12-31-2007

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study

Lorrie Cranor  
*Carnegie Mellon University*

Serge Egelman  
*Carnegie Mellon University*

Janice Tsai  
*Carnegie Mellon University*

Alessandro Acquisti  
*Carnegie Mellon University*

Follow this and additional works at: [http://aisel.aisnet.org/icis2007](http://aisel.aisnet.org/icis2007)

Recommended Citation


[http://aisel.aisnet.org/icis2007/20](http://aisel.aisnet.org/icis2007/20)

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2007 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
THE EFFECT OF ONLINE PRIVACY INFORMATION ON PURCHASING BEHAVIOR: AN EXPERIMENTAL STUDY

Janice Y. Tsai  
Carnegie Mellon University  
5000 Forbes Ave.  
Pittsburgh, PA 15213  
jytsai@andrew.cmu.edu

Serge Egelman  
Carnegie Mellon University  
5000 Forbes Ave.  
Pittsburgh, PA 15213  
egelman@cs.cmu.edu

Lorrie Cranor  
Carnegie Mellon University  
5000 Forbes Ave.  
Pittsburgh, PA 15213  
lorrie@cs.cmu.edu

Alessandro Acquisti  
Carnegie Mellon University  
5000 Forbes Ave.  
Pittsburgh, PA 15213  
acquisti@andrew.cmu.edu

Abstract

Companies’ efforts to manage their information practices to produce transparent privacy policies have yielded mixed results. Web retailers detail such practices in their online privacy policies, but most of the time this information remains invisible to consumers. This paper reports on research undertaken to determine whether a more prominent display of privacy information will cause consumers to incorporate privacy considerations into their online purchasing decisions. We designed an experiment in which a shopping search engine interface, Privacy Finder, clearly displays privacy policy information. When such information is made available, consumers tend to purchase from online retailers who better protect their privacy. Importantly, our study indicates that once privacy information is made more salient, some consumers are willing to pay a premium to purchase from more privacy protective websites. This suggests that companies may be able to leverage privacy protection as a selling point.

Keywords: Privacy, Information Systems, Economics, Experimental Economics, E-Commerce
Introduction

Most Americans believe that their right to privacy is “under serious threat,” (CBS News, 2005) and express concern about companies collecting their personal data (CBS News, 2005; Harris Interactive, 2001; P&AB, 2005; Turow, et al., 2005). One method industry uses to address privacy concerns is to post privacy policies to convey their information practices. However, 70% of people in a recent study disagreed with the statement “privacy policies are easy to understand,” (Turow, et al., 2005) and few people make the effort to read them (Privacy Leadership Initiative, 2001; TRUSTe, 2006). Other studies indicate that people are often willing to provide personal information for small or no rewards (Acquisti and Grossklags, 2005).

This paper reports on research that examines whether the prominent display of privacy information will cause consumers to incorporate this information into their online purchasing decisions. In turn, answering this question can cast a light on whether companies can use privacy in a strategic way and leverage its protection for competitive advantage. Our study focuses on the role of information technology in privacy communications. We investigate what happens when tools become available that prominently display an organization’s privacy policies.

Contrary to the common view that consumers are unlikely to pay for privacy, formed due to the failure of online anonymity services (Brunk, 2002) and research described in the following Section, we found that consumers in our study were willing to pay a premium for privacy when privacy information was made more salient. However, consumers who were not presented with prominent privacy information were likely to make purchases from the vendor with the lowest price.

Background

Surveys consistently indicate that people have concerns about their personal information and how companies will use that information: so much so that these concerns continue to hinder consumers from making online purchases. A 2005 survey conducted by Privacy & American Business (P&AB) found that concerns about the use of personal information led 64% of respondents to decide not to purchase something from a company, while 67% of respondents decided not to register at a website or shop online because they found the privacy policy to be too complicated or unclear (P&AB, 2005).

On the other hand, consumers have also been found to be willing to provide personal information for small discounts or rewards. Tedeschi (2002) reported on a 2002 Jupiter Research study that found 82% of online shoppers willing to give personal data to new shopping sites in exchange for the chance to win $100. In an experimental investigation, Spiekermann et al (2001) found evidence that even privacy concerned individuals are willing to trade-off privacy for convenience and discounts. This dichotomy between professed attitudes and actual behavior has prompted a number of experiments aimed at gaining an understanding of what really drives users’ valuations of privacy. Huberman, et al. (2005) used a second-price auction experimental setup to study the monetary value of private information to individuals. Information considered more “sensitive” or “undesirable” had a greater impact on what price was demanded to reveal that information. When asked to provide an estimate (in a contingent valuation survey) of how much consumers would value having enforceable property rights to their personal information, Rose (2005) found that while participants expressed high sensitivity to privacy, only about 47% would be willing to pay for those property rights (an average of NZD 55.40 or USD 28.25). Hui, et al. (2006) used a field experiment in Singapore to study the values of various privacy assurance measures. They found that privacy statements and monetary incentives could both induce more information disclosures.

Several possible explanations for this apparent dichotomy have been discussed in the literature (Acquisti, 2004; Acquisti and Grossklags, 2003; Shostack, 2003; Syverson, 2003; Wathieu and Friedman, 2005): from incomplete information about privacy threats and defenses, to bounded ability to deal with their complex trade-offs; from low (and decreasing) privacy sensitivities to behavioral motivations such as immediate gratification. It is likely that not one single factor can, alone, explain the dichotomy. The studies we present in this paper focus on the relationship between availability of privacy information and ecommerce decisions. Our survey and experiment focus on the effects of signals in privacy decision-making, and therefore cast a light on the relationship between incomplete/asymmetric information and privacy valuations (Acquisti, 2004).

