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

Janice Tsai, Serge Egelman, Lorrie Cranor, Alessandro Acquisti
Carnegie Mellon University

The 6th Workshop on the Economics of Information Security (WEIS)
June 2007

Abstract

While most people claim to be very concerned about their privacy, they do not consistently take actions to protect it. Web retailers detail their information practices in their 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 provided by retailers in a machine-readable format. Privacy Finder annotates search results with a "privacy icon" and a "privacy report." The privacy icon provides a privacy rating for the retailer on a five-point scale. The privacy report summarizes information contained in traditional privacy policies in a short, concise format. Our research shows that providing accessible privacy information reduces the information asymmetry gap between merchants and consumers. This reduction tends to lead consumers to purchase from online retailers who better protect their privacy. Additionally, 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.

1 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 (Harris Interactive, 2001; CBS News, 2005; P&AB, 2005; Turow, *et al.,* 2005). One method the government and industry use to address privacy concerns is to recommend that businesses post privacy policies to convey their privacy 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. We conducted an online privacy concerns survey to determine the privacy concerns and perceived risks associated with online shopping, and we conducted an experiment in which participants had to make purchase decisions that would *directly* affect their privacy. We framed the experiment as an online shopping experience at existing (rather than simulated) online merchants, and tested whether signals about the different levels of privacy protection among merchants would affect the participants' price sensitivity and purchase decisions.

Contrary to the common view that consumers are unlikely to pay for privacy, formed due to the failure of online anonymity services (Brunk, 2002), we found that when privacy information is made more salient, consumers are willing to pay a premium for privacy when purchasing both non-privacy-sensitive and privacy-sensitive items. However, those individuals who were not presented with prominent privacy information were likely to make purchases from the vendor with the lowest price, regardless of that site's privacy policies.

Our study provides evidence of the role of incomplete information on privacy-relevant decision-making, and offers new insight on consumers' valuations of personal data. 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. Our results indicate that providing privacy information in a clear-cut fashion reduces information asymmetry (the gap between the merchant's and the consumer's knowledge of what will happen to the consumer's data) and the burden on the individual to calculate the risks and benefits of providing their personal information, thus also addressing the problem of bounded rationality.

In Section 2 we present background information on privacy concerns and privacy policies, and describe our search engine privacy interface, Privacy Finder. We describe our research methodology in Section 3 and the results of our online shopping user study in Section 4. We present our conclusions in Section 5.

2 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).

An individual's specific privacy concerns may vary due to the situation or circumstances. Smith, *et al.* (1996) outlined four dimensions of privacy concerns for organizational practices: *collection* of personal information, *unauthorized secondary use* of personal information, *errors* in personal information, and *improper access* to personal information. For online marketing, the dimensions of concern are reframed as the *collection* of personal information, the *control* over the use of personal data, and the *awareness* of privacy practices and uses of personal information (Malhotra, *et al.* 2004). Brown and Muchira (2004) identified three dimensions of consumer concern in online purchasing behavior: *unauthorized secondary use, errors* in personal information, and the *invasion of privacy*.

Despite their concerns, consumers have also been found to be willing to provide personal information for small discounts and 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. This dichotomy between professed attitudes and actual behavior has led a number of experiments aimed at gaining an understanding of what really drives users' valuations of privacy. Rose (2005) used a contingent valuation survey to estimate the economic value subjects place on a change in data protection laws that would give the subjects enforceable property rights in their personal information. The author found that while most survey participants expressed high sensitivity to privacy, their willingness to pay for such strong property rights was low – only 47.5% of those surveyed would pay for it (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. In addition, providing personal information to an online merchant may decrease future search or transaction costs, with positive implications for both seller and buyer (Brynjolfsson *et al.,* 2003). Still, Chellapa and Sin (2005), in a study of the trade-offs consumers face between personalization and privacy, noted that online companies need to gain consumers' trust if they want to implement personalization, in order to overcome the negative implications of their privacy concerns.

Several possible explanations for this apparent dichotomy have been discussed in the literature (Acquisti and Grossklags, 2003; Shostack, 2003; Syverson, 2003; Acquisti, 2004): 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 phenomena, 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).

While privacy policies are an attempt to reduce information asymmetry and have become prevalent (Milne and Culnan, 2002), privacy information remains invisible to Internet users: privacy policies have not been effective at making privacy information accessible. People rarely read them (Privacy Leadership Initiative, 2001; Jensen, *et al.*, 2005), and the policies themselves are difficult to understand (Hochhauser, 2003; Jensen and Potts, 2004). 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 developed the Platform for Privacy Preferences (P3P) to make privacy policies more usable and reduce information asymmetry. P3P is a standard machine-readable format for privacy policies. People can use software tools called "P3P user agents" to define their privacy preferences and determine if websites' P3P privacy policies match those preferences (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).

The Carnegie Mellon University Usable Privacy and Security (CUPS) Laboratory developed a P3P-enabled search engine named Privacy Finder (http://privacyfinder.org) that 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.

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 user's privacy preferences. The icons represent a five-point privacy "meter," as shown in 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 do not have a privacy icon associated with them.

Icon	***Site***
	Matches privacy preferences
	
	
	Does not match privacy preferences
	

Table 1: Privacy Finder's privacy indicators

Privacy Finder also provides a link to the privacy report for each P3P-enabled website. This report (shown in Figure 1) is generated from the site's P3P policy. 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).

