosure and retention; (6) accuracy; (7) safeguards; (8) openness; (9) individual access and correction; and (10) challenging compliance (National Trust Council 2005). These are essentially modeled after the framework proposed by the Organization for Economic Co-operation and Development (OECD).

websites publish privacy statements, which describe their policies regarding collected consumer information. Some also display privacy seals issued by independent third parties (*BBBOnline*, *Truste*, *Trustsg*, etc.).[3,4]

In principle, privacy statements and privacy seals help consumers make a more accurate assessment of the risks of disclosing personal information to websites, and therefore displaying them should promote consumer disclosure (Milne and Culnan 2004). A basic premise for these privacy assurances to function as intended, however, is that consumers trust and value them. How do we know that this is the case now? Given the popularity of these privacy assurances (see, e.g., footnote 3), it is surprising that there is little research assessing their influences on consumer behavior. Our research questions are therefore posed as follows:

Do consumers value privacy statements and privacy seals? If so, do they affect consumer disclosure of personal information?

We conducted an exploratory *field experiment* to address these questions. Specifically, we varied the provision of privacy assurance among three levels of treatments and recorded how consumers responded to each of them. The treatments were: (1) no information was given about whether a firm followed FIP; (2) a privacy statement outlining the firm's data policy was displayed; and (3) in addition to the privacy statement, a *Truste* privacy seal was displayed. These treatments were randomly shown to a group of subjects who were asked to browse a website and provide some personal information and opinion to our partner firm, which specialized in market research in Singapore. The experimental website was hosted under the

[3] For a summary of display of privacy statements and privacy seals on popular U.S. and U.K. websites, see Federal Trade Commission (2000) and Jamal et al. (2003, 2005). In Singapore, the NTC issues the *Trustsg* mark to websites that comply with a set of code of practice (including FIP). Among 36 Singapore websites that had highest traffic in September 2005 (as listed on http://www.getforme.com/trafficranksingaporewebsites.htm) and that were accessible at the time of writing this paper, 27 published a privacy statement and 9 displayed a privacy seal.

[4] Throughout this paper we call privacy statements and privacy seals "privacy assurances". Similarly, we use the words "data" and "information" synonymously.

firm's homepage and carried the firm's domain name; only the firm (but not the authors of this paper) interacted with the subjects. The subjects were not informed of the experiment, and therefore their responses should reflect their true preferences given the privacy assurances presented to them.

We further manipulated two factors in the experiment, monetary incentive and information request. This was because, as mentioned above, consumers may perform a risk-benefit tradeoff when deciding whether to disclose their personal data, and monetary incentive is the most straightforward benefit that can be conveniently manipulated. Previous research has found that monetary incentive affects consumer preferences for privacy (Hann et al. 2002; Milne and Gordon 1993). By incorporating it in our experiment, we could infer whether a risk-benefit tradeoff is indeed performed for privacy, and whether privacy assurance is "tradable" by consumers. Similarly, information requests affect the risk side of the privacy tradeoff, and hence should reduce the extent of consumer disclosure (Hine and Eve 1998; Nowak and Phelps 1997; Phelps et al. 2000). Because consumer information is requested in most online transactions, it is worthwhile to assess its impact in our experiment.

This study is generally related to the literature of privacy concern and FIP (Culnan 1993; Culnan and Armstrong 1999; Hoffman et al. 1999; Phelps et al. 2000), which has suggested that consumers are less concerned if proper steps are taken to assure their privacy. Hence, firms are advised to follow FIP and communicate their information policies and commitments effectively to consumers (Culnan and Bies 2003; Milne and Culnan 2004).

Existing privacy research, however, lacks empirical observation of consumers' *behavioral responses* in *real online settings*. Past privacy studies have mostly employed surveys, wherein consumers were asked to respond to hypothetical scenarios. There are two weaknesses to such approaches. First, directly prompting consumers with questions about privacy may lead to biased responses: People may inflate their concerns and emphasize protective measures if they are asked to provide "cheap" opinions (Harper and Singleton 2001). Thus, these opinions may not reflect their true attitude toward information privacy. Second, survey responses may not be indicative of final choices (see, e.g., Berendt et al. 2005). When evaluating privacy assurances, it is important to observe consumer choices in field settings. Since such observations are missing from extant literature, our research represents a first step in this direction.

2. Theory

Contemporary choice theory assumes that people make choices by maximizing a utility function that is decomposable into multiple contributors (Ben-Akiva and Lerman 1985; Luce 1959; McFadden 1986, 2001). These contributors – often called *attributes* of choice alternatives – may comprise both economic (e.g., money, time) and psychological factors (e.g., pleasure, risks), and they are *compensatory* in nature, i.e. the utility due to desirable attributes may offset the disutility due to undesirable ones. In other words, people make tradeoffs among attributes, and this could occur in privacy choices as well (see, e.g., Dinev and Hart 2006; Hann et al. 2002; Laufer and Wolfe 1977).

In online transactions, the request for personal data from consumers may create disutility, because people are inclined to avoid unwanted disclosure (Goodwin 1991, 1992). This could be due to the risks of information misuse: Once a firm possesses consumer data, it is difficult for consumers to remove them or control their future use.

To reduce the disutility caused by data collection, obviously, firms need to commit to use consumer data responsibly, and should convey these commitments to consumers. This could be achieved, for example, by displaying a privacy statement or privacy seal, which may reduce consumers' perceived risks of information disclosure and hence raise their utility of trading with the firms. Since utility is decomposable, and, more important, compensatory, privacy assurance may offset undesirable attributes, such as requests to provide more personal data. Similarly, monetary incentives may offset information requests or a lack of privacy assurances.[5]

3. Methodology

We designed a field experiment for this research. Specifically, we invited a group of subjects by electronic mail (email) to visit our experimental website (which was hosted by a Singapore firm that specialized in market research) to fill out a survey about mobile computing products.[6] We assigned a unique one-time access code to each invited subject to prevent repeated participation (i.e., subjects had to enter a valid code before they could access the survey). We did not reveal the experiment to subjects, and we presented the three treatments – privacy assurance, monetary incentive, and information request – to subjects only after they entered a valid access code.