Information asymmetry plays a double role in privacy decision-making. To use an example from the context of electronic markets purchases, before a consumer completes his first purchase at an online merchant, the merchant has none or limited information about the consumer’s taste, reservation price, identity, and so forth (see Acquisti and
Varian 2005; Taylor 2004). However, after a transaction is completed, the consumer has incomplete information on how the merchant will use the personal information directly or indirectly revealed through the transaction (Acquisti and Grossklags 2005). This particular form of asymmetric information may, in theory, decrease the willingness of consumers’ to transact with merchants whose privacy policies are not known. While that may sometimes be true, the literature above indicates that consumers rarely pay attention to merchants’ online privacy policies, and are easily convinced to provide personal information online. One hypothesis underlying this behavior is that the prospected cognitive costs of reducing the information asymmetry about how a merchant handles consumers’ information are too large. Another explanation is that consumers are not immediately aware of, or do not focus upon, possible privacy concerns when transacting online. Subsequently, the weight of privacy concerns in the consumer’s utility function is significantly less than factors such as price. Providing clearer information about a merchant’s privacy policy may reduce this information asymmetry. Thus, privacy considerations may now play a more significant role in the consumer’s utility function and decision-making process.

Privacy policies are such an attempt to reduce information asymmetry and have become prevalent (Milne and Culnan, 2002). However, privacy information remains invisible to Internet users. People rarely read privacy policies (Jensen, et al., 2005; Privacy Leadership Initiative, 2001), and the policies themselves are difficult to understand (Hochhauser, 2003; Jensen and Potts, 2004). Vila, et al. (2004) modeled the dynamics of privacy policies and the people who read them as a “lemons market,” in which it is expensive for consumers to gain information about a company’s data practices by looking at its privacy policy, and consumers are unaware of the costs of privacy violations. People also make mistaken assumptions about these policies: one study found that a majority of Americans who report having seen privacy policies on popular websites believe the presence of a link to a privacy policy means that their data is protected (Turow, et al., 2005). While individuals may be aware that a company or organization has a privacy policy, they still lack enough information to make informed decisions.

The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences (P3P) to make privacy policies more usable and to reduce information asymmetry. P3P is a standard machine-readable format for privacy policies. Companies can adopt that standard to post online privacy policies readable by P3P-enabled web browsers and P3P “user agents” (Cranor, 2002). P3P user agents can also translate computer-readable privacy policies into natural language and display them in their entirety or in simplified formats (Cranor, et al., 2006). In addition, a P3P-enabled search engine named Privacy Finder (http://privacyfinder.org) annotates search results with privacy information derived from P3P policies and generates “privacy reports” for P3P-enabled websites. The privacy information and reports are intended to provide a risk communication to consumers, allowing them to make “informed, independent judgments” (Morgan, et al., 2002) about the websites they visit. By providing this privacy information in an Internet search engine interface while people are actively seeking web pages, Privacy Finder further reduces the privacy information asymmetry that makes it so difficult for people to act consistently with their privacy preferences. In turn, by adapting their information systems to produce machine-readable privacy policies, corporations can ensure that their policies will become more accessible to visitors and consumers.

Privacy Finder submits search queries to Google and Yahoo!, obtains the results, and checks for P3P policies. It then displays the results annotated with privacy indicators or “privacy icons” that graphically represent how well a website’s P3P policy matches the privacy preferences specified by the user. The icons represent a five-point privacy “meter” (see Table 1). The meter is composed of a set of four boxes that are shown as green (filled) or white (empty) based on an algorithm that accounts for the number of privacy preference mismatches. Thus, a site that violates most of the user’s preferences will have zero or one box filled, while a site with only a few mismatches might have two or three filled boxes. Sites without P3P policies are not annotated with a privacy icon.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Filled Boxes]</td>
<td>Matches privacy preferences</td>
</tr>
<tr>
<td>![Filled and Empty Boxes]</td>
<td>Does not match privacy preferences</td>
</tr>
</tbody>
</table>

Table 1: Privacy Finder’s privacy indicators
Privacy Finder provides a link to the privacy report for each P3P-enabled website. The privacy report includes a “Privacy Policy Check” section that highlights the specific areas where the policy does not match the user’s privacy preferences. The privacy report has been designed to present the privacy information that is “of greatest concern to users” in a simplified format (Cranor, et al., 2006). One version of Privacy Finder, designed for online shopping, submits search queries via the Google and Yahoo! shopping interfaces and returns search results annotated with product photographs and price information, in addition to the privacy information described above.

In a previous study that employed an earlier version of Privacy Finder, we found preliminary evidence that when privacy policy information is made available in search engines; online shoppers seek out more privacy-friendly websites (Gideon, et al., 2006). However, in that study participants were reimbursed for their purchases, and thus had no direct incentive to consider price in their purchasing decisions. In this paper we describe an experiment designed to determine whether online shoppers will actually pay a premium to make their purchases from the more privacy-friendly merchants, once privacy policy information is made more accessible to them.

Objectives and Hypotheses

The goal of this study is to determine whether the prominent display of privacy information in search engine results causes privacy-concerned users to take privacy into account when making online purchasing decisions, and whether privacy-concerned users are willing to pay a premium to make their purchases from the more privacy-friendly merchants.

Our study, rather than looking at all of the possible factors that affect privacy behavior, focuses on the relationship between the availability of privacy information and ecommerce decisions. We used Privacy Finder as the interface for our experiment, asking each participant to purchase two items (a privacy-sensitive item and a non-privacy-sensitive item) from existing (rather than simulated) merchants and using their own names and credit card information. Participants were assigned to one of three treatment conditions: a privacy information condition, in which the Privacy Finder results were annotated with icons representing the actual privacy rating of the various merchants; and two control conditions: a baseline condition in which search results were not annotated with icons or privacy information; and an “irrelevant information” condition in which search results were annotated with icons representing intentionally irrelevant information.