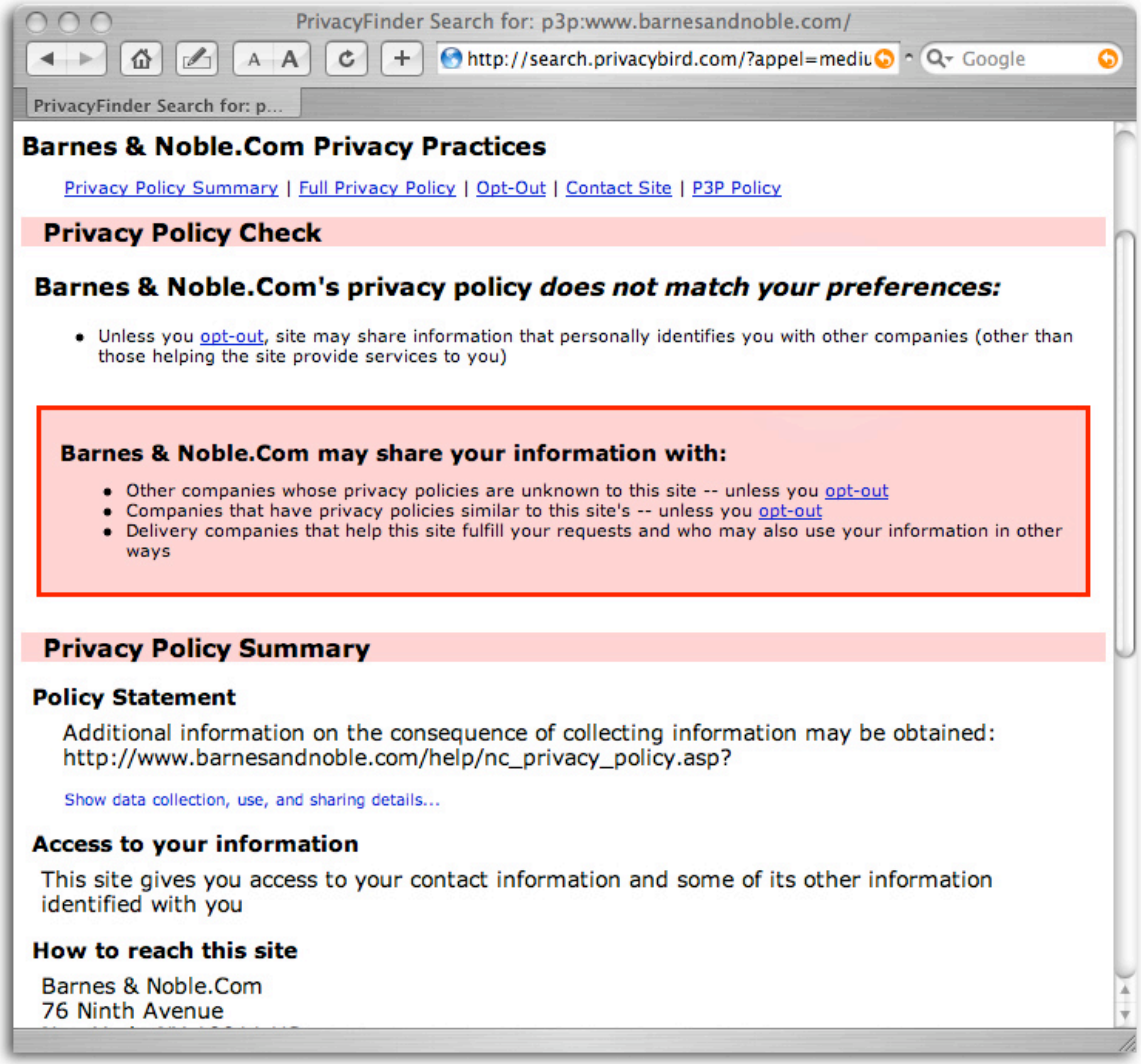


Figure 1: Privacy policy summary generated for BarnesandNoble.com

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 using 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.

3 Methodology

The goal of this study was 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. We investigated these questions through a laboratory experiment and exit survey. In addition, we conducted a preliminary survey that aided in the design of the laboratory experiment.

The preliminary survey was designed to investigate what types of privacy concerns individuals have when they use the Internet to shop. Its results informed the design of the user experiment. The user experiment was designed to examine the role that prominent privacy information plays in 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. We used three groups in our between-subjects design: a control group that saw search results without any annotations (the "no information" condition); a second control group that saw search results annotated with icons representing irrelevant information (the "irrelevant information" condition); and an experimental group that saw search results annotated with privacy icons and privacy reports (the "privacy information" condition). The experiment was structured such that we could test the following hypotheses:

Hypothesis 1: Participants in the privacy information condition will be more likely than those in the irrelevant information condition 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 condition to purchase from websites annotated with the four-green-boxes icon.

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.

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

Hypothesis 4: Icons or symbols will affect purchase decisions, regardless of meaning.

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.

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

3.1 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.

In September 2006, we solicited participants to complete an “Online Privacy Concerns” survey, administered via SurveyMonkey, an online survey creation and administration tool.[1] Notices about the survey were posted on the *Volunteers* section of Craigslist, a free online message board/classified posting website, in the major metropolitan areas of the United States. The survey was available for one week and used a lottery for a 4 GB iPod Nano music player as the incentive for participation. In the recruiting message, we solicited individuals who were over the age of 18 and who had made at least one online purchase in the past year.

[1] SurveyMonkey.com. http://surveymonkey.com/.

3.1.1 Basic Demographics

The final sample included 276 individuals. The ages of the participants ranged from 18 to 71 years old (M = 30.2 years). Of all the respondents, 62.5% were female. The individuals in our sample were well-educated, with 85.5% reporting that they had completed at least a college degree.

Respondents tended to be heavy Internet users with about 75% of respondents reporting spending more than 10 hours online per week. Our sample consisted of people who were also very experienced in shopping online: 43.5% had made 2 or 3 online purchases in the previous month while 27.2% had made 4 or more purchases.

3.1.2 Scenarios

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 the following:

- If your credit card number were stolen after you made an online purchase? (Credit Card)
- If you received unwanted emails after you made a purchase? (Unwanted Email)
- If you continued to receive email from an online store even after you've asked them to take you off their mailing list? (Continued Contact)
- If an online store sold your name and contact information to other companies after you made an online purchase? (Information Sold)
- If an online store kept track of all the items you click on at their website? (Track Items)
- If an online store inferred information about your habits or interests after you make a purchase? (Infer Information)
- If your search engine history was made public? (Search History)
- If your purchase history from multiple online stores was combined with other personal information to produce a detailed profile about you? (Dossier)
- If your family members or friends accessed your online purchase records without your permission? (Family/Friends)
- If current, perspective, or future employers learned about your online purchase history? (Employers)
- If your purchase history from an online store was made available during a lawsuit you are involved in? (Lawsuit)

The responses to the online concern scenarios are detailed in Figure 2.

Respondents seemed to be the least concerned with the scenarios that they found to be 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 policies and Privacy Finder were the ones that respondents 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.

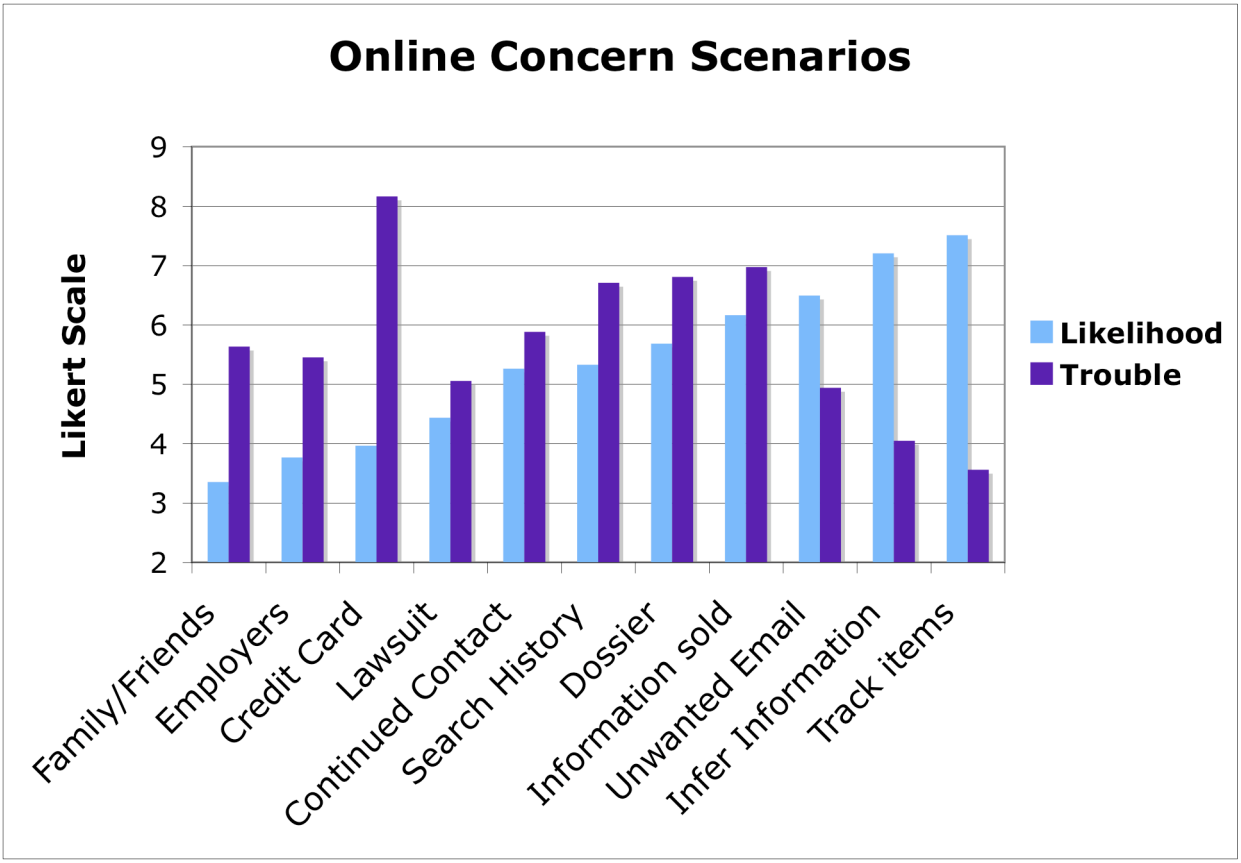


Figure 2: Online concern scenarios with the trouble caused and average likelihood based on an 11-point Likert scale.