The survey contained some *mandatory* information items that subjects were required to provide to complete their participation, and a set of *optional* questions about mobile computing products. The optional questions were included to disguise the study's purpose; answers to these questions were not used in the analysis. Subjects were told that their responses to the survey would help design future products and promotions.

Regardless of whether subjects completed the survey (which required them to provide all requested mandatory items), a follow-up survey was posed to elicit some necessary information

[5] This discussion assumes that consumers make rational tradeoffs. For the purpose of our analysis, however, we do not require every consumer to make privacy tradeoffs – we could allow for the existence of some "stubborn" consumers. For empirical evidence, see Westin (2001), who found three types of consumers: privacy unconcerned, privacy fundamentalists, and privacy pragmatists. The last type, who constituted the largest segment of Westin's sample, consists of the people who would most likely make privacy tradeoffs. See, also, Acquisti (2004) for an interesting analysis on why some people are willing to give up privacy for seemingly small rewards. Such people may correspond to Westin's privacy unconcerned consumers.

[6] The webpages used for this experiment are available from the authors upon request.

including manipulation checks, past experiences, etc. To encourage subjects to do the follow-up survey, we gave each of them 20 Singapore dollars (≈ US$12) as a participation incentive. This was considered sufficient as the follow-up survey required only 10 to 15 minutes of effort, and asked mostly for personal opinions. It was therefore less intrusive than the main survey, which requested sensitive data such as name and household income.

Manipulations

We created three scenarios for privacy assurance: (1) no assurance; (2) assurance by means of a privacy statement; and (3) assurance by means of both a privacy statement and privacy seal. The website of our partner firm was certified by *Truste*, which was among the most popular privacy seals used by online firms. Because scenario (3) encompassed scenario (2), the extent of privacy assurance presented to subjects followed an ascending order (i.e., (1) < (2) < (3).[7])

For the monetary incentives, once subjects arrived at the experimental website, we informed them that they would receive a check upon completing the (main) survey. The value of the check was not disclosed in the invitation email, but was revealed only after subjects arrived at the website. It varied from one to nine Singapore dollars (US$0.60 to US$5.40). The check (and a separate check for 20 Singapore dollars if a subject also completed the follow-up survey) was mailed to each subject after the experiment by our partner firm.

Finally, we manipulated the information requests by varying the number of *mandatory* items in the main survey. Each subject was asked to disclose between 4 and 23 pieces of personal information (the complete list of items is reported in Appendix A). We ordered the items so that the longer treatments always encompassed the shorter ones. The base treatment

[7] Note that for the privacy assurances to function, consumers must read or notice the existence of the assurances. See Milne and Culnan (2004) for a first attempt to investigate what makes people read online privacy notices. We used the *Truste* seal because it was better known than the local privacy seals in Singapore (see Section 4).

asked for only name, email, address, and citizenship. The next treatment added gender, then marital status, ethnicity, and so on. This helped ensure effective variation in information requests across subjects.

Note that two information characteristics, *quantity* and *sensitivity*, were implicitly varied when we requested for different sets of items.[8] Our manipulation of how much information was requested (and, for that matter, any other manipulations that involve varying the number of items) encompassed changes in both quantity and sensitivity at the same time, but it was useful to separately assess their effects on consumer disclosure. To do that, we asked subjects to rate the sensitivity of each *mandatory* item that they were asked to provide on a seven-point scale (not sensitive to extremely sensitive) in the follow-up survey. We used these scores (see Appendix A) later in the data analysis to determine the influence attributable to information sensitivity (cf. quantity, which was directly captured by number of items).

To summarize, we composed different experimental stimuli by using one of the three levels of privacy assurance, providing one to nine dollars of incentive, and requesting 4 to 23 pieces of personal information. The experimental stimuli were randomly generated using a uniform probability distribution and assigned to subjects when they arrived at the website. We controlled for information sensitivity in the follow-up survey.

Controls

We collected additional data in the follow-up survey and used them as control variables in the subsequent analysis. The measurement items for these control variables are presented in the first table in Appendix B. First, we measured subjects' propensity to trust others with two seven-

[8] The relevance of the requested items may also affect consumer disclosure. In our experiment, because we needed to pay subjects, the first three items – name, email, and address – were obviously relevant. The other 20 items were not directly relevant to the experimental task. Because we requested for the first three items from *every* subject and varied the requests only for the other 20 items, relevance may not pose a significant threat to our findings.

point Likert scale items (all Likert scale items in this study had the anchors 1 = totally disagree and 7 = totally agree). Trust propensity may affect subjects' confidence in our partner firm and hence their extent of disclosure in the experiment (Culnan and Bies 2003).

Second, we asked subjects whether they had prior experience with personal information misuse. The social exchange theory (Emerson 1972; Homans 1974) posits that the value of social reward or cost to a person depends on how often and how recently the reward or cost was incurred. If a person has recently encountered a cost (e.g., information misuse), then she is less likely to perform actions (e.g., registering with a website) that impose a similar cost. Therefore, we expect less disclosure from subjects who have experienced information misuse.

