The Impact of Salient Privacy Information on Decision-Making

Submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Engineering and Public Policy

Janice Y. Tsai

B.S., Mathematical Methods in the Social Sciences, Northwestern University
M.L.I.S., School of Communication and Information, Rutgers
M.S., Engineering and Public Policy, Carnegie Mellon University

Carnegie Mellon University
Pittsburgh, PA

December 2009

Thesis Committee:

Lorrie F. Cranor, Chair

Alessandro Acquisti

Baruch Fischhoff

Jason Hong

Peter Swire

Keywords: Privacy, Online Privacy, Mobile-Location Privacy, Technology Adoption, Behavioral Economics

To grandparents
and to my husband Richard W. Sharp III, without whom this would not have been possible.

Acknowledgments

I recently took a trip to Taiwan to visit my grandparents. At their apartment, my grandfather proudly displayed the bookshelf of the theses of his children and grandchildren. The value that my parents and grandparents placed on education makes it possible for me to complete my PhD today.

I was drawn to the Department of Engineering and Public Policy because the person who would become my advisor, Lorrie Cranor, took the time to thoughtfully answer my email inquiry about graduate studies at Carnegie Mellon. I am thankful for her willingness to always make time for her students. She has been a truly inspirational advisor, and has helped me to transform as a researcher. Her support and encouragement enabled me to pursue and complete my PhD.

I am privileged to be a member of the Department of Engineering and Public Policy. Granger Morgan has created a program whose alumni change the world. I thank him for his vision as well as Patti Steranchak, Vicki Finney, and Barbara Bugosh who make EPP thrive. I would especially like to mention Patrick Wagstrom, whose advice continues to be useful and wise; and Jenny Logue for her encouragement.

No one could wish for better collaborators than those found in the CUPS Laboratory. I thank Alessandro Acquisti for his intellectual input: our discussions have been essential in my involvement in the areas of behavioral economics and privacy. Serge Egelman was an instrumental partner in our Privacy Finder research. Patrick Gage Kelley has been a good friend and provided insightful comments on my work. I have appreciated the camaraderie provided by Steve Sheng and Aleecia McDonald, my fellow CUPS Lab EPP students. I would also like to recognize Julie Downs and Mandy Holbrook for their advice and expertise in survey design and analysis, Ponnurangam Kumaraguru for his attention and feedback in presentations, and Jennifer Lucas for her administrative knowledge and ability to get things done at Carnegie Mellon.

I would like to thank the CMU Mobile Commerce Lab and Norman Sadeh for his leadership of the group; Jason Hong for his input related to location-sharing, privacy, and HCI; and Paul Hankes Drielsma and Eran Toch for their insights and conversations regarding feedback and expressiveness.

My friends have contributed a significant amount to my life. I would like to thank Scott Craver for being my inspiration to make a difference in the arena of technology policy, Kate and Pat Zimmerman for their enthusiasm, and Eugene Cheung for always listening.

Finally, this work is