3.1.3 Survey Insights

We used the survey results to help identify products for participants to purchase in our online shopping experiment. We wanted to find a privacy-sensitive item that would raise significant concerns for most participants as well as an item that would not raise privacy concerns. We posed the following survey 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. Figure 3 shows the list of items and their purchase likelihood scores.

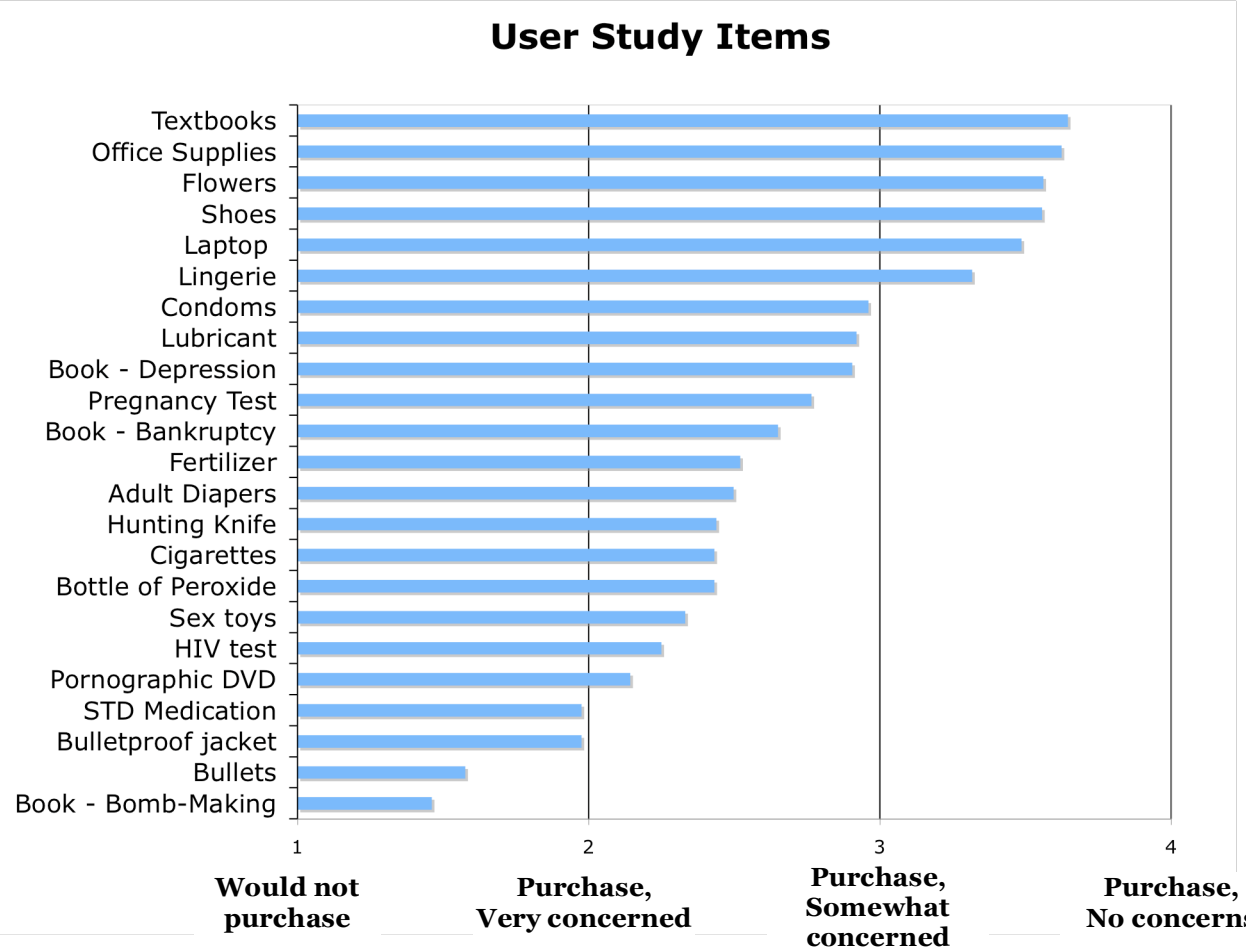


Figure 3: User study items and their corresponding purchase likelihoods.

Most participants showed little resistance to purchasing common products, such as office supplies, online. We detected increasing hesitance as we moved to items that involved personal values and mental states, such as items related to sex and books related to depression. When the items were indicative of violent behavior, such as bullets and a book on bomb-making, we found significant reservations and reluctance to purchasing the items.

3.2 Online Shopping Experiment

We conducted an online shopping experiment in our laboratory at Carnegie Mellon University. In this section we describe our participant recruitment, screening survey, experimental protocol, and exit survey.

3.2.1 Participant Recruitment

Participants were recruited from the general Pittsburgh population. Flyers for an "Online searching and shopping study" were posted around Pittsburgh and online in the *Volunteers* section of Craigslist Pittsburgh.[2] The study was also posted on the experiments scheduling site for the Center of Behavioral and Decision Research at Carnegie Mellon.[3] Participants were required to be at least 18 years old, have a personal credit card for use during the study, and

[2] Pittsburgh Volunteers Classifieds – Craigslist. http://pittsburgh.craigslist.org/vol/.

[3] Experiments at Carnegie Mellon University. http://cbdr.cmu.edu/experiments/.

have experience shopping online. The flyer also advertised that participants would be paid to shop online using our money and "Keep[ing] the change."

3.2.2 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 only 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 are equally important.

We used the purchasing factors ratings to determine what factors have minimal impact on purchase decisions and thus can be considered irrelevant. 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.

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

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*.

We also used the screening survey to learn about respondents' concerns regarding various privacy practices. Table 3 depicts the mean responses as well as the significance of each item. The responses to these questions reflect the components of a P3P policy. Since participants cared very strongly about these aspects of privacy, it suggests that Privacy Finder is serving users well.

Item of Concern	Average Response	t Value	*p* Value
A site uses information that does not personally identify you to determine habits, interests, or other characteristics	2.97	-0.013	0.9
A site shares information that does not personally identify you	3.25	1.13	0.26
A site contacts you about other services via email or postal mail	3.65	3.52	0.0008
A site uses your health information to determine content or ads	3.83	3.9	0.0002
A site uses personally identifying information to determine your habits, interests, or other characteristics	4.04	5.24	<.0001
A site makes its privacy policy available	4.45	6.97	<.0001
A site contacts you about services or products via telephone	4.83	11.6	<.0001
A site shares your health information with other companies	5.01	11.9	<.0001
A site uses your financial information to determine content or ads	5.03	11.69	<.0001
A site shares personally identifying information with other companies	5.08	13.56	<.0001
A site does not allow you to find out what information it stores about you	5.35	17.86	<.0001
A site does not allow you to be removed from mailing lists	5.42	18.28	<.0001
A site shares your financial information with other companies	5.54	19.78	<.0001

Table 3: Average answers to the privacy concern questions in the screening survey. The scores are based on a 7-point Likert scale with a maximum value of 6.0, ranging from *Not Concerned At All* to *Extremely Concerned*. The significance was calculated in a t-test comparing the responses to a neutral baseline of 3.0.