Third, prior Internet shopping experiences may affect consumer choice. Consumers who have shopped online are more familiar with Internet transactions and the implications of information disclosure. Such familiarity may reduce the cognitive effort needed to perform similar tasks (in our experiment, answering the survey from our partner firm and disclosing certain personal data). This may make the tasks more acceptable to consumers (Alba and Hutchinson 1987; Ratchford 2001). Further, people exhibit various preferences for privacy and online shopping (Laufer and Wolfe 1977; Stone and Stone 1990). Their past online shopping experiences and responses in our experiment may correlate because of such idiosyncratic preferences. Hence, to take into account these (familiarity and preference) effects, we included an item to check if subjects had shopped on the Internet in the past 12 months.

Finally, we measured subjects' privacy concerns by two means. First, we asked them to indicate the cookie setting in their Internet browser, and grouped those who changed the setting to more stringent ones as being more privacy-concerned. Second, we adapted eight questions from the study conducted by Smith et al. (1996). These two measures were included separately into the data analysis. Generally, we expect subjects who were more privacy-concerned to show less positive responses (i.e., were less likely to disclose personal information).

Subjects

Our sampling frame consisted of 600 business students at a large Singapore university who had no previous transaction history with our partner firm. An email was sent by the firm to these 600 students to invite them to fill in a survey. Over two weeks, 137 students visited the experimental website and, among them, 109 completed the experiment. The remaining 28 did not complete the follow-up survey; in fact, 20 of them did not give us any information. Hence, we were not able to collect the necessary data (control variables, manipulation checks, etc.) from them for our analysis.[9] Accordingly, the overall response rate was 18.2%, which was considered acceptable, since people often delete solicitation emails (Pitkow and Kehoe 1996).

Table 1 presents descriptive statistics of the 109 subjects who completed the experiment, and the treatments that they received. On average, the subjects were 24 years old; the age range was 21-28. Fifty-three percent were female. Because these subjects responded to our invitation email, they could be more receptive to email solicitations and performing Internet transactions. Hence, there could be a self-selection bias in our sample.[10] It is important for readers to take note of this sampling bias when interpreting the subsequent results.

[9] These 28 subjects received similar treatments as the other 109 subjects – the average incentive that they received was $5.25 (cf. $4.76 for the other 109 subjects); the average number of items requested was 13.25 (cf. 13.41); 75% of them were presented a privacy statement (cf. 65%); and 36% of them were presented a privacy seal (cf. 27%). All of these differences were statistically insignificant. Hence, the non-response of these 28 subjects was not related to our treatments.

[10] Specifically, we stated in the email that the purpose of the survey was to seek respondents' views and opinions on mobile devices, and that we would provide a monetary reward to those who complete the survey. This could have led to a sampling bias in that we could have drawn people who were more prone to the influence of monetary incentive, or who were more eager to share their views and opinions. Nevertheless, we *did not* mention the collection of personal information or present the treatment levels in the email. The subjects were asked to provide personal information and received the treatments (including the actual amount of money provided for completing the

<Insert Table 1 here>

4. Results

Responses to a seven-point Likert scale item in the follow-up survey indicated that the subjects were familiar with the *Truste* privacy seal (mean = 6.58, standard deviation = 0.87). This was much higher than their familiarity with local privacy seals (mean = 2.62, standard deviation = 1.77), which suggested that our choice of the *Truste* seal for the experiment was appropriate (the familiarity measures are presented in the last table in Appendix B).

Manipulation Checks

We used various items, which are reported in the second table in Appendix B (together with a summary of the subjects' responses), to verify the salience of our treatments. First, all the 109 subjects correctly indicated the existence or absence of the privacy assurances, which confirmed their awareness of the assurances. Further, it appeared that those who were presented the privacy assurances had gone through them and understood their purposes.

Second, we included two seven-point Likert scale items to assess the manipulation of monetary incentive. A regression of the subjects' responses on the provided monetary incentives yielded a positive coefficient of 0.08, but it was insignificant (p = 0.14). This could have been caused by badly worded items.[11] However, as we shall illustrate below, monetary incentive had a positive and significant influence on the subjects' disclosure. Hence, the monetary treatments were effective, despite the inappropriate manipulation check items.

survey) *only after they had entered a valid access code at the website.* Hence, their decision to visit the website should *not* be related to their information privacy concern or our experimental treatments.

[11] Specifically, we used phrases such as "effort and time" and "worth the information that I give" in the questions, which might have inadvertently affected the subjects' responses. The subjects might have indicated the overall effectiveness (an outcome measure) rather than their perceived level of monetary incentives. We thank the associate editor for pointing out this problem and the explanation.

Finally, we also employed two seven-point Likert scale items to verify the manipulation of information request. A regression of the subjects' responses on the number of items requested yielded a positive coefficient of 0.10 ($p < 0.01$). Hence, the manipulation was successful.

The Basic Model

To complete the main survey, subjects were required to provide all requested mandatory items. Hence, their choice was discrete (to disclose or not to disclose), and we fitted their responses to a logit function, with "disclosure" as a *binary* dependent variable. The independent variables comprised the three manipulated treatments (privacy assurance, monetary incentive, and information request), average information sensitivity across the items rated by each subject, and the four control variables. The estimation results are reported in Table 2, column 1. Of the 109 subjects, 86 disclosed the requested data.

<Insert Table 2 here>

The explanatory variables were jointly significant, with a likelihood ratio test statistic of 38.20 ($p < 0.01$, d.f. = 9). The Hosmer-Lemeshow (1989) goodness-of-fit test showed that the model fitted the data reasonably well (χ-square = 12.12, d.f. = 8, $p = 0.15$). Also, the McFadden R-square was 0.34, indicating moderate explanatory power of our model.

The coefficient for privacy statement was positive and marginally significant, and that for privacy seal was positive but insignificant. Monetary incentive had a positive coefficient, and the number of items requested had a negative coefficient. Both of them were statistically significant. The coefficient for information sensitivity was negative but insignificant.