The experiment, described in detail in the following section, was so structured to test the following hypotheses:

**Hypothesis 1:** Participants in the privacy information condition will be more likely than those in the irrelevant information or no information conditions to purchase from websites annotated with icons.

**Hypothesis 2:** Participants in the privacy information condition will be more likely than those in the irrelevant information or no information conditions to purchase from websites annotated with the four-green-boxes icon.

Hypotheses 1 and 2 follow from the theoretical background presented in the previous section. Under uncertainty or ignorance of the merchant’s privacy practices and potential privacy issues, privacy concerns play a limited role in purchasing decision-making (Acquisti 2004). The provision of accessible privacy information gives more weight to privacy considerations in the consumer’s utility function, which should be reflected in the heightened propensity of consumers under the privacy information condition to purchase from merchants with better privacy policies.

**Hypothesis 3a:** Participants presented with prominent privacy information (those in the privacy information condition) will be more likely than those in the other conditions to pay a premium to purchase from sites that have better privacy policies.

Once more information about privacy is provided and privacy considerations take a more significant role in the consumer’s utility function, one would expect that certain consumers may be willing to trade money for privacy, depending on the relative strength of their privacy and price sensitivities (see also Acquisti and Varian 2005 and Taylor 2004 for a privacy model with price discrimination).

**Hypothesis 3b:** In the absence of prominent privacy information, people will purchase where price is lowest.

This hypothesis follows directly from microeconomic theory and is used purely as a control for Hypothesis 3a.

**Hypothesis 4:** Icons or symbols will affect purchase decisions, regardless of meaning.
This hypothesis is inspired by the literature on “institutional based trust” that studies structures and situations that affect trust-based individuals decision-making (McKnight and Chervany, 2002). For instance, trust seals can be a proxy for merchant quality in consumer decision-making (Riegelsberger et al, 2005). Hence, in the “irrelevant information” condition, the green icons visible through the interface may be interpreted as proxies of merchant quality regardless of their actual meaning (see also Jensen, et al., 2005). We wish to differentiate between the actual impact of privacy information and the impact of institutional-based trust.

**Hypothesis 5a:** The effect of the privacy information will be greater when participants purchase privacy-sensitive items than when they purchase non-privacy-sensitive items.

The purchase of privacy-sensitive items should raise more significant privacy concerns. Once privacy information is made available, the concerns should correspondingly affect purchasing behavior.

**Hypothesis 5b:** When no privacy information is provided, privacy-sensitive and non-privacy-sensitive purchase decisions will be treated similarly.

This hypothesis is used as a control for Hypothesis 5a. In the absence of privacy information, privacy concerns will not play a significant role in purchase decision-making regardless of the relative degree of concern.

**The Study**

Our study consisted of an online concerns survey followed by an online shopping experiment in a laboratory setup.

**Online Concerns Survey**

We developed a survey with a few high-level questions in mind. Because our experiment relied on the purchase of a privacy-sensitive item, we wanted to determine the types of products that may or may not elicit privacy responses in a purchasing scenario. We were also interested in examining what types of privacy concerns individuals have when they use the Internet to shop online and the risk individuals associate with each of these concerns to confirm that the information provided in the Privacy Finder interface addresses the data practices that individuals are most concerned about and view as likely to occur.

Due to page constraints, we only briefly summarize the methodology and results of our online concerns survey. The survey was administered through SurveyMonkey, an online survey creation and administration tool.\(^1\) Notices about the survey were posted on the Volunteers section of Craigslist. The final sample included 276 individuals. We asked participants to evaluate the likelihood of certain online scenarios and provide a rating on an 11-point Likert scale of how much “trouble” it would cause them if the scenario were to occur. The situations included scenarios such as “If your credit card number were stolen after you made an online purchase?” or “If you received unwanted emails after you made a purchase?”

Respondents seemed to be the least concerned with the scenarios that they rated the most likely. These included “receiving unwanted email,” having “online stores track the items they click on,” and having “online stores infer information” about them. We found that the concerns addressed by Privacy Finder were the ones rated with the highest likelihood. These items are *Continued Contact*, *Dossier*, *Information Sold*, *Unwanted Email*, *Infer Information*, and *Track Items*. This indicates that Privacy Finder is an appropriate tool for our experiment.

We also used the survey results to help identify products for participants to purchase in our online shopping experiment. We posed the following question:

> We will be conducting studies for an online shopping and privacy research project in which we will pay participants to make online purchases with their own credit cards. Each participant will receive enough money to cover the cost of the purchase plus $10. If you were asked to participate, would you be willing to purchase the items below with your own credit card, and how concerned would you be about doing so?

We gave the following response options: “*Would not purchase,*” “*Purchase, Very Concerned,*” “*Purchase, Somewhat Concerned,*” and “*Purchase, No concerns.*” We coded these on a 4-point scale to compute an average

---

purchase likelihood score for each product. The list of items ranged from textbooks or flowers to HIV tests, pornographic material, and books on bomb-making. Most participants showed little resistance to purchasing common products, such as office supplies. We detected increasing hesitance for items of a more personal nature, such as items related to sex and books related to depression. When the items were suggestive of violent behavior, such as bullets or a book on bomb-making, we found significant reservations and reluctance to purchasing the items.

**Online Shopping Experiment**

We conducted the online shopping experiment in the Carnegie Mellon Usable Privacy and Security (CUPS) laboratory in Pittsburgh, PA. In this section we describe our experimental design, participant recruitment, screening survey, experimental protocol, and exit survey.

**Experimental Design**

We compared participant actions in the following between-subjects design to gauge the impact of providing privacy information. Each participant was presented with a Search Engine Key (similar to the one in Figure 1). Unknown to the participants, their search results for the purchasing tasks had been pre-coded and made identical across conditions. The only difference across conditions consisted of the annotated icons that accompanied the results:

- **Condition 1**, No information: This control group viewed search results without any annotations. Participants were given a Search Engine Key that highlighted the type of data that the search engine made visible: merchant names and URLs, product prices, products photos, and so on. During the experiment, their search results did not include any Privacy Finder icons.