3.3 Laboratory Experiment

Participants who responded to the scheduling inquiry were randomly assigned to one of the three study conditions (no information, irrelevant information, and privacy information). The experiment was conducted in the CUPS lab with one, two, or three participants at a time. Participants were told that the purpose of the study was to test the usability of a "new searching and shopping search engine developed at Carnegie Mellon University." 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 herself 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," (see Appendix A: Search Engine Keys) to inform them of the multiple features of the search engine (including the total price, with shipping, displayed next to each search result). The Search Engine Key was different for each condition, as explained in Section

3.3.3. Participants kept the Search Engine Key on the desk next to them 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 (see Appendix B: Experiment Instructions). The fourth and sixth tasks required participants to search for vendors that sell a specified item, and select one from which to make a purchase. Participants were instructed to purchase the item using their own credit card. They were asked to write down the website from which they had made their purchase and the total price they paid. One purchasing task involved a privacy-sensitive item and the other involved a non-privacy-sensitive item. We randomized the order in which the two purchasing tasks were presented to participants.

We paid participants $45 for their participation in the study. They were also permitted to keep the items they purchased. The items selected for purchase each cost around $15, including shipping.

3.3.1 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 have 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 P3P-enabled privacy policies.[4] 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." Based on the online concerns survey we believed that this was an item that people would purchase despite having significant privacy concerns.

3.3.2 Incentives and Reimbursements

We provided participants with a price incentive by providing a "lump sum" payment greater than the average cost of the items. The participants kept 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 is sold by a web site that does not have a P3P policy (thus no privacy information is readily available). Subsequent results increased in order from low to high privacy as the prices increased, as shown in Table 4. 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.

[4] If we provided search results from well-known websites or stores, there is a potential for bias: participants might make their purchase decisions for reasons other than the websites' privacy policies or the price of the items.

Optimal search results		
Result #	**Privacy Level**	**Price Difference**
1	None	*n*
2	Low ▢▢▢▢	*n* + ~$.25
3	Medium ■■▢▢	*n* + ~$.50
4	High ■■■■	*n* + ~$.75
5	None	*n* + ~$1.00
6	Low ▢▢▢▢	*n* + ~$1.25
7	Medium ■■▢▢	*n* + ~$1.50
8	High ■■■■	*n* + ~$1.75

Table 4: Optimal search results for purchasing tasks, $n \approx$$15.00. The first four results are the most important since pilot studies showed us that participants are unlikely to examine the other search results.

We paid close attention to how we would reimburse participants for their purchases. If a participant expects to cancel their order after the study, it is unlikely that he or she will give much thought to anything other than a site's return policy. User study payments were made in two installments to prevent this scenario. 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 the remaining payment as money orders.

Since we used actual merchants, we were unable to find sites that offered our ideal price distribution. Instead, we used results that had similar pricing differentials. Due to product availability and the fluctuation of product and shipping prices, we used marginally different sets of search results during the study[5] (see Appendix C: 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 various purchases, we continued to recruit participants until we had collected 48 complete responses for the study.[6]

[5] 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 because we were unable to determine if these participants purchased from the second result due to its price, privacy policy, or for other reasons. As a result we had to recruit 18 additional participants.

[6] Due to the nature of the privacy-sensitive product, two participants opted to cease their participation in the study altogether, 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. As a result we had to recruit additional participants. (Some of these participants are also the ones for which the batteries went out of stock.)

3.3.3 Experimental Design

We compared participant actions in the following three conditions to gauge the impact of providing privacy information.

- Condition 1, no information: 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 (see Appendix A: Search Engine Keys). During the experiment, their search results did not include any Privacy Finder icons (see Appendix D: Search Results Interfaces).
- Condition 2, 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: 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 as shown in Table 5.

	First Item			
	Non-Privacy-Sensitive		**Privacy-Sensitive**	
Condition 1: No Information	F = 4	M = 4	F = 4	M = 4
Condition 2: Irrelevant Information	F = 4	M = 4	F = 4	M = 4
Condition 3: Privacy Information	F = 4	M = 4	F = 4	M = 4

Table 5: User study conditions

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.

3.4 Exit Survey

Upon completion of the study tasks, participants completed an exit survey. This survey was designed to glean information about how privacy played a role in their purchasing decisions. We asked the participants about their concerns with each product, and how the online vendors

addressed those concerns. 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. We also provided each participant with the privacy report for each site from which they made their purchase, if it had one. Otherwise, the participant was given the privacy report for a site with a "medium" level of privacy. We asked if they had read the privacy report if they would have selected a different site from which to make a purchase and if they felt that the site adequately protected their privacy.

4 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 other 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 (such as handicap accessibility), 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.

4.1 Meaningful Privacy Information

Hypothesis 1: Participants in the privacy information condition will be more likely than those in the irrelevant information condition 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 6.

Purchases made from sites Annotated with a Privacy Icon

	Condition 1: No Information	**Fisher's Exact *p* (Condition 1 & 3)**	**Condition 3: Privacy Information**	**Fisher's Exact *p* (Condition 2 & 3)**	**Condition 2:** Irrelevant Information
% Purchase Battery	11.1%	< .0001	**79%**	< .002	25%
% Purchase Vibrator	16.0%	< .005	**66.7%**	< .02	27.8%

Table 6: 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 in the privacy condition 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 condition 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 $p < .0001$).[7] For each condition, the total number of purchases made at each level of privacy is depicted in Figure 4.

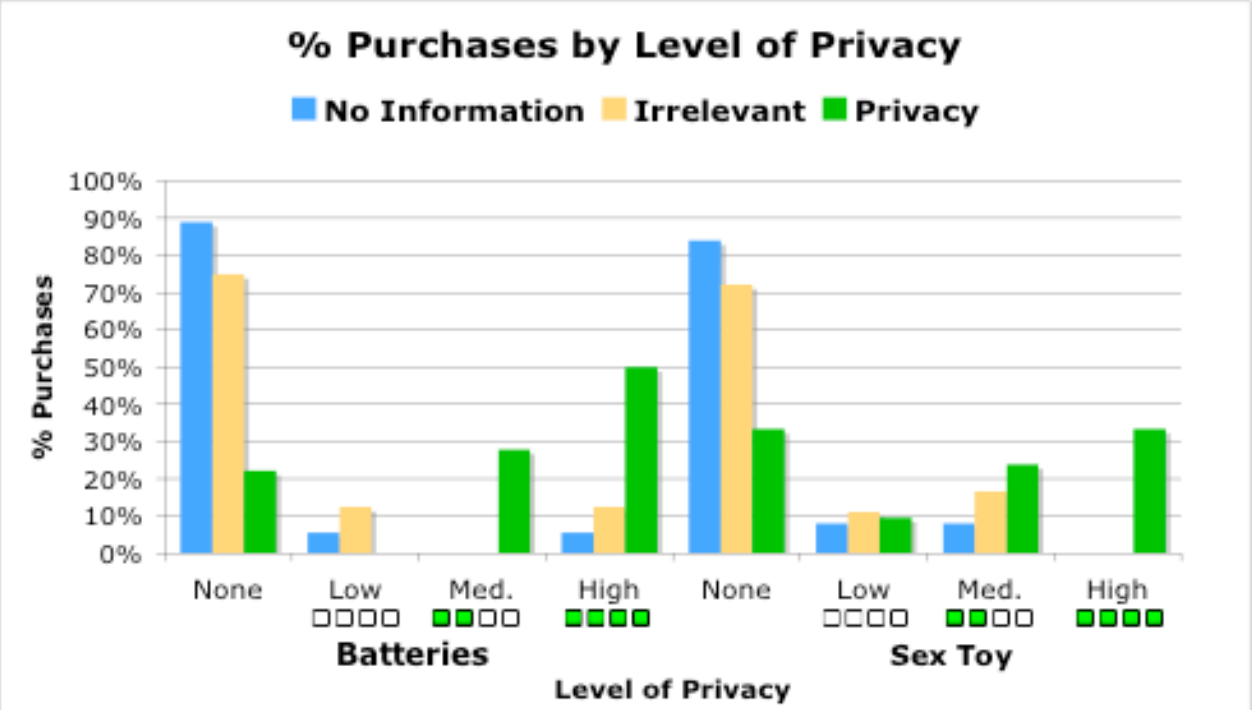


Figure 4: The percentage of purchases made for each product, by level of privacy, for each condition.