The signs of the control variables were consistent with a priori expectations. People who tended to trust others or who had previous Internet shopping experience were more likely to disclose the requested information, whereas those who had information misuse experience were less likely to disclose. The coefficient of privacy concern (as measured by cookie preference settings) was negative but insignificant.

Robustness

We tested a few alternative specifications. First, our basic model controlled for the effect of information sensitivity by including the *average* sensitivity score across the items rated by each subject as an independent variable. However, several requested items (e.g., identity card number, personal debt) were quite sensitive, and it was possible for the subjects to change their behavior upon being asked for such items. To account for this, instead of using average sensitivity score, we used the *highest* sensitivity score (as rated by a subject for her set of items) as an independent variable. The new results are reported in Table 2, column 2.

Next, we used the scores obtained from the measures developed by Smith et al. (1996) in place of cookie preference setting for privacy concern. The results are reported in Table 2, column 3. Generally, the results of these two alternative specifications were similar to those obtained from the basic model, which strengthens the confidence in our basic findings.

Alternative Explanations

We found that privacy statements exerted a marginally significant positive effect on disclosure. One possible explanation of this effect being weak is that the subjects did not read the privacy statement in detail (Milne and Culnan 2004). To test this explanation, instead of using the privacy statement variable directly, we multiplied it with the subjects' responses to the item: "*I have read through Company X's privacy statement and understood it fully*" (mean = 4.62, standard deviation = 1.47), and used the new variable in place of the original in the regression. The results are reported in Table 2, column 4. Although the coefficient changed considerably because of the multiplication, it remained close to marginally significant (p = 0.10). Hence, taking into account the subjects' understanding of the privacy statement did not change our findings.

Similarly, we found privacy seal to have an insignificant positive effect. Could this be due to the Singapore subjects not being familiar with the *Truste* privacy seal? To test this, we multiplied the privacy seal variable with the subjects' responses to the item: "*I understand the purpose of Truste's privacy seal fully*" (mean = 4.48, standard deviation = 1.53), and used the new variable in place of the privacy seal variable in the regression. The results are reported in Table 2, column 5, and they are similar to those obtained above. The coefficient of privacy seal remained positive but insignificant.

Finally, we found no significant influence of information sensitivity on disclosure. An alternative explanation of this finding was that some of the subjects may have lied to earn the monetary incentive (in which case the actual sensitivities of the items that they provided would be lower than the scores obtained in the follow-up survey). Given that we could not check for data accuracy, it was impossible for us to rule out this alternative explanation. However, we included a seven-point Likert scale item: "*Sometimes, I give false information*" (mean = 2.51, standard deviation = 1.60) in the follow-up survey to explore the effect of lying.

As suggested above, if a person had lied, the *actual sensitivity* of the information that she disclosed might be lower than her ratings submitted in the follow-up survey. Accordingly, we could calibrate her sensitivity scores by her (general) tendency to lie. A straightforward way to do this is to divide the average sensitivity score of each subject by her response to the above item (i.e., higher discounts on the provided information sensitivity were applied to subjects who were more likely to lie). We then used the transformed variable in place of the information sensitivity variable in the regression. The results are reported in Table 2, column 6. Once again, even when lying was taken into consideration, our conclusions remained similar.[12]

Predictions

The classification results obtained from the basic model are reported in Table 3. Evidently, our model was quite effective in predicting the "success" cases, but its performance in predicting the "withdraw" cases was moderate: It correctly classified only 57% of those who chose not to disclose in the main survey.

<Insert Tables 3 and 4 here>

The contribution of the experimental treatments can be inspected using the fitted logit function. Specifically, we could substitute the estimated coefficients into the logit function and compute the probabilities of disclosure (for brevity, we omit the detailed computations). Using mean values for the right-hand-side variables (or, in other words, for an "average" subject), the predicted probabilities of disclosure are reported in Table 4.

The disclosure probabilities implied by the data were somewhat high. This could have been due to the use of student subjects in the experiment, or the sampling bias due to subjects' self-selection (see footnote 10) and the non-response of a small group of people (see footnote 9 and the discussion preceding it). In spite of these limitations, the probabilities in Table 4 should provide a preliminary reference for the relative impact of our treatments.

5. Discussion

By conducting an exploratory field experiment in Singapore, we found that:

[12] It should be noted, however, that the item that we used to measure the subjects' tendency to lie was very general, and it did not specifically ask whether the subjects had lied in *this* experiment. Hence, the followed procedures represented only an exploratory attempt to assess the impact of lying in our study.

(1) The existence of a privacy statement induced more people to disclose their personal information to a website. By contrast, presenting a *Truste* privacy seal did not have any significant influence. These findings were robust regardless of whether the subjects had read and understood the purpose of the privacy statement and privacy seal.

(2) Monetary incentive had a positive influence on disclosure.

(3) The amount of information requested had a negative influence: The more information requested, the less likely the subjects were to disclose them. The sensitivity of the information, however, had no significant influence.

(4) Results (1)-(3) were robust across alternative specifications that used different measures for information sensitivity and privacy concern.

Our finding on privacy statements differs from that of Berendt et al. (2005), who found privacy statements to have no impact on consumer behavior. This could be due to differences in context: Their study was conducted in Europe, which generally has stronger legal protections of privacy (Smith 2001). Further, they conducted a laboratory experiment, and hence their subjects might have exhibited more trust in the research setting. Both of these contextual factors might have weakened the role of privacy statement in their study.

By contrast, in a field experiment where subjects had no prior trust or information about a firm, and where privacy protection was largely self-regulated, we found privacy statement useful in inducing disclosure (albeit with only marginal statistical significance). This result suggests that there is indeed a business incentive for firms to observe FIP and enhance their privacy statements. Further, the positive coefficient of the interaction variable (on the subjects' reading of the privacy statement) in Table 2, column 4 supports the view that people who read privacy statements are more likely to disclose their information to partake in online activities. It is indeed worthwhile to persuade consumers to read online privacy notices (Milne and Culnan 2004).

