

# Studying the Impact of Privacy Information on Online Purchase Decisions

**Serge Egelman**  
Carnegie Mellon University  
egelman@cs.cmu.edu

**Janice Tsai**  
Carnegie Mellon University  
jytsai@andrew.cmu.edu

**Lorrie Faith Cranor**  
Carnegie Mellon University  
lorrie@cs.cmu.edu

**Alessandro Acquisti**  
Carnegie Mellon University  
acquisti@cmu.edu

## ABSTRACT

Search engines play an important role in helping users find desired content. With the increasing deployment of computer-readable privacy policies encoded using the standard W3C Platform for Privacy Preferences (P3P) format, search engines also have the potential to help users identify web sites that match their privacy preferences. We implemented a “privacy-enhanced” search engine to aid users in choosing web sites that meet their privacy needs. While we conducted a study to determine the rate of P3P adoption and whether or not most searches yield multiple P3P-enabled web sites, we now wish to conduct user studies. User studies may help establish whether or not the tool is intuitive, and whether or not users actually care about web site privacy practices. In this paper, we outline our motivation and methodology for these studies. Specifically, we plan on conducting at least three different user studies to determine whether users care about privacy when making shopping decisions, what aspects of privacy they care most about, and whether or not our service intuitively addresses these privacy concerns.

## INTRODUCTION

Numerous studies have found that Internet users are concerned about online privacy and are worried about what e-commerce web sites might do with their personal data [8, 12]. However, few users make the necessary effort to read privacy policies [16], let alone seek out the web sites that have the best privacy policies. One explanation for this disparity between what consumers say and what they do may be the presentation of privacy information in privacy policies, as privacy policies are difficult and time consuming to read and understand [13, 14, 2]. A variety of online price comparison services makes it easy for users to identify e-commerce sites offering a particular product at the lowest prices. However, prior to Privacy Finder, [4] no such search engine existed to compare sites based on privacy preferences.

Extending work begun at AT&T Labs [6], we created the Privacy Finder service and made it available to the public in Summer 2005 to address this lack of privacy comparison information. Privacy Finder is a privacy-enhanced search engine that looks for machine-readable privacy policies formatted using the Platform for Privacy Preferences (P3P) standard. P3P specifies a common XML format for creating machine-readable privacy policies. Privacy Finder allows a user to conduct a search using either the Google or Yahoo! search engines and then to view annotated results based on whether or not each site complies with the user’s stated privacy preferences. Privacy preferences are entered alongside the search terms; the user has a choice between “high,” “medium,” “low,” or custom settings. The three preset settings are based on the three presets available in the Privacy Bird P3P user-agent program [3]. The custom setting is entered by answering twelve yes or no questions; it is then saved for each user as a cookie.

Upon receiving a list of search results from the search API selected, Privacy Finder attempts to locate a P3P policy on each web site. When a policy is found, it is evaluated against the user’s preferences. Sites that comply with the user’s preferences are displayed at the top of the list of search results, and sites that do not comply are displayed next. Sites that do not publish P3P policies are displayed at the bottom of the list. In addition to displaying privacy preference compliance information, Privacy Finder also allows users to view web site privacy policies without having to first view the site. The P3P metadata allows us to translate the XML tags back into natural language, thus allowing the user to view privacy policies that are both easy to read and use a consistent vocabulary.

We have recently begun studying the usability and usefulness of the Privacy Finder service and its impact on online purchasing decisions. The first study that we conducted determined whether or not a sufficient number of sites have implemented P3P to make searches yield useful results. We hypothesize that users will be more likely to take advantage of privacy information if it is intuitive and made readily available to them. Now, we wish to determine how useful this service is from the user’s perspective.

## SEARCH STUDY RESULT

In 2005, we completed a study on the rate of P3P adoption with regard to search engine results [10]. Internet users regularly use search engines to find web sites, and previous studies examining the P3P adoption rates for “popular” or industry-specific web sites tell us little about P3P adoption rates for this common scenario. Thus, working with AOL, we conducted search queries using a list of 20,000 “typical” search terms. These search terms were randomly selected from a week-long log of actual queries. Each term was entered into Google, Yahoo!, and the AOL search engine, and the first twenty results were examined.

Overall, we found that just over 10% of all web sites found by using the typical search terms were P3P-enabled. However, when using “e-commerce” search terms, we found that roughly 22% of the search results were P3P-enabled. Additionally, 15% of all searches yielded at least two web sites among the first ten results that complied with the “low” preference setting. This implies that while the overall P3P adoption rate is still low, common search engine queries still yield multiple P3P-enabled web site, allowing users to make choices with regard to their privacy preferences.