Figure 4 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.

4.2 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, we designed this experiment to determine whether or not individuals would be willing to pay a premium for enhanced privacy protections. It is important to note that the goal of the study was *not* to quantify a specific premium for the selected products.[8] When

[7] 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.

[8] An experiment to capture an absolute premium for privacy would need to test a variety of price differentials or make offers to participants based on specific privacy information: "If this website did not

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 Table 7.

Privacy Premium

	Condition 1: No Information	**Condition 2:** Irrelevant Information	**Premium**	***p* Value**
Mean Price - Batteries	$14.64	$14.69	$0.05	0.64
Mean Price - Vibrator	$15.26	$15.30	$0.04	0.65

Table 7: 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.

When comparing the no information condition to the privacy information condition, we found statistically significant privacy premiums for both products, as detailed in Table 8. Note, 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.

Privacy Premium

	Condition 1: No Information	**Condition 3:** Privacy Information	**Premium**	***p* Value**
Mean Price - Batteries	$14.64	$15.23	$0.59	0.0007
Mean Price - Vibrator	$15.26	$15.88	$0.62	0.00005

Table 8: T-test comparison of mean price paid for each product in the no information condition and the privacy information condition.

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

---

sell your email address, would you pay $.10 more, $.50 more, or $1.00 more?" etc.

better privacy policies. This effect was present for purchases of the privacy-sensitive item as well as the non-privacy-sensitive item.

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

Participants in the no information and irrelevant information conditions tended to purchase both items from the least expensive (first) website:[9] 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 who were not shown prominent privacy information were significantly more likely to make their purchases from the cheapest website they encountered. 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.

4.3 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 no information and irrelevant information purchasing patterns, detailed in Table 9. Despite the presence of green boxes, the icon itself was not a decision-making factor for the irrelevant information condition.[10] This implies that our results are not due to the impact of the icons alone but to the privacy signals that the icons carry. Future studies may not need to account for this factor, since icons that users do not understand may not play a significant role in their decision-making process.

[9] The proportions are found by comparing the rank of the website from which the purchase was made in each condition for each product and the whether or not the purchase was made from a site with privacy icon.

[10] In a test of proportions comparing the number of purchases made at sites with privacy icons, when comparing the no information and the irrelevant information conditions, for the batteries, 16% in the no information condition purchased from those sites as compared to 27.8% in the irrelevant information condition, Fisher's exact $p = 0.19$. For vibrator purchases, 11.1% in the no information condition made purchases from those sites compared to 25% in the irrelevant information condition, Fisher's exact $p = 0.21$. For both of the products, the null hypotheses that the proportions are equal cannot be rejected.

Purchases Made between Conditions from Sites Annotated with a Privacy Icon

	Condition 1: No Information	**Condition 2:** Irrelevant Information	**Fisher's Exact *p***
% Purchase Battery	11.11%	25%	0.39
% Purchase Sex Toy	16.0%	27.8%	0.46

Table 9: 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.

4.4 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***

While participants generally indicated that they had more privacy concerns when purchasing the vibrator as compared to the batteries,[11] 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 10. Instead, Figure 5 indicates that there are larger clusters of purchases made at the high privacy sites for both batteries and vibrators.

[11] 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.

Purchases made within each condition from sites annotated with Privacy Icons

	% Purchase Battery	% Purchase Vibrator	McNemar's *p*
Condition 1: No Information	12.5	12.5	1.0
Condition 2: Irrelevant Information	25.0	18.8	1.0
Condition 3: Privacy Information	81.3	62.5	0.38

Table 10: 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.

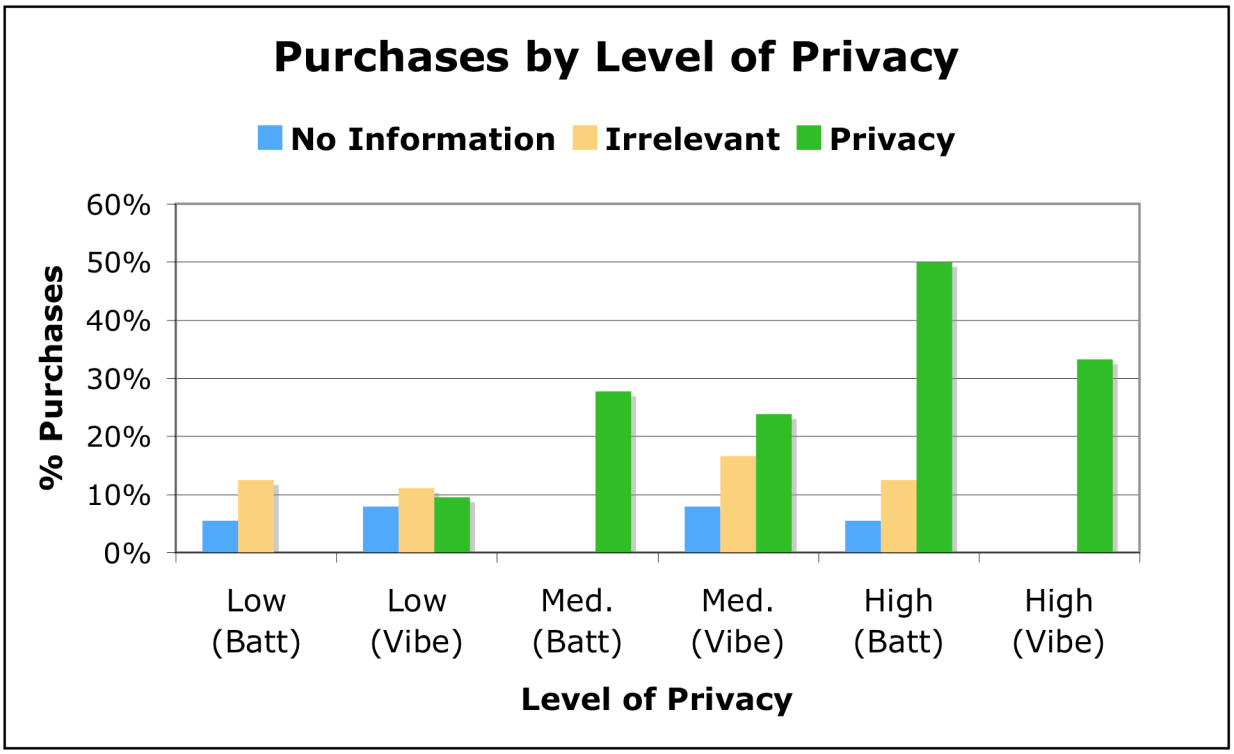


Figure 5: Percentage of purchases made for each product at all the different levels of privacy for each condition.

It is important to note that in the design of the study, there was a smaller premium for privacy with regard to the batteries[12] than with the vibrator,[13] and this may have been a factor in the

[12] In the two sets of results presented to participants the premium for high privacy was $0.54 and $0.69.

[13] In the two sets of results presented to participants the premium for high privacy was $1.18 and $1.46.

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, yet were not willing 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.

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,[14] physical address,[15] and purchase history.[16] 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 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.[17] Similarly, there were no statistically significant correlations between purchasing from sites with privacy icons and gender or age.[18]

4.5 Risk Communication

Overall, Privacy Finder served as an effective means for communicating privacy information. In the "privacy information" condition, 92% noticed the Privacy Icons (95% CI = 74% - 99%), and 32% of participants read the Privacy Reports (95% CI = 15% - 53.5%). In the exit survey 60% of the participants in the privacy condition reported that privacy information influenced the sites they *visited* and the sites from which they *purchased* (95% CI = 38.7% - 78.9%). Additionally, there were no statistical differences between *noticing* the privacy icon and *purchasing* from a website with a displayed privacy icon. This indicates that once privacy information was made available, it led people to purchase from sites that better protect their privacy. This was true for both the batteries and the vibrator.[19]

---

[14] 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.