On the other hand, we found no significant effect of privacy seals in the experiment. This result is important, because privacy seals are often displayed by popular websites; its inception has triggered a sizeable market for Web assurance services in the USA (Jamal et al. 2003, 2005), and a series of government-supported initiatives in Singapore.[13] Evidently, privacy seals have spawned many new economic activities. Our finding thus prompts the question of why it was ineffective in encouraging consumer disclosure.

Generally, given that our subjects were familiar with *Truste*, one possible explanation for its insignificance in the experiment is that the subjects did not trust it, and hence that their behavior was not affected by its presence. To test this possibility, we included in the follow-up survey an item: "*I trust Company X in handling my information*". If the subjects trusted the privacy seal, then those who saw it should provide a *higher* score to this item.

The mean responses to this item were 5.40 (for those in the privacy statement treatment groups) and 5.17 (for those in the privacy statement + privacy seal treatment groups), but they were not statistically different. Apparently, displaying the privacy seal did not raise the trust of the subjects toward our partner firm.[14]

Collectively, results (1)-(3) support the theory that people make risk-benefit tradeoffs for privacy (Dinev and Hart 2006; Laufer and Wolfe 1977). Firms can offer monetary incentives to increase the benefit and use privacy assurance or collect less consumer information to reduce the risk of a transaction. The negative effect of information request is particularly noteworthy (e.g.,

[13] For instance, the NTC regularly features a list of Singapore merchants which are members of the *Trustsg* program. It has also appointed several existing trust mark providers (e.g., CommerceNet Singapore, Consumer Association of Singapore) as authorized code owners (ACO) of *Trustsg*.

[14] Interestingly, Edelman (2006) finds that websites that display the *Truste* seal are actually *less trustworthy* than those that do not. This might explain why it did not raise the trust of the subjects in our experiment.

see the sharp drop in disclosure probability in Table 4), because it implies that firms should minimize data collection, or else consumers may simply withdraw from online transactions.

Limitations

There are several limitations in this study. First, the study was conducted in Singapore, which generally has a collectivistic and low uncertainty avoidance culture.[15] Prior research has found that people with these cultural characteristics tend to be less concerned about privacy (Milberg et al. 1995; Milberg et al. 2000), and hence our subjects might be less wary about disclosing their personal information to others.[16] Also, the use of student subjects, although in line with many past privacy studies (e.g., Culnan 1993; Dinev and Hart 2006; Smith et al. 1996), may contribute to the high extent of disclosure that we had observed. Hence, our findings, especially the high observed disclosure rate, may not be generalizable to other consumer populations.

Second, our task of filling in a survey differed from typical online transactions that involve money-good exchanges, and we did not explicitly manipulate information relevancy or reputation in the experiment. Both of these may explain why some subjects withdrew without considering the website's offers. Also, our results may generalize only to people who choose to visit a website, which inevitably comprises a small portion of Internet users – in the experiment, only 23% of the invited people opened our partner firm's website. Our sample size was rather small, too, which might have weakened the statistical conclusions drawn in this paper.

[15] According to Hofstede's analysis (see http://www.geert-hofstede.com/hofstede_dimensions.php), Singapore had an individualism score of 20, and an uncertainty avoidance score of 8, and it was ranked among the lowest in these two dimensions in the 56 countries studied.

[16] A comparison with samples of Smith et al. (1996, Table 9) showed that our subjects indeed had lower privacy concern – the overall privacy concerns of that study's U.S. (undergraduate, MBA, and working adult) subjects ranged from 5.56 to 5.74, whereas that of our subjects was 4.31. Note that because of length consideration we used only eight items from Smith et al.'s 15-item instrument, but we selected two items from each of the four dimensions in their instrument. Hence, all four dimensions of privacy concern were measured in our study. As in Smith et al., we computed the overall privacy concern score by averaging the subjects' responses to the eight items.

In terms of methodology, because of the need to capture subjects' background and their ratings of information sensitivity, we had to exclude some subjects who did not do the follow-up survey, and this could have introduced a sampling bias. Also, due to length considerations, some of the variables (e.g., trust propensity, the subjects' understanding of the privacy statement/seal) were measured by only one or two items, and hence we were not able to ensure their reliabilities. Our consideration of lying was exploratory and limited too (see footnote 12): Only one item was used to measure the subjects' general inclination to lie. Clearly, classifying "lying" and "honest" consumers poses an important challenge for future privacy research.

Managerial Implications

Notwithstanding the above limitations, our findings exhibit a few practical implications for both privacy seal issuers and online firms. Issuers need to raise consumer trust in their seals. In particular, the value added by privacy seal is limited if issuers remain passive; in some jurisdictions (e.g., the USA), not complying with the clauses stated in a privacy statement is illegal. Hence, if privacy seal issuers do not actively monitor their clients, but wait for consumers to report infringements, their seals add little value over a privacy statement. Perhaps more reviews and audits (like what AICPA does for *WebTrust*) are desirable (Jamal et al. 2003).

For online firms, the implication is straightforward – adopt fair information practices, and communicate commitment to consumers. The benefit of privacy statement and privacy seal can materialize only if firms play their part by adhering to the stated policies and publicizing it. By doing so, they would eventually gain by having higher browser-to-customer conversion rates. Also, firms should collect less consumer information as and when possible. If they do not need or intend to use some data, then they should not request for such data. Monetary incentives could be used to boost disclosure, too, but doing so is obviously costly.