- **Condition 2**, Irrelevant information: The results in this control group were annotated with icons representing irrelevant information. Participants were given a Search Engine Key that highlighted the presence of green box icons indicating a "rating calculated based on our analysis of the site's computer readable accessibility information for vision-impaired users." During the experiment, the search results visible to participants in this condition included such icons.

- **Condition 3**, Privacy information: Privacy icons and links to privacy reports were presented to this experimental group. Participants in this condition were given a Search Engine Key that highlighted the presence of green box icons indicating a "rating calculated based on our analysis of the site's computer readable privacy policy." During the experiment, the search results visible to participants in this condition included such icons.

We selected an irrelevant information condition to determine if the presence of an icon itself would influence purchase decisions. In previous studies, other content-free symbols (including credit card logos) have increased the willingness to trust certain sites (Jensen, et al., 2005).

To determine the sample size for the study, we performed a power analysis for two proportions, evaluating whether 50% of the participants in the privacy condition would purchase from “high privacy” sites as compared to 10% in the other conditions ($\alpha = 0.05$, $\beta = 0.2$). To yield a power of 80%, 16 participants were required for each condition, for a total of 48 participants. In each condition, the participants were divided equally by gender.
Participant Recruitment

Participants were recruited from the general Pittsburgh population. Flyers for an “Online searching and shopping study” were posted around town and online in the Volunteers section of Craigslist. The study was also posted on the experiments scheduling site for the Center of Behavioral and Decision Research at Carnegie Mellon. Participants were required to be at least 18 years old, have a personal credit card for use during the study, and have experience shopping online. The flyer also advertised that participants would be paid to shop online using our money and would get to “Keep the change.”

Screening Survey

Interested participants were directed to a preliminary survey online. We received 272 complete responses. Our study was designed specifically to target privacy concerned individuals rather than the population at large. We assumed that our interface and risk communication tool would be helpful to people who have some online privacy concerns. Therefore we calculated a “risk score” for each participant and used it to screen out those who perceived little or no privacy risk when shopping online. Based on this requirement, we screened out 12.5% of the total respondents. Participants who met our requirements were contacted via email several weeks later to schedule a laboratory session. Because of the delay between the survey and the laboratory sessions, we believe there is little chance that the screening questions primed participants to think about privacy during the laboratory sessions.

We also used the screening survey to ask participants to rate the importance of various factors that might go into a participant’s decision to make a purchase from a particular website. These factors and their mean ratings are detailed in Table 2. Participants primarily make purchasing decisions based on price, and then return policy. Shipping speed, customer service, privacy policy, website design, and customer reviews were rated as equally important.

We used the purchasing factors ratings to determine what factors have minimal impact on purchase decisions. We selected the label of “Handicap Accessibility” for our irrelevant information condition because participants reported that “Accessibility for sight-impaired users” had almost no impact on their purchase decisions.
### Table 2: Paired t-test comparison of purchasing factors to “Privacy Policy,” with 70 degrees of freedom and a maximum value of 6.0. Scores are based on a 7-point Likert scale from No Consideration to A Great Deal of Consideration.

<table>
<thead>
<tr>
<th>Factors</th>
<th>Mean</th>
<th>t value</th>
<th>p Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price</td>
<td>5.61</td>
<td>-6.88</td>
<td>&lt;.0001</td>
</tr>
<tr>
<td>Return Policy</td>
<td>4.72</td>
<td>-2.69</td>
<td>0.009</td>
</tr>
<tr>
<td>Shipping Speed</td>
<td>4.46</td>
<td>-0.9</td>
<td>0.37</td>
</tr>
<tr>
<td>Customer Service</td>
<td>4.44</td>
<td>-0.76</td>
<td>0.45</td>
</tr>
<tr>
<td>Privacy Policy</td>
<td>4.27</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Website Design</td>
<td>4.11</td>
<td>0.63</td>
<td>0.53</td>
</tr>
<tr>
<td>Customer Reviews</td>
<td>3.9</td>
<td>1.37</td>
<td>0.18</td>
</tr>
<tr>
<td>Software Compatibility</td>
<td>3.69</td>
<td>2.36</td>
<td>0.02</td>
</tr>
<tr>
<td>Webpage Load Speed</td>
<td>3.63</td>
<td>2.69</td>
<td>0.009</td>
</tr>
<tr>
<td>Popularity</td>
<td>3.55</td>
<td>2.85</td>
<td>0.0058</td>
</tr>
<tr>
<td>Physical Location</td>
<td>2.48</td>
<td>8.01</td>
<td>&lt;.0001</td>
</tr>
<tr>
<td>Cell Phone Compatibility</td>
<td>0.46</td>
<td>19.5</td>
<td>&lt;.0001</td>
</tr>
<tr>
<td>Accessibility for Sight-Impaired Users</td>
<td>0.3</td>
<td>21.0</td>
<td>&lt;.0001</td>
</tr>
</tbody>
</table>

**Experimental Protocol**

Participants were randomly assigned to one of the three study conditions and told that the purpose of the study was to test the usability of a “new searching and shopping search engine developed at Carnegie Mellon.” To reduce any framing effects, Privacy Finder was renamed Finder, and participants did not see or have access to the privacy preference settings. Instead, Finder was configured to use the “medium” privacy setting. The “medium” setting calculates a warning based on the sharing of personal financial information, purchase information, or personally identifying information; the refusal of a website to allow a user to remove their personal information from marketing lists; and the lack of the ability to allow users to view their own information.