[15] 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).

[16] 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).

[17] 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 of these products, the null hypothesis that the proportions for each gender are equal cannot be rejected.

[18] The correlations are the following: Age and BatteryPrivacy (β = .33, p = 0.17), Age and VibePrivacy (β = -0.23, p = 0.33), Gender and BatteryPrivacy (β = -0.027, p = 0.91), Gender and VibePrivacy (β = -0.13, p = 0.56). The high p values indicate that these correlations are not statistically significant.

[19] In the privacy condition, when comparing "noticing the privacy icons" and "purchasing batteries from a website with privacy icons," 100% noticed, and 79% purchased, with McNemer's p = .13. This indicates that you cannot reject the null hypothesis that the proportion of participants who noticed the privacy icons is equal to the proportion who purchased the batteries from sites with privacy icons. Similarly, for the vibrator, 90.5% noticed and 66.7% purchased, with McNemar's p = .13, also indicating that the null

When asked, “Which factor had the most influence on your decision?” in the exit survey, participants in the privacy condition, when purchasing batteries, were more likely to write in “privacy” or "privacy policy" (32% vs 0% in the no information condition; Fisher’s Exact p = .001). Since concerns already existed for the privacy-sensitive item, participants in the privacy condition were not significantly more likely to list “Privacy Policy,” with 14.8% in the no information and 36% in the privacy condition listing “Privacy Policy” as their most influential factor, Fisher’s exact p = 0.11. The privacy information provided in Privacy Finder had the effect of heightening privacy awareness for an innocuous item such as batteries.

In the privacy condition, 32% of participants read the Privacy Report (95% CI = 15% - 53.5%). When asked about the number of boxes filled in with green, 48% believed that a site with four boxes adequately protects their privacy (CI = 27.8 - 68.7%), 24% believed a 2-box site adequately protects their privacy (CI = 9.4% - 45.1%), and 56% did not believe that a site with blank boxes adequately protects their privacy (CI = 34.9% - 75.5%). When reading the privacy report, people were most interested in finding out which how their information was going to be used, conditions under which websites may share personal information, and company contact information, followed by the location of the website’s full privacy policy and the list of personal information that is being collected. Other items of interest include links to opt-out of additional communication and how to resolve privacy related disputes.

When purchasing batteries, 73.7 % of participants in the privacy condition felt that the site they purchased from (containing a privacy icon) adequately protects their privacy. Similarly, when purchasing the vibrator, 47.6% in participants in the privacy condition felt that the site they purchased from (containing a privacy icon) adequately protects their privacy.

After purchasing batteries and being shown the privacy report, participants in the privacy condition were more likely to think that the site they purchased from protected their privacy if they purchased from a site with “high privacy” (56.25%) as compared to those who purchased from a “medium privacy” site (31.25%) or a site with no privacy information at all (12.5%), Fisher’s exact p = .01. This indicates that for the batteries, the level of privacy for a particular site did have an impact on whether or not participants felt that their privacy was adequately protected.

Similarly, while not statistically significant (Fisher’s exact p = 0.33), after purchasing the vibrator and being shown the privacy report, participants in the privacy information conditions were also more likely to think that their purchase from a “high privacy” site (41.7%) better protected their privacy as compared to “medium privacy” purchasers (33.3%) and those who purchased from a site without any privacy indicators (16.7%).

These results indicate that once provided with privacy information, people do choose sites that they feel protect their privacy and that there is a perceived difference between sites that offer “high privacy” as compared to the medium and low levels of privacy, as indicated by the privacy icon.

5 Conclusion

The goal of this study was to determine whether the availability and accessibility of privacy information affects individuals’ purchasing decision. 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

---

hypothesis cannot be rejected that these proportions are equal.

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 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 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.

References

Acquisti, A. and Grossklags, J. 2003. Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. *In 2nd Annual Workshop on Economics and Information Security (WEIS '03).*

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

Brown, M. and Muchira, R. 2004. Investigating the Relationship between Internet Privacy Concerns and Online Purchase Behavior. *Journal of Electronic Commerce Research*, vol. 5, n. 1, pp. 62-70, 2004.

Brunk, B. D. 2002. Understanding the privacy space. *First Monday,* v. 7, n. 10. http://firstmonday.org/issues/issue7_10/brunk/index.html.

Brynjolfsson, E., A.A. Dick, and M.D. Smith 2003, Search and Product Differentiation at an Internet Shopbot, MIT Sloan Working Paper No. 4441-03

CBS News. 2005. "Poll: Privacy Rights Under Attack." http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml.

Chellapa, R., and R. G. Sin 2005. "Personalization Versus Privacy: An Empirical Examination of the Online Consumers' Dilemma". Information Technology and Management. Volume 6, No. 2-3. pp 181-202.

Cranor, L. 2002. *Web Privacy with P3P*. O'Reilly & Associates, Sebastopol, CA.

Cranor, L., Guduru, P., and Arjula, M. 2006. User Interfaces for Privacy Agents. *ACM Transactions on Computer-Human Interaction* 13(2), June 2006.

Gideon J., Egelman, S.,Cranor, L., and Acquisti. A. 2006. Power Strips, Prophylactics, and Privacy, Oh My! In *Proceedings of the 2006 Symposium On Usable Privacy and Security*, 12-14 July 2006, Pittsburgh, PA. http://cups.cs.cmu.edu/soups/2006/proceedings/p133_gideon.pdf

Harris Interactive. 2001. "Privacy On & Off the Internet: What Consumers Want." Tech report. http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf.

Hochhauser, M. 2003. Why Patients Won't Understand Their HIPAA Notices. Privacy Rights Clearinghouse. http://www.privacyrights.org/ar/HIPAA-Readability.htm.

Hui,K. L., Teo, H.H., and Lee, T. S.Y. 2006. The Value of Privacy Assurance: A Field Experiment, mimeo.

Jensen, C., and Potts, C. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. *Proceedings of the SIGCHI conference on Human Factors in Computing systems*, Vienna Austria, p. 471-478.

Jensen, C., Potts, C. and Jensen, C. 2005. Privacy Practices of Internet Users: Self-reports versus Observed Behavior. *International Journal of Human-Computer Studies,* v. 63, pp 203 – 227.

Malhotra, N., Kim, S. S., and Agarwal, J. 2004. Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research,* vol. 15, n. 4, pp. 336-355.

Milne, G.R. and Culnan, M.J. 2002. Using the Content of Online Privacy Notices to Inform Public Policy: A Longitudinal Analysis of the 1998-2002 U.S. Web Surveys. *The Information Society* (18), 5 (October 2002), 345-359.

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

Morgan, M. G., Fischhoff B., Bostrom, A., and Atman, C. 2001. *Risk Communication: A Mental Models Approach*. Cambridge University Press: New York.

Privacy & American Business (P&AB). 2005. "New Survey Reports an Increase in ID Theft and Decrease in Consumer Confidence." Conducted by Harris Interactive, May 2005. http://www.pandab.org/deloitteidsurveypr.html.

Privacy Leadership Initiative. 2001. "Privacy Notices Research Final Results." Conducted by Harris Interactive, December 2001. http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf.

Rose, E. 2005. Data Users versus Data Subjects: Are Consumers Willing to Pay for Property Rights to Personal Information? In *Proceedings of the 38th Hawaii International Conference on System Sciences*.

Shostack, A. 2003. Paying for privacy: Consumers and infrastructures. In *2nd Annual Workshop on Economics and Information Security (WEIS '03)*.

Smith, H. J., Milberg, S., and Burke, S. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly,* vol. 20, n. 2, pp. 167-196, 1996.

Spiekermann, A. Grossklags, J. and Berendt, B. 2001. E-privacy in 2nd generation e-commerce: Privacy preferences versus actual behavior. In *Proceedings of the ACM Conference on Electronic Commerce (EC '01)*, pages 38–47.