Our results regarding the control variables also carry useful implications. Some consumer traits, such as trust propensity and prior Internet shopping experiences, could help identify potential new customers. Hence, firms may want to spend more resources to harvest regular Internet browsers or shoppers. The recency effect (Tubbs et al. 1990) may also matter: Consumers who recently experienced information misuse may have a bad impression about online transactions. Firms should stay clean and avoid being associated with online malpractices.

Further Research

This study has revealed some patterns of consumer behavior that deserve attention in future research. First, our model did not predict the "withdraw" cases well; there were 20 subjects who, despite visiting our website, consistently refused to provide any information or opinions. Other than privacy concerns, could there be contextual or individual factors that caused them to remain silent? Second, some subjects exited partway through answering the follow-up survey, which means that they were willing to disclose information but then declined to finish for other reasons. Was it the length of the survey that caused this problem? Would splitting a long survey or registration form into multiple pages help? Finally, since privacy is tradable in a real online environment, economic solutions (see, e.g., Laudon 1996) may help resolve the Internet privacy problem. How they should be implemented is an immediate challenge for future work.

6. Concluding Remarks

This study contributes to the privacy literature by empirically assessing the value of commonly used privacy assurances, and showing how consumer disclosure can be raised by devising better offers. Given the exploratory nature of our experiment and the evolving technologies and new online practices (Milne 2000), it is obvious that more research on Internet privacy is needed.

The strength of our study is the use of a field experiment, which observed what people *actually do* instead of what they think they *should do*. Because of this methodological choice, we found some departures in results from past studies (e.g., displaying a privacy statement was helpful for online firms). We believe context-rich research along the direction of this study would give a more complete picture of consumers' online behavior, particularly with respect to information disclosure. We urge the academic and the business communities to undertake such research in the future.

References

Acquisti, A. "Privacy in Electronic Commerce and the Economics of Immediate Gratification," *Proceedings of the ACM Electronic Commerce Conference (EC 04)*, New York, ACM Press, 2004, pp. 21-29.

Alba, J.W., and Hutchinson, J.W. "Dimensions of Consumer Expertise," *Journal of Consumer Research* (13:4), March 1987, pp. 411-454.

Ben-Akiva, M., and Lerman, S.R. *Discrete Choice Analysis: Theory and Application to Travel Demand*. Cambridge, MA: MIT Press, 1985.

Berendt, B., Gunther, O., and Spiekermann, S. "Privacy in E-Commerce: Stated Preferences vs. Actual Behavior," *Communications of the ACM* (48:4), April 2005, pp. 101-106.

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, pp. 341-363.

Culnan, M.J., and Armstrong, K.P. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), January-February 1999, pp. 104-115.

Culnan, M.J., and Bies, J.R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), 2003, pp.323-342.

Culnan, M.J., and Milberg, S.J. *The Second Exchange: Managing Customer Information in Marketing Relationships*. Unpublished manuscript, Georgetown University, Washington DC. 1998.

Dinev, T. and Hart, P. “An Extended Privacy Calculus Model for E-Commerce Transactions,” *Information Systems Research* (17:1), March 2006, pp. 61-80.

Edelman, B. “Adverse Selection in Online Trust Certifications,” *Working Paper*, Harvard University, May 2006. Available at http://weis2006.econinfosec.org/docs/10.pdf. [Accessed July 21, 2006].

Emerson, R.M. “Exchange Theory Part I: A Psychological Basis for Social Exchange,” and “Exchange Theory Part II: Exchange Relations and Network Structures,” in *Social Theories in Progress*, Joseph Berger, Morris Zelditch, Jr., Bo Anderson (eds.), Houghton Mifflin Company, 1972, pp. 38-87.

Federal Trade Commission. *Privacy Online: Fair Information Practices in the Electronic Marketplace: a Report to Congress*. May 2000. Available at http://www.ftc.gov/reports/privacy2000/privacy2000.pdf. [Accessed December 7, 2005].

Goodwin, C. “Privacy: Recognition of a Consumer Right,” *Journal of Public Policy and Marketing* (10:1), Spring 1991, pp. 149-166.

Goodwin, C. “A Conceptualization of Motives to Seek Privacy for Nondeviant Consumption,” *Journal of Consumer Psychology* (1:3), 1992, pp. 261-284.

Hann, I.H., Hui, K.L., Lee, T.S.Y., and Png, I.P.L. “Online Information Privacy: Measuring the Cost-Benefit Tradeoff,” *Proceedings of the Twenty-Third International Conference on Information Systems*, Barcelona, Spain, 2002, pp. 1-10.

Harper, J., and Singleton, S. *With a Grain of Salt: What Consumer Privacy Surveys Don’t Tell us*. Competitive Enterprise Institute, June 2001.

Hine, C., and Eve, J. “Privacy in the Marketplace,” *Information Society* (14), 1998, pp. 253-262.

Hoffman, D.L., Novak, P.T., and Peralta, A.M. “Building Consumer Trust Online,” *Communications of the ACM* (42:4), April 1999, pp. 80-85.

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

Hosmer, D.W., and Lemeshow, S. *Applied Logistic Regression*. New York: Wiley, 1989.

Jamal, K., Maier, M., and Sunder, S. “Privacy in E-Commerce: Development of Reporting Standards, Disclosure, and Assurance Services in an Unregulated Marketing,” *Journal of Accounting Research* (41:2), May 2003, pp. 285-315.

Jamal, K., Maier, M., and Sunder, S. “Enforced Standards versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the United States and the United Kingdom,” *Journal of Accounting Research* (43:1), March 2005, pp. 73-96.

Laudon, K.C. “Markets and privacy,” *Communications of the ACM* (39:9), 1996, pp. 92-104.

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, pp. 22-42.

Luce, R.D. *Individual Choice Behavior: A Theoretical Analysis*. New York: Wiley, 1959.

McFadden, D.L. “The Choice Theory Approach to Market Research,” *Marketing Science* (5:4), Fall 1986, pp. 275-297.