After reading and signing the human subjects informed consent form, participants were given a Search Engine Key to refer to throughout the experiment. To familiarize participants with the interface and draw the focus away from the purchasing tasks, participants were asked to complete a total of six search tasks, where instructions were provided for each task, one task at a time. The fourth and sixth tasks required participants to search for vendors that sell a specified item (one a privacy-sensitive item and one a non-privacy sensitive item); to select one site from which to make a purchase with their credit card; and to write down the website from which they had made their purchase and the total price they paid. We randomized the order in which the two purchasing tasks were presented to participants. The web browsers were configured so that all traffic passed through a proxy server to create logs noting the number of websites browsed, visits to the privacy reports, and visits to the privacy policies of the websites perused.

**Product Selection**

We selected the non-privacy-sensitive item and privacy-sensitive item based on the online concerns survey. Due to budgetary constraints, we selected products that had an average cost of $15 per item including shipping. These products also had to be available from a variety of websites unknown to the participants with diverse privacy policies. The non-privacy-sensitive item is an office supply product: an 8-pack of Duracell AA batteries. The privacy-sensitive item is a vibrating sex toy, the “Pocket Rocket Jr.”
Incentives and Reimbursements

We paid participants a two-part “lump sum” payment of $45 for their participation in the study. The participants kept the products and the remainder of the money after the purchases were made. To best capture a “premium” that participants paid for privacy, we ordered search results based on both level of privacy and price. The first item was the least expensive and sold by a web site without a P3P policy (thus no privacy information was readily available). Subsequent results increased from low to high privacy as the prices increased, as shown in Figure 2. Based on previous pilot studies, we found that participants were unlikely to browse beyond the first four search results. Thus, we did not care about the specific order of privacy levels beyond these first four sites.

Figure 2: Search engine results interface viewed by participants in the Privacy Information condition.

We paid close attention to how we would reimburse participants for their purchases. User study payments were made in two installments to prevent gaming the study (for instance, canceling the purchase after the study). At the end of the session, participants were given $10 in cash. Once the products shipped and the study participants sent us tracking numbers or product packing slips, they were mailed money orders as the remaining payment.

Due to product availability and the fluctuation of product and shipping prices, we used marginally different sets of search results during the study2 (see Appendix A: Search Results), while keeping both the price and privacy policy distributions fairly constant. The premium for “high privacy” for batteries ranged from 3-5% of the product cost while the premium for the vibrator ranged from 7-10%. Due to problems encountered with the retailers during the purchasing tasks and some participants’ refusal to make some of the purchases, we continued to recruit participants until we had collected 48 complete responses for the study.3

Exit Survey

Upon completion of the study tasks, participants completed an exit survey. We asked how the privacy icon (if seen) played a role in their purchasing decisions, whether they understood what the icon represented, whether they read any of the privacy policies, and if those privacy policies influenced their purchasing decisions.

---

2 The first (and cheapest) result for the batteries search was out of stock while 18 participants completed the experiment. Thus we could not use these participants’ battery purchase data and recruited 18 additional participants.

3 Due to the nature of the privacy-sensitive product, two participants opted to cease their participation in the study, six opted out of the privacy-sensitive product purchase but completed the remainder of the study, and one decided not to purchase either item but completed the exit survey.
Results

We found that participants in the privacy information condition were more likely to make purchases from websites offering medium or high levels of privacy, while those in the control conditions generally made purchases from the lowest priced vendor. This indicates that individuals are likely to pay a premium for privacy once the privacy information is made more accessible. Furthermore, individuals presented with the same indicators as those used for the privacy group, but ostensibly attached to irrelevant merchants’ features, were unlikely to take these indicators into consideration when making purchases. Thus, we demonstrate that the behavior we observed cannot be attributed to an interest in purchasing from web sites labeled with attractive indicators.

Meaningful Privacy Information

Hypothesis 1: Participants in the privacy information condition will be more likely than those in the irrelevant information or no information conditions to purchase from websites annotated with icons. – Supported.

One of the goals of this study was to determine whether having clearly defined privacy indicators makes a significant difference over the irrelevant “handicap accessibility” icons, or “no information” as seen by the control groups. Overall, we found that there were statistically significant results in this area as shown in Table 3.

<table>
<thead>
<tr>
<th></th>
<th>Condition 1: No Information</th>
<th>Fisher's Exact $p$ (Condition 1 &amp; 3)</th>
<th>Condition 2: Irrelevant Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Purchase Battery</td>
<td>11.1%</td>
<td>&lt; .0001</td>
<td>79%</td>
</tr>
<tr>
<td>Fisher's Exact $p$ (Condition 1 &amp; 3)</td>
<td>&lt; .0001</td>
<td>79%</td>
<td>&lt; .002</td>
</tr>
<tr>
<td>Condition 3: Privacy Information</td>
<td>79%</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>Fisher's Exact $p$ (Condition 2 &amp; 3)</td>
<td>&lt; .002</td>
<td>25%</td>
<td></td>
</tr>
<tr>
<td>% Purchase Sex Toy</td>
<td>16.0%</td>
<td>&lt; .005</td>
<td>66.7%</td>
</tr>
<tr>
<td>Fisher's Exact $p$ (Condition 1 &amp; 3)</td>
<td>&lt; .005</td>
<td>66.7%</td>
<td></td>
</tr>
<tr>
<td>Condition 3: Privacy Information</td>
<td>66.7%</td>
<td>27.8%</td>
<td></td>
</tr>
<tr>
<td>Fisher's Exact $p$ (Condition 2 &amp; 3)</td>
<td>&lt; .02</td>
<td>27.8%</td>
<td></td>
</tr>
</tbody>
</table>

Table 3: A between-subjects comparison of the proportion of purchases made from sites with privacy icons in the privacy condition and those sites in the No Information and Irrelevant Information conditions.