Syverson, P. 2003. The paradoxical value of privacy. In *2nd Annual Workshop on Economics and Information Security (WEIS '03)*.

Tedeschi, B. 2002. Everybody talks about online privacy, but few do anything about it. *New York Times*, June 3, 2002, Section C , Page 6 , Column 1.

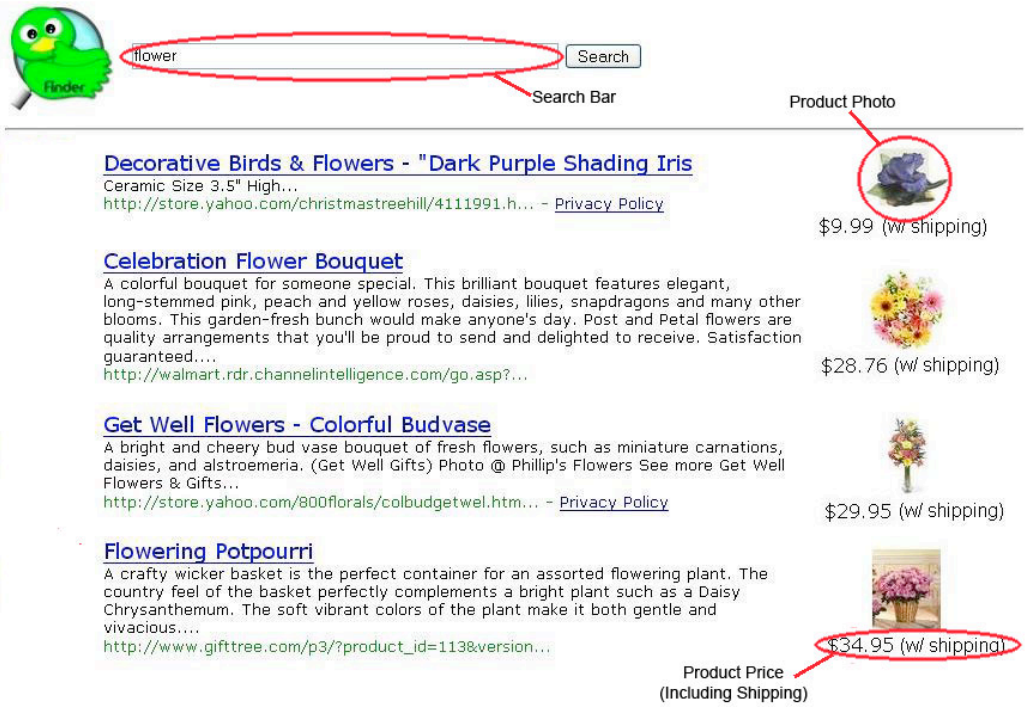
TRUSTe. 2006. "Consumers have a false sense of security about online privacy – Actions inconsistent with Attitudes." Conducted by TNS, December 2006. http://www.truste.org/about/press_release/12_06_06.php.

Turow, J., Feldman, L., and Meltzer, K. 2005. "Open to Exploitation: American Shoppers Online and Offline." A Report from the Annenberg Public Policy Center of the University of Pennsylvania.

Appendix A: Search Engine Keys

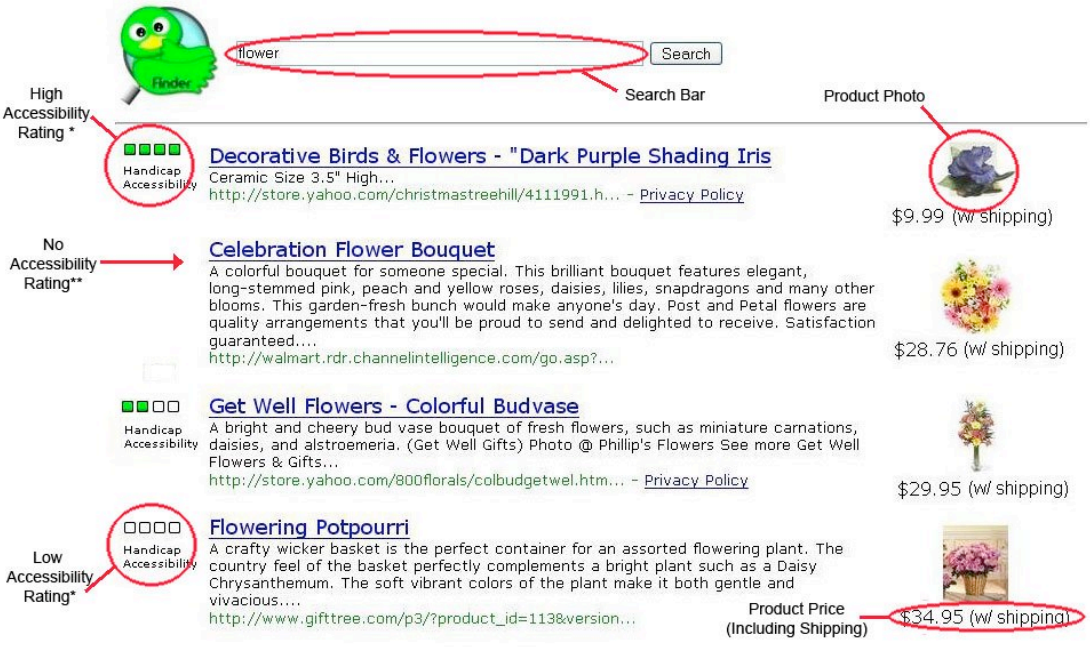
Condition 1: No Information

Search Engine Page Description



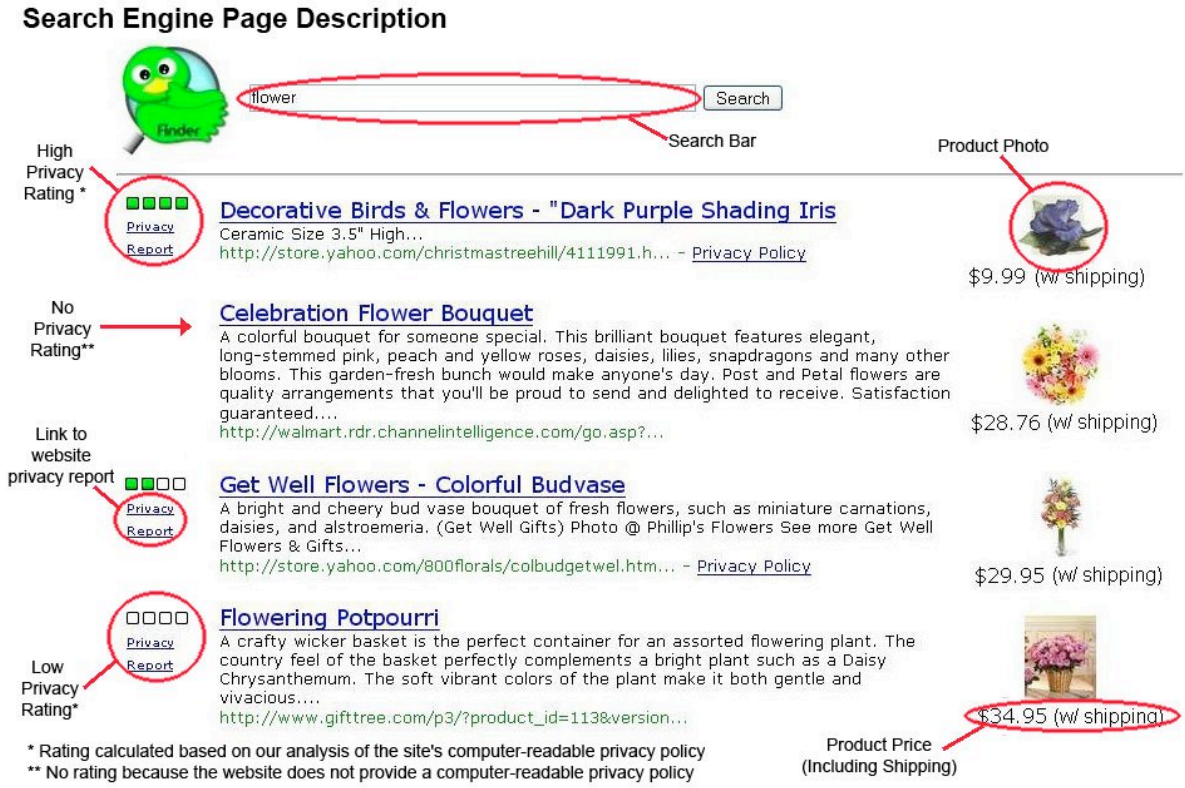
Condition 2: Handicap Accessibility Information