McFadden, D.L. “Economic Choices,” *American Economic Review* (91:3), June 2001, pp. 351-378.

Milberg, S.J., Smith, H.J. and Burke, S.J. “Information Privacy: Corporate Management and National Regulation,” *Organization Science*, (11:1), 2000, pp. 35-57.

Milberg, S.J., Burke, S.J. and Smith, H.J. “Values, Personal Information Privacy, and Regulatory Approaches,” *Communications of the ACM*, (38:12), 1995, pp. 65-74.

Milne, G.R., “Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue,” *Journal of Public Policy and Marketing* (19:1), 2000, pp. 1-6.

Milne, G.R., and Culnan, M.J. “Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices,” *Journal of Interactive Marketing* (18:3), Summer 2004, pp. 15-29.

Milne, G.R., and Gordon, E.M. “Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract,” *Journal of Public Policy and Marketing* (12:2), Fall 1993, pp. 206-215.

National Trust Council. *Model Data Protection Code*. Available at http://www.trustsg.com.sg/downloads/Data_Protection_Code_v1.3.pdf [Accessed December 7, 2005].

Nowak, G.J., and Phelps, J. “Direct Marketing and the Use of Individual-Level Consumer Information: Determining how and When ‘Privacy’ Matters,” *Journal of Direct Marketing* (11:4), Fall 1997, pp. 94-109.

Phelps, J., Nowak, G.J., and Ferrell, E. “Privacy Concerns and Consumer Willingness to Provide Personal Information,” *Journal of Public Policy and Marketing* (19:1), spring 2000, pp. 27-41.

Pitkow, J.E., and Kehoe, M.C. “Emerging Trends in the WWW User Populations,” *Communications of the ACM* (39:6), June 1996, pp. 106-108.

Ratchford, B.T. “The Economics of Consumer Knowledge,” *Journal of Consumer Research* (27:4), March 2001, pp. 397-411.

Smith, H.J. “Information Privacy and Marketing: What the U.S. Should (and Shouldn’t) Learn from Europe,” *California Management Review* (43:2), Winter 2001, pp. 8-33.

Smith, H.J., Milberg, J.S., and Burke, J.S. “Information Privacy: Measuring Individuals’ Concerns about Organizational Practices,” *MIS Quarterly* (20:2), June 1996, pp. 167-196.

Stone, E.F., and Stone, L.D. “Privacy in Organizations: Theoretical issues, Research findings, and Protection mechanisms,” *Research in Personnel and Human Resources Management* (8), 1990, pp. 349-411.

Tubbs, R.M., Messier, W.F., and Knechel, W.R. “Recency Effects in the Auditor’s Belief-Revision Process,” *The Accounting Review* (65:2), April 1990, pp. 452-460.

Westin, A. *Opinion Surveys: What Consumers have to Say about Information Privacy*. Hearing before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, U.S. House of Representative. May 8, 2001. Available at http://energycommerce.house.gov/107/action/107-35.pdf [Accessed January 7, 2006].

Appendix A

Requested Information[++]	Average sensitivity[+]	Number of subjects[+]
1. Name	3.83	109
2. Email address	3.87	109
3. Address	5.02	109
4. Citizenship	2.74	109
5. Gender	2.31	103
6. Marital status	2.51	99
7. Ethnicity	2.46	93
8. Country of residence	2.55	87
9. Phone number	5.79	84
10. Occupation	3.04	77
11. Household size	3.60	70
12. Monthly household income	5.25	64
13. Identity card / passport number	5.81	62
14. Banks / financial companies that you have accounts	5.27	55
15. Bank account balance	6.53	49
16. Personal monthly expenditure	4.90	42
17. Types of credit cards owned	4.50	38
18. Types of personal debt	5.37	30
19. Amount of personal debt	5.92	24
20. Highest education achieved	2.79	19
21. Name of educational institution corresponding to (20)	3.19	16
22. Average grade point average	4.20	10
23. Number of courses failed in the past	3.75	4

[+] The sensitivity scores were obtained by asking subjects to rate (on a seven-point scale – not sensitive to extremely sensitive), in the follow-up survey, the sensitivity of each of the information items that they were asked to provide in the main survey. We then averaged the scores across subjects to obtain the scores in the second column. Note that since we varied how much information was requested, not all subjects rated every item. The number of subjects who were asked to provide each item is shown in the last column.

[++] Items 1-3 and 9 can be roughly classified as personal identifier information, 4-8 and 10-11 can be classified as demographics information, 12-19 can be classified as financial information, and, finally, 20-23 can be classified as education information. The mean sensitivities of these four categories were, respectively, 4.63, 2.74, 5.44, and 3.48 (out of 7). Perhaps unsurprisingly (see, e.g., Phelps et al. 2000), t-tests showed that personal identifiers and financial information were significantly more sensitive than the other two categories; demographics information was significantly less sensitive than the other three categories.

Appendix B

Control variables

Trust propensity	• I feel that people are generally trustworthy. • I feel that people are generally reliable.
Information misuse experience	• How many times of personal information misuse have you encountered in the past?
Internet shopping experience	• In the past year, how many times have you shopped via the Internet?
Privacy concerns	(a) Cookie setting – we asked subjects to select their cookie policy from the following list (subjects who chose one of the last three options were considered more concerned about privacy): o My preferences are set to always accept cookies. o I don't know what a cookie is. o I don't know what my cookie preferences are set to. o My browser doesn't support cookies. o My preferences are set to only accept cookies from the same site I am browsing. o My preferences are set to warn me before accepting cookies. o My preferences are set to ignore/never accept cookies. (b) Measures of Smith et al. (1996) – the eight items were: o I'm concerned that companies are collecting too much personal information about me. o Companies should have better procedures to correct errors in personal information. o Companies should never sell the personal information in their computer databases to other companies. o Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers. o Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information. o When companies ask me for my personal information, I sometimes think twice before providing it. o Computer databases that contain personal information should be protected from unauthorized access – no matter how much it costs. o Companies should devote more time and effort to verifying the accuracy of the personal information in their databases. The responses to these eight questions were averaged to produce a privacy concern score for each subject.