## RESEARCH PLAN

### Communicating Privacy Information

Numerous studies have showed that privacy is consistently at the top of Internet users’ concerns [5, 12, 16, 18, 11]. At the same time, these concerns are not reflected by most users’ behaviors [17, 1]. Web site privacy policies often provide incomplete information and are written above the reading level of most users, leaving users unable to determine the risks of providing personal information [19, 9, 1]. In addition, various psychological distortions, including the value of immediate gratification, may lead people to act against their own best interests [1]. We believe that Privacy Finder can address the problems related to privacy information by making this information both easier to locate and easier to comprehend.

The privacy policy summary provided by the current version of our P3P-enhanced search tool is based directly on the policy summary provided by Privacy Bird. It includes a brief English language translation of most of the XML tokens contained in a P3P policy, formatted as a set of bold headings and short bulleted lists. Buttons are provided to allow users to hide or reveal the bulleted lists. Based on our Privacy Bird studies [7], we believe the policy summary display can be further improved by highlighting the privacy information that is most likely to be relevant. We suspect that users will be most interested in knowing about the extent that their personal information may be shared, and whether or not the site they are visiting is going to send them unwanted communications. However, further work is needed to better understand users needs and to develop a privacy policy summary that best addresses these needs. Before this can happen, we need to determine whether or not users will take advantage of this added information, as well as the best way of conveying it.

## User Studies

We propose to conduct a series of studies to refine the P3P-enhanced search policy summary display and configuration interface, and then we will evaluate the influence of privacy information on e-commerce behaviors. We will begin by conducting a survey of Internet users aimed at determining which privacy-related risks they are most concerned about, which threats they believe to be the most credible, and what information they find to be the most useful in a P3P policy. Based on our survey results, we will refine our user interfaces and conduct additional user studies, consisting of economic experiments in which subjects will select a real web site from which to make a real purchase given behavior incentives in the form of money or discounts on items the subjects had planned to purchase. We would like to compare the effects of providing this information through a browser-based P3P user agent such as Privacy Bird, through our P3P-enhanced search tool Privacy Finder, and through a P3P-enhanced price comparison tool (e.g. using Privacy Finder to create a service similar to Google’s Froogle service). We would also like to examine the situation where users are motivated to find the cheapest price when price is not an issue (perhaps because the price does not actually vary very much). Our hypothesis is that use of a P3P user agent will have some influence on purchasing decisions, while use of a P3P-enhanced search tool or price comparison tool will have a larger influence. In price-sensitive situations, we expect that privacy information will have less of an influence on purchase decisions, and that the P3P-enhanced price comparison tool will prove to be the most useful. We describe a possible progression of studies. Depending on the outcome of the early studies, we may alter subsequent studies or introduce additional studies.

### *Influencing Purchasing with Privacy Information*

Our first study will be designed for 40 subjects in each of eight conditions. Subjects in each condition will be asked to purchase an item using a web browser and one of the three privacy tools described above, or with no privacy tool. In addition, half the subjects will be given a purchasing task that is not sensitive to price, and the other half will be given a price-sensitive task. For the price-insensitive task, we will fully reimburse subjects for the cost of the item they purchase, so that they have no incentives to purchase the item from the least expensive vendor. For the price-sensitive task, we will design the study so that the subjects have incentives to save money. We will either reimburse them only partially for the item they purchase, or reimburse them fully and offer a bonus payment for saving money. For example, we may offer to reimburse subjects for the full price of the item up to \$30, and let them keep any left over money. Subjects will use their own credit cards and provide their own personal information to the web sites where they make the purchases. We will ask subjects to compare three web sites before making their purchase.

In selecting the item for subjects to purchase, we will find an item that generally costs less than \$30, making sure that it is readily available from multiple web sites that have a variety of P3P-defined privacy policies. For example, books

are available from several vendors, such as Barnes & Noble, which has a P3P-enabled privacy policy, and Amazon.com, which does not. But, one potential difficulty with having subjects purchase books is that many individuals frequently buy books online and have a favorite bookstore. Whatever item we select, we will have to account for the fact that when subjects already have a preferred vendor, they are likely to continue making purchases from that vendor because they have already setup an account with that vendor and presumably find them trustworthy and reliable.

We will survey subjects about their previous e-commerce shopping experiences to control for other factors such as prior experience doing business with a particular web site. Additionally, after the subjects have made their purchases, we will ask them to explain the reason they selected a particular web site to make their purchase. We will also ask them to review the privacy policies at each of the three web sites they compared and evaluate how satisfactory they find the privacy practices. Finally, we will ask them to evaluate the usefulness and ease-of-use of the privacy tool that they used.