Search Engine Page Description



* Rating calculated based on our analysis of the site's computer-readable accessibility information for vision-impaired users
** No rating because the website does not provide computer-readable accessibility information for vision-impaired users

Condition 3: Privacy Information



Appendix B: Experiment Instructions

Each part was given one at a time on a separate piece of paper. The order of the purchase tasks was randomly assigned (Parts 4 and 6). Below are the instructions where the participant has been assigned the batteries first.

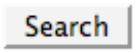
Parts 1, 2, and 5 used the general Privacy Finder search engine. Parts 3, 4, and 6 used the Privacy Finder shopping engine.

Part 1: Carnegie Libraries

1. Double-click the  Firefox icon to launch the web browser. The webpage that appears should display the *Finder* search engine.
2. User the search engine to answer the following question:
   How many "Carnegie libraries" are there in the world?

   _____
3. Raise your hand to notify the experiment administrator when you have finished Part 1.

Part 2: Ugg Boots

1. Search for **Ugg Boots** in the search bar and click 

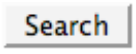
.
2. Browse the results, and list 3 colors that are available for Women's Ugg Boots.

   _____

   _____

   _____
3. Raise your hand to notify the experiment administrator when you have finished Part 2.

Part 3: Black Ugg Boots

1. Search for **Ugg Boots** in the search bar and click 

.
2. Browse the results, and answer the following question:
   What is the lowest price for Women's Black Ugg Boots?

   _____
3. Raise your hand to notify the experiment administrator when you have finished Part 3.

Part 4: Duracell AA Batteries

1. Search for batteries.

   Type **Duracell AA batteries 8-pack** in the search bar and click Search.

2. Browse the results and select a website from which to purchase the product. Follow the directions given on the website to make the purchase. Have your credit card information and shipping address on hand to complete your purchase.

   If you do not wish to keep the item, please use the following address as the shipping address:

   <*Your Name Here*>
   c/o CyLab CUPS Laboratory
   4720 Forbes Ave. Room 2207
   Pittsburgh, PA 15213

3. After you complete your purchase, please record the following information:

   Name of website:_____

   Website Address (URL):_____

   Total price of product (including fees/shipping): $_____

4. Raise your hand to notify the experiment administrator when you have *the purchase confirmation* page or *receipt* displayed so that they can print the purchase information for your records.

Part 5: Computer recycling

1. Use the search engine to answer the following question:

   Where can you drop off your computer in Pittsburgh to have it recycled?

   _____

2. Raise your hand to notify the experiment administrator when you have finished Part 5.

Part 6: Pocket Rocket Jr.

1. Search for a vibrating sex toy.

   Type **Pocket Rocket Jr. Red** in the search bar and click Search.

2. Browse the results and select a website from which to purchase the product. Follow the directions given on the website to make the purchase. Have your credit card information and shipping address on hand to complete your purchase.

   If you do not wish to keep the item, please use the following address as the shipping address:

   <Your Name Here>
   c/o CyLab CUPS Laboratory
   4720 Forbes Ave. Room 2207
   Pittsburgh, PA 15213

3. After you complete your purchase, please record the following information:

   Name of website:_____

   Website Address (URL):_____

   Total price of product (including fees/shipping): $_____

4. Raise your hand to notify the experiment administrator when you have *the purchase confirmation* page or *receipt* displayed so that they can print the purchase information for your records.

Appendix C: 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. The "Premium for High Privacy" is the difference between the fourth result with "high privacy" and the first result.

Non-Privacy Sensitive Item

Duracell AA Batteries – 8 Pack

Session 1:

URL	Price with Shipping	Difference	Privacy Level	Privacy Icon
DiscountOfficeItems	$14.60	$0.00	N/A	
InstaOffice	$14.96	$0.36	Low	☐☐☐☐
Efunctional	$15.07	$0.11	Medium	■■☐☐
OfficeQuarters	$15.14	$0.07	High	■■■■
LowCostBatteries	$15.85	$0.71	N/A	
NexImaging	$15.98	$0.13	Medium	■■☐☐
Cybergift Center	$16.42	$0.44	High	■■■■
Emartinc	$16.85	$0.43	N/A	

Premium for High Privacy **$0.54** **3.7%**

Session 2:

URL	Price with Shipping	Difference	Privacy Level	Privacy Icon
CCV Software	$14.45	$0.00	N/A	
DiscountOfficeItems	$14.60	$0.15	Low	☐☐☐☐
InstaWares	$14.80	$0.20	Medium	■■☐☐
OfficeQuarters	$15.14	$0.34	High	■■■■
LowCostBatteries	$15.85	$0.71	N/A	
NexImaging	$15.98	$0.13	Medium	■■☐☐
Cybergift Center	$16.42	$0.44	High	■■■■
Emartinc	$16.85	$0.43	N/A	

Premium for High Privacy **$0.69** **4.8%**

Privacy Sensitive Item

Pocket Rocket Jr.

Session 1:

URL	Price with Shipping	Difference	Privacy Level	Privacy Icon
Sensual Universe	$15.08	$0.00	N/A	
PinkPecker	$15.74	$0.66	Low	☐☐☐☐
AdamandEve	$15.90	$0.16	Med	■■☐☐
AdultDVDExplorer	$16.54	$0.64	High	■■■■
Desired-Pleasures	$16.79	$0.25	N/A	
PassionBunny	$16.79	$0.89	N/A	
VitaMaker	$17.94	$1.15	Low	☐☐☐☐
SheVibe	$18.95	$2.16	High	■■■■

Premium for High Privacy **$1.46** **9.7%**

Session 2:

URL	Price with Shipping	Difference	Privacy Level	Privacy Icon
FindaPleasure	$15.36	$0.00	N/A	
PinkPecker	$15.74	$0.38	Low	☐☐☐☐
AdamandEve	$15.90	$0.16	Med	■■☐☐
AdultDVDExplorer	$16.54	$0.64	High	■■■■
Desired-Pleasures	$16.79	$0.25	N/A	
PassionBunny	$16.79	$0.89	N/A	
VitaMaker	$17.94	$1.15	Low	☐☐☐☐
SheVibe	$18.95	$2.16	High	■■■■

Premium for High Privacy **$1.18** **7.7%**

Appendix D: Search Results Interfaces

Condition 1: No Information

Duracell AA batteries 8-pack Search

Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.html?record@56119

$14.45 (w/shipping)

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovy.com/product/DURMN15RT12Z

$14.60 (w/shipping)

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Bat...

$14.80 (w/shipping)

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500B8...

$15.14 (w/shipping)

Condition 2: Handicap Accessibility Information

Duracell AA batteries 8-pack Search

Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.html?record@56119

$14.45 (w/shipping)

Handicap Accessibility

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovy.com/product/DURMN15RT12Z

$14.60 (w/shipping)

Handicap Accessibility

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Batt...

$14.80 (w/shipping)

Handicap Accessibility

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500B8...

$15.14 (w/shipping)

Condition 3: Privacy Information