The proportion of purchases from sites with privacy icons was greater for both products as compared to the no information and irrelevant information conditions. These results indicate that providing privacy information in a more salient format does help people choose sites that have better privacy policies.

Hypothesis 2: Participants in the privacy information condition will be more likely than those in the irrelevant information and no information conditions to purchase from websites annotated with the four-green-boxes icon. – Supported

When purchasing from sites with privacy icons, participants in the privacy condition selected from sites with the four-green-box “high privacy” symbol for 60% of the battery purchases (Fisher’s exact $p < .0001$), and 50% of the sex toy purchases (Fisher’s exact $p < .0001$). For each condition, the percentage of purchases made at each level of privacy is depicted in Figure 3.

Figure 3 also clearly indicates the differences between the conditions of the user study. There were a greater percentage of purchases made at four-green-box sites with privacy information than with no information or irrelevant information for both items. Additionally, there do not seem to be very large differences in the purchasing patterns for the no information and irrelevant information conditions.

---

4 These results are based on a test of proportions in the privacy condition comparing purchases made from sites with privacy icons to the level of privacy indicated by those icons.
Privacy Premium

Hypothesis 3a: Participants presented with prominent privacy information (those in the privacy information condition) will be more likely than those in the other conditions to pay a premium to purchase from sites that have better privacy policies. – Supported

As stated previously, this experiment also allowed us to determine whether or not individuals would be willing to pay a premium for enhanced privacy protections (although it is important to note that the goal of the study was not to quantify a specific premium for the selected products). When comparing the average purchase prices of the no information group with the purchase prices of the irrelevant information group in a t-test, we did not find significant differences in the prices paid for each product, as shown in Error! Reference source not found.

Table 4: Comparison of mean price paid for each product in the control conditions. Based on t-tests, there was no significant difference between displaying irrelevant information, and displaying no information.

<table>
<thead>
<tr>
<th></th>
<th>Condition 1: No Information</th>
<th>Condition 2: Irrelevant Information</th>
<th>Premium</th>
<th>p Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Price - Batteries</td>
<td>$14.64</td>
<td>$14.69</td>
<td>$0.05</td>
<td>0.64</td>
</tr>
<tr>
<td>Mean Price – Sex Toy</td>
<td>$15.26</td>
<td>$15.30</td>
<td>$0.04</td>
<td>0.65</td>
</tr>
</tbody>
</table>

When comparing the no information condition to the privacy information condition, we found statistically significant privacy premiums for both products, as detailed in Table 5. Note that, in the course of the study, due to product constraints and fluctuating prices, the first result for the batteries was replaced with a slightly cheaper result, while the first result for the vibrator was replaced with a slightly more expensive result. All of these changes were on the order of a few cents and we found no evidence that these changes impacted purchase decisions. Based on t-tests, we found that individuals who were shown privacy information were significantly more likely (p < 0.001 in both cases) to pay a premium to purchase from sites with better privacy policies. This effect was present for purchases of the privacy-sensitive item as well as the non-privacy-sensitive item.
Privacy Premium

<table>
<thead>
<tr>
<th></th>
<th>Condition 1: No Information</th>
<th>Condition 3: Privacy Information</th>
<th>Premium</th>
<th>p Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean Price - Batteries</td>
<td>$14.64</td>
<td>$15.23</td>
<td>$0.59</td>
<td>0.0007</td>
</tr>
<tr>
<td>Mean Price - Sex Toy</td>
<td>$15.26</td>
<td>$15.88</td>
<td>$0.62</td>
<td>0.00005</td>
</tr>
</tbody>
</table>

Table 5: T-test comparison of mean prices paid in the no information and the privacy information conditions.

Hypothesis 3b: In the absence of prominent privacy information, people will purchase where price is lowest. – Supported

Participants in the control conditions tended to purchase both items from the least expensive (first) website: for batteries, 83.3% in the no information condition (Fisher’s exact p = .007), and 75% in the irrelevant information condition (Fisher’s exact p < .0001); and for the sex toy, 80% in the no information condition (Fisher’s exact p < .0001), and 66.7% in the irrelevant information condition (Fisher’s exact p < .0001). This indicates that participants not shown prominent privacy information were significantly more likely to make their purchases from the cheapest website. Since these websites were also the first search results listed, it is unclear if participants made their decisions solely based on price or if they simply went to the first sites listed, as they were likely unfamiliar with all of the sites in the search results. Thus, there is a chance that without additional information, participants were trying to finish the task as quickly as possible.

The Impact of Icons

Hypothesis 4: Icons or symbols affect purchase decision, regardless of meaning. – Not Supported

We detected no statistically significant differences between the control condition purchasing patterns, detailed in Table 6. The green box icon itself was not a decision-making factor for the irrelevant information condition. This implies that our results are due to the privacy signals that the icons carry. Future studies may not need to account for the “icon as a decision-making factor.”

Purchases Made between Conditions from Sites Annotated with a Privacy Icon

<table>
<thead>
<tr>
<th></th>
<th>Condition 1: No Information</th>
<th>Condition 2: Irrelevant Information</th>
<th>Fisher’s Exact p</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Purchase Battery</td>
<td>11.11%</td>
<td>25%</td>
<td>0.39</td>
</tr>
<tr>
<td>% Purchase Sex Toy</td>
<td>16.0%</td>
<td>27.8%</td>
<td>0.46</td>
</tr>
</tbody>
</table>

Table 6: This table indicates that there were no significant differences between the group without annotated search results and the group with search results annotated with irrelevant information.