#### *Privacy-Sensitive Purchasing Decisions*

In our second study, we propose to investigate the extent to which the availability of privacy-related information influences privacy-sensitive online purchasing decisions. In typical online shopping experiences, shoppers may have concerns about exposing their contact and payment information, but many shoppers may not be particularly concerned about exposing their transaction history. We would like to create a situation in which subjects are likely to be concerned about the privacy of their transaction history, but have tools readily available that will enable them to easily discover vendors who promise to protect their privacy. Our hypothesis is that in this “best case scenario” we should see privacy information playing a greater role in purchasing decisions than in scenarios where shoppers are less concerned about the privacy of their transaction history or in situations when subjects do not have privacy-related information readily available to them.

Our second study will be designed for 40 subjects in each of two conditions. Subjects in each condition will be asked to purchase an item that is likely to raise privacy concerns. One set of subjects will make their purchase without the benefit of a privacy information tool. The other set of subjects will use Privacy Finder (or perhaps one of the other P3P tools, depending on the results of the previous study). As in the previous study, subjects will use their own credit cards and be asked to compare three sites before making a purchase. Subjects will be reimbursed for their purchase. Depending on the results of the previous study, we may design this as a price-sensitive or price-insensitive task. We will select an item for purchase that is legal for our subjects to purchase, but may make them feel uncomfortable. For example, subjects might purchase condoms, or a book about recovering from alcohol addiction. Since these are items that the subjects may not necessarily want to have, we will have the subjects make the purchases on our behalf and have the items shipped to our laboratory (although they will still use their

credit cards and provide their own names and billing addresses). We will donate the items to an appropriate organization if possible. To determine what items are most likely to raise privacy concerns, we will include some questions about privacy concerns associated with specific purchases on our panel survey in the earlier phase of this project. We will use a screening questionnaire to select subjects who indicate that purchasing these items would raise privacy concerns.

#### *Valuation of Privacy*

In our third study, we will investigate the value people place on privacy in an e-commerce environment. This study will extend the previous study by investigating whether different degrees of privacy protection (reported in the merchants online privacy policies) will affect subjects price sensitivity and purchasing decisions. As in the previous study, we would like to create a situation in which subjects are likely to be concerned about the privacy of their transaction history, but have different choices or incentives regarding where to purchase a certain item. The different choices reflect not just different merchants, but merchants with different privacy policies. For this goal, we may emphasize the role of the policy summaries that are displayed by Privacy Finder. At the same time, we will vary the incentives the subjects may be receiving from transactions from different merchants. Our hypothesis is that subjects may tend to assign low values to privacy protection (versus economic benefits) in the scenario in which no tool to filter policy information is offered (by always opting for the cheaper offer, regardless of the merchants privacy policies differences); however, when a tool is used, subjects may display decreased price sensitivity and increased sensitivity to privacy.

This study will be designed for 40 subjects in each of six conditions, based on a  $2 \times 3$  matrix of two instruments. The first instrument has two conditions: the presence or absence of a tool enabling the communication of privacy policy information. One set of subjects will make their purchase without the benefit of a privacy information tool. The other set of subjects will use Privacy Finder. The second instrument is the incentive provided to the study participants to purchase the good from one merchant versus the another, and has three conditions. Under the first condition, subjects will simply be reimbursed for the purchase they make they will not receive additional benefits (on top of the show-up fee). This implies that they will receive the same amount independently of the merchant from which they decide to purchase the good. In the second condition, the subjects will be offered various bonus payments for purchasing from various merchants. The size of the bonus offered will be inversely proportional to the merchants privacy ranking, calculated on the basis of the subjects revealed preferences. For example, a subject may receive a benefit of  $\$x$  to purchase the good from the merchant that most closely matches her privacy preference,  $\$y$  to purchase the good from a merchant that does not closely match her privacy preference but is not the most distant from them, and up to a maximum of  $\$z$  (with  $x < y < z$ ) for the merchant that least closely matches her privacy preference. The third condition is like the second, only that all payment bonuses will be proportionally larger by a factor  $c$ , ranging

from  $\$cx$  to  $\$cz$ . (A variation of this instrument that we will also consider, inspired by the contingent-valuation methodology [15], would involve randomizing the benefits offered across all subjects participants by discrete increments, from \$0 to a vector of amounts  $w$ , each vector embodying different bonuses inversely proportional to the merchants privacy ranking for each subject.)

The goal of this study is to gain more granular information (rather than binary data, as in purchase or not purchase) about subjects sensitivity to different benefits (expressed as the varying benefits we will offer) for the same good, versus different privacy policies by the different merchants.