Note: for information misuse and Internet shopping experiences, because the subjects' responses were noisy (some subjects entered rounded or wide ranges of numbers), we coded their responses as binary variables – having or not having the experiences. All Likert scale items in this study (including the manipulation checks and the measures in the following two tables) had the anchors 1 = totally disagree and 7 = totally agree.

Manipulation Checks

Privacy assurances	• Company X has a privacy statement. • Company X has a Truste privacy seal. For those who were presented a privacy statement: • I have read through Company X’s privacy statement and understood it fully (mean = 4.62, standard deviation = 1.47). For those who were also presented a privacy seal: • I understand the purpose of Truste’s privacy seal fully (mean = 4.48, standard deviation = 1.53).
Monetary incentive	• The amount of money I received is adequate to compensate my effort and time spent in participating in the mobile device survey. • The reward I received from participating in the mobile device survey is worth the information I gave. (mean = 4.66, standard deviation = 1.45)
Information request	• I feel that the mobile device survey is collecting too much personal information about me. • I am giving out a lot of information. (mean = 4.54, standard deviation = 1.46)

Other Measures

Familiarity with privacy seals	• I am familiar with foreign privacy seals such as Truste, WebTrust and BBBOnline (mean = 6.58; standard deviation = 0.87). • I am familiar with local privacy seals such as Trustsg and CaseTrust (mean = 2.62, standard deviation = 1.77)
Tendency to lie	• Sometimes, I give false information (mean = 2.51, standard deviation = 1.60)
Trust in information handling practice	• I trust Company X in handling my information (mean = 5.46, standard deviation = 1.34).

Table 1. Descriptive Statistics

Subjects’ background	
Trust propensity	mean = 3.09; std. dev. = 0.98
Internet shopping experience	yes = 41; no = 68
Information misuse experience	yes = 47; no = 62
Cookie preference setting	changed = 48; not changed = 61
Privacy concern scores	mean = 4.31; std. dev. = 0.68
Experimental treatment	
No assurance	38
Assurance by only a privacy statement	42
Assurance by both a privacy statement and privacy seal	29
Monetary incentive	mean = 4.76; std. dev. = 2.46
Number of information items requested	mean = 13.41; std. dev. = 5.66
Average sensitivity of solicited information (measured in the follow-up survey)	mean = 3.86; std. dev. = 1.01

Table 2. Logit Estimation Results^{+}

	Baseline model (1)	Highest sensitivity (2)	Measure of Smith et al. (3)	Read privacy statement (4)	Understood privacy seal (5)	Lying and sensitivity (6)
Constant	-1.13 (2.06)	-0.39 (3.93)	-3.59 (3.00)	-0.83 (2.04)	-1.39 (2.01)	-1.91 (1.79)
Privacy statement	1.22* (0.70)	1.11^{++} (0.69)	1.10^{++} (0.70)	0.21^{++} (0.13)	1.07^{++} (0.11)	1.16* (0.68)
Privacy seal	0.97 (1.15)	1.11 (1.14)	1.08 (1.14)	1.15 (1.13)	0.44 (0.35)	1.18 (1.13)
Monetary incentive	0.39*** (0.14)	0.38*** (0.14)	0.39*** (0.14)	0.35** (0.14)	0.39*** (0.14)	0.37*** (0.14)
Number of items requested	-0.14** (0.07)	-0.13* (0.07)	-0.13** (0.07)	-0.13** (0.06)	-0.13** (0.07)	-0.14** (0.07)
Information sensitivity	-0.26 (0.33)	-0.27 (0.56)	-0.24 (0.32)	-0.26 (0.33)	-0.22 (0.32)	-0.07 (0.22)
Trust propensity	1.10*** (0.37)	1.09*** (0.37)	0.87** (0.39)	1.02*** (0.36)	1.09*** (0.37)	1.09*** (0.37)
Information misuse experience	-1.14* (0.66)	-1.19* (0.65)	-1.05^{++} (0.65)	-1.07* (0.65)	-1.23* (0.66)	-1.21* (0.67)
Internet shopping experience	1.77** (0.76)	1.75** (0.76)	1.41** (0.71)	1.73** (0.75)	1.71** (0.76)	1.75** (0.76)
Privacy concern	-0.51 (0.66)	-0.49 (0.66)	-0.68 (0.59)	-0.44 (0.66)	-0.46 (0.67)	-0.55 (0.68)
Sample size	109	109	109	109	109	109
Log likelihood	-37.07	-37.26	-36.70	-37.29	-36.19	-37.34
McFadden R-square	0.34	0.34	0.35	0.34	0.36	0.34

*** p < 0.01; ** p < 0.05; * p < 0.10.

$^{+}$ Standard errors are presented in parentheses.

$^{++}$ p-values very close to marginally significant, with values in the range of 0.10 to 0.11.

Table 3. Classification Table

	Predicted frequency		
Observed frequency	Withdraw	Disclose	Percentage correct
Withdraw	13	10	56.52
Disclose	3	83	96.51
Overall percentage			88.07

Table 4. Predicted Disclosure Probabilities

Scenario	Probability
No treatment (baseline)	90.33%
Add a privacy statement	96.94%
Add a privacy statement and privacy seal	98.81%
Add $5	98.48%
Request for mean number of items (as reported in Table 1), with mean information sensitivity	34.50%
Add all treatments together	97.03%