Product Differences

Hypothesis 5a: The effect of the privacy information will be greater when participants purchase privacy-sensitive items than when they purchase non-privacy-sensitive items. – Not Supported

Hypothesis 5b: When no privacy information is provided, privacy-sensitive and non-privacy-sensitive purchase decisions will be treated similarly. – Supported

---

5 The proportions compare the rank of the purchase website in each condition for each product and the whether or not the site had (or would have had based on the condition) a privacy icon.
While participants generally indicated that they had more privacy concerns when purchasing the vibrator as compared to the batteries, their purchasing patterns did not reflect these concerns. Participants within each condition did not purchase from a significantly greater number of sites with “better” privacy policies when purchasing the vibrator, as compared to the batteries. These proportions are detailed in Table 7. Instead, Figure 4 indicates that there are larger clusters of purchases made at the high privacy sites for both batteries and vibrators.

<table>
<thead>
<tr>
<th>Condition 1: No Information</th>
<th>% Purchase Battery</th>
<th>% Purchase Sex Toy</th>
<th>McNemar’s p</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>12.5</td>
<td>12.5</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition 2: Irrelevant Information</th>
<th>% Purchase Battery</th>
<th>% Purchase Sex Toy</th>
<th>McNemar’s p</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>25.0</td>
<td>18.8</td>
<td>1.0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition 3: Privacy Information</th>
<th>% Purchase Battery</th>
<th>% Purchase Sex Toy</th>
<th>McNemar’s p</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>81.3</td>
<td>62.5</td>
<td>0.38</td>
</tr>
</tbody>
</table>

Table 7: Comparison within each condition for the proportion of products purchased from sites annotated with privacy icons. The high p value indicates that the null hypothesis cannot be rejected.

Figure 4: Percentage of purchases made for each product at all the different levels of privacy for each condition.

When asked in the exit survey about the levels of concern for personal information when purchasing the two products, there were differences between the items. Specifically, when purchasing the vibrator, people expressed greater concern about what a company would do with an email address, physical address, and purchase history. This is understandable because the purchase of a vibrator from an online sex store generates concerns about receiving unwanted email with sexually-related content, having others accidentally receive your product or

---

6 We asked participants “What was your level of concern for your privacy when you were purchasing the products in this study?” A paired t-test indicated a statistically significant difference between the levels of concern for each item (based on a 7-point Likert scale for the participant’s level of concern ranging from Not Concerned At All to Very Concerned). The sex toy (M = 4.97) had a higher level of concern compared to batteries (M = 3.33), t(69) = -6.3, p < .001.

7 A paired t-test for all participants indicated a higher level of concern for what a company would do with an email address for the vibrator (M = 4.77) as compared to the battery, (M = 4.1), t(69) = -3.43, p = .001.

8 A paired t-test for all participants indicated a higher level of concern for what a company would do with a physical address for the vibrator (M = 4.76) over the battery (M = 3.84), t(69) = -4.62, p < .0001.

9 A paired t-test for all participants indicated a higher level of concern for what would be done with a purchase history for the vibrator (M = 4.14) over the battery (M = 3.17), t(69) = -5.25, p < .0001.
promotional materials, and having “that type of purchase” attached to your purchase or credit history. As one participant noted, “It is just sort of weird to give random sex sites your email address because that's pretty much just asking for spam.”

In the privacy condition, no differences were detected between the proportions of males or females who purchased from sites with privacy icons, for either product. Similarly, there were no statistically significant correlations between purchasing from sites with privacy icons and gender or age.

It is important to note that in the design of the study, there was a smaller premium for privacy with regard to the batteries than with the vibrator, and this may have been a factor in the purchasing patterns. The privacy premium—the additional amount of money participants paid to purchase from a site with a better privacy policy, as opposed to the cheapest site—for high privacy for batteries was around $0.63, whereas the privacy premium for the vibrator was around $1.32. This may indicate that participants were willing to pay around fifty cents for increased privacy, but were unwilling to spend much more than a dollar, regardless of the nature of the item. This finding may show a need for future studies that examine exactly how much people are willing to pay for better privacy.

**Contributions and Implications**

Our study provides evidence of the role of privacy information on privacy-relevant decision-making, and offers new insight on consumers’ valuations of personal data. We found that participants provided with clear and accessible privacy information condition took that information into consideration during their decision-making, making purchases from websites offering medium or high levels of privacy. From a research perspective, our results indicate that, contrary to the common view that consumers are unlikely to pay for privacy, consumers may be willing to pay a premium for privacy. Two implications for future research are the need to estimate the relationship between privacy and price sensitivity, and a more granular understanding of the behavioral and cognitive factors that change consumer’s decision when privacy information is made more accessible.

Our results also indicate that companies may combine a) privacy-friendly privacy policies, and b) technological means to clearly showcase the former to prospective consumers to gain a competitive advantage. In other words, companies may direct their policies and their information systems to strategically manage their privacy strategies in ways that are not only compatible with government best-practices and self-regulatory recommendations, but are actually profit-maximizing. Specifically, as the adoption of P3P increases, it would behoove companies who are protective of customer privacy to post P3P policies to signal their “good” privacy practices to attract consumers. Survey data indicates that online consumers place greatest importance on knowing what will be done with personal information, and how they can have direct control over their information (Malhotra, et al. 2004). In many instances, consumers have little control over the practices of those collecting their information. Where consumers do have control is in the selection of businesses with whom they share their information, and the type of information provided.

**Limitations**

It is important to note that the goal of the study was not to determine any absolute premium for the selected products. Additionally, the impact of the type of product as compared to the premium that consumers are willing to pay needs further investigation. In the design of this study, there was a smaller premium for privacy with regard to the batteries than with the sex toy and this may have been a factor in the purchasing patterns. This finding may show a need for future studies that examine exactly how much people are willing to pay for better privacy.