## CONCLUSION

Privacy concerns are prevalent among users' current apprehensions about using the Internet for making purchases. While tools are available to make certain aspects of Internet shopping easier (e.g. comparing prices across various vendors), no tools are in widespread usage for evaluating vendors' privacy practices. For such privacy-enhancing tools to become successful, studies need to be conducted to better determine and analyze users' privacy concerns. We believe that through the users studies that we have just described, we can gain a better understanding of user's attitudes towards privacy when making purchasing decisions. Additionally, these studies will also yield information about the utility of Privacy Finder and P3P in general.

## REFERENCES

1. A. Acquisti. Privacy in electronic commerce and the economics of immediate gratification. In *ACM Electronic Commerce Conference (EC '04)*, pages 21–29, New York, NY, 2004. ACM Press.
2. A. Anton, J. Earp, M. Vail, N. Jain, C. Gheen, and J. Frink. An analysis of web site privacy policy evolution. Technical Report TR-2004-21, North Carolina State University, 2004.  
[http://www.theprivacyplace.org/papers/hipaa\\_7\\_24\\_submit.pdf](http://www.theprivacyplace.org/papers/hipaa_7_24_submit.pdf).
3. Carnegie Mellon University. Privacy Bird, 2005.  
<http://www.privacybird.com/>.
4. Carnegie Mellon University. Privacy Finder, 2005.  
<http://search.privacybird.com/>.
5. CBS News. Poll: Privacy rights under attack. *CBS News*, October 2, 2005.  
<http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml>.
6. L. F. Cranor, S. Byers, D. Kormann, and P. McDaniel. Searching for Privacy: Design and Implementation of a P3P-Enabled Search Engine. In *Proceedings of the 2004 Workshop on Privacy Enhancing Technologies (PET2004)*, May 26-26, 2004.
7. L. F. Cranor, P. Guduru, and M. Arjula. User interface for privacy agents. *ACM Transactions on Computer-Human Interaction*, 2006.
8. L. F. Cranor, J. Reagle, and M. S. Ackerman. Beyond concern: Understanding net users' attitudes about online privacy. *AT&T Labs-Research Technical Report TR 99.4.3*, 14 April 1999.  
<http://www.research.att.com/resources/trs/TRs/99/99.4/99.4.3/report.htm>.
9. M. J. Culnan and G. R. Milne. The Culnan-Milne survey on consumers and online privacy notices, 2001.  
[http://intra.som.umass.edu/georgemilne/pdf\\_files/culnan-milne.pdf](http://intra.som.umass.edu/georgemilne/pdf_files/culnan-milne.pdf).
10. S. Egelman, L. F. Cranor, and A. Chowdhury. An analysis of P3P-enabled web sites among Top 20 search results (under review). November 2005.  
<http://lorrie.cranor.org/pubs/www06.html>.
11. S. Fox, L. Rainie, J. Horrigan, A. Lenhart, T. Spooner, and C. Carter. Trust and privacy online: Why Americans want to rewrite the rules. August 20, 2000.  
[http://www.pewinternet.org/pdfs/PIP\\_Trust\\_Privacy\\_Report.pdf](http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf).
12. Harris Interactive. A survey of consumer privacy attitudes and behaviors, 2001.  
<http://www.bbbonline.org/UnderstandingPrivacy/library/harrissummary.pdf>.
13. M. Hochhauser. Why patients won't understand their HIPAA notices. 2003.  
<http://www.privacyrights.org/ar/HIPAA-Readability.htm>.
14. C. Jensen and C. Potts. Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pages 471–478, Vienna, Austria, 2004.
15. R. C. Mitchell and R. T. Carson. *Using Surveys to Value Public Goods: The Contingent-Valuation Method*. Resource for the Future, Washington, D.C., 1st edition, 1989.
16. Privacy Leadership Initiative. Privacy notices research final results, December 2001.  
<http://www.ftc.gov/bcp/workshops/glb/supporting/harris%20results.pdf>.
17. S. Spiekermann, J. Grossklags, and B. Berendt. E-privacy in 2nd generation E-Commerce: Privacy preferences versus actual behavior. *ACM Conference on Electronic Commerce - EC '01*, pages 38–47, 2002.
18. H. Taylor. Most People are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits. 17, 2003.  
[http://www.harrisinteractive.com/harris\\_poll/index.asp?PID=365](http://www.harrisinteractive.com/harris_poll/index.asp?PID=365).
19. J. Turow. Americans and online privacy: The system is broken, 2003.  
<http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf>.