Our next steps include implementing a Privacy Finder field study so that we can evaluate the impact of privacy information in a more natural setting. We plan to solicit participants to use Privacy Finder as their primary search engine. We will use cookies and server logs to track anonymized searches and results, and analyze web-browsing

---

10 Comparing the proportions of battery purchases, 42.1% of females compared to 36.8% of males purchased from sites with a privacy icon, Fisher’s exact \( p = 1.0 \). For the vibrator, 38.1% of females and 28.6% of males purchased from sites with a privacy icon, Fisher’s exact \( p = 0.66 \). For both, the null hypothesis that the proportions for each gender are equal cannot be rejected.

11 The correlations are the following: Age and BatteryPrivacy (\( \beta = .33, p = 0.17 \)), Age and VibePrivacy (\( \beta = -0.23, p = 0.33 \)), Gender and BatteryPrivacy (\( \beta = -0.027, p = 0.91 \)), Gender and VibePrivacy (\( \beta = -0.13, p = 0.56 \)). The high \( p \) values indicate that these correlations are not statistically significant.
behavior. With this information we can determine if participants visit sites with privacy icons, the privacy levels of those sites, and if they view privacy reports. We also plan to conduct additional user studies to determine the privacy premium for certain products. For these studies, we can eliminate either the no information or irrelevant information condition, since there were no significant differences in the purchasing patterns of these conditions. We also plan to contact the websites selected for the purchasing tasks and make arrangements with them so that they will not change their prices or run out of inventory during the course of the study.

Conclusions

The goal of this study was to determine whether the availability and accessibility of privacy information affects individuals’ purchasing decision. In turn, investigating that question would allow us to discuss whether companies can leverage privacy protection as a selling point. Our study focused on what happens when tools become available to prominently display an organization’s privacy policies. We used Privacy Finder to display the privacy policies of certain online shopping sites in a fashion that, arguably, reduces the gap of information asymmetry that separates merchants and customers vis a vis the usage of the customer’s data. We found that participants were affected by having this additional information displayed to them. Our experiment shows that that once privacy information is made more visible, people will tend to purchase from merchants that offer more privacy protection and even pay a premium to purchase from such merchants. This was true for both privacy-sensitive and non-privacy-sensitive items. Our results suggest that companies have ways to turn self-regulative efforts to protect consumers’ privacy into tools for competitive advantage.

References


Appendix A: Search Results

Below are the search results presented to the participants in the purchasing tasks for the user study. The “Difference” is the difference between the total price of that item and the item previous.

**Non-Privacy Sensitive Item**

Duracell AA Batteries – 8 Pack

<table>
<thead>
<tr>
<th>Price with Shipping</th>
<th>Difference</th>
<th>Privacy Level</th>
<th>Privacy Icon</th>
<th>Price with Shipping</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$14.60</td>
<td>$0.00</td>
<td>N/A</td>
<td></td>
<td>$14.45</td>
<td>$0.00</td>
</tr>
<tr>
<td>$14.96</td>
<td>$0.36</td>
<td>Low</td>
<td>☐ ☐ ☐ ☐</td>
<td>$14.60</td>
<td>$0.15</td>
</tr>
<tr>
<td>$15.07</td>
<td>$0.11</td>
<td>Med</td>
<td>☐ ☐ ☐ ☐</td>
<td>$14.80</td>
<td>$0.20</td>
</tr>
<tr>
<td>$15.14</td>
<td>$0.07</td>
<td>High</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$15.14</td>
<td>$0.34</td>
</tr>
<tr>
<td>$15.85</td>
<td>$0.71</td>
<td>N/A</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$15.85</td>
<td>$0.71</td>
</tr>
<tr>
<td>$15.98</td>
<td>$0.13</td>
<td>N/A</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$15.98</td>
<td>$0.13</td>
</tr>
<tr>
<td>$14.60</td>
<td>$0.44</td>
<td>Low</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$16.42</td>
<td>$0.84</td>
</tr>
<tr>
<td>$14.96</td>
<td>$0.43</td>
<td>High</td>
<td>☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$16.85</td>
<td>$0.34</td>
</tr>
</tbody>
</table>

Premium for High Privacy (Session 1) $0.54 3.7%
Premium for High Privacy (Session 2) $0.69 4.8%

**Privacy Sensitive Item**

Pocket Rocket Jr.

<table>
<thead>
<tr>
<th>Price with Shipping</th>
<th>Difference</th>
<th>Privacy Level</th>
<th>Privacy Icon</th>
<th>Price with Shipping</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>$15.08</td>
<td>$0.00</td>
<td>N/A</td>
<td>☐ ☐ ☐ ☐</td>
<td>$15.36</td>
<td>$0.00</td>
</tr>
<tr>
<td>$15.74</td>
<td>$0.66</td>
<td>Low</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$15.74</td>
<td>$0.38</td>
</tr>
<tr>
<td>$15.90</td>
<td>$0.16</td>
<td>Med</td>
<td>☐ ☐ ☐ ☐ ☐</td>
<td>$15.90</td>
<td>$0.16</td>
</tr>
<tr>
<td>$16.54</td>
<td>$0.64</td>
<td>High</td>
<td>☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$16.54</td>
<td>$0.64</td>
</tr>
<tr>
<td>$16.79</td>
<td>$0.25</td>
<td>N/A</td>
<td>☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$16.79</td>
<td>$0.25</td>
</tr>
<tr>
<td>$16.79</td>
<td>$0.89</td>
<td>N/A</td>
<td>☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$16.79</td>
<td>$0.89</td>
</tr>
<tr>
<td>$17.94</td>
<td>$1.15</td>
<td>Low</td>
<td>☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$17.94</td>
<td>$1.15</td>
</tr>
<tr>
<td>$18.95</td>
<td>$2.16</td>
<td>High</td>
<td>☐ ☐ ☐ ☐ ☐ ☐ ☐</td>
<td>$18.95</td>
<td>$2.16</td>
</tr>
</tbody>
</table>

Premium for High Privacy (Session 1) $1.46 9.7%
Premium for High Privacy (Session 2) $1.18 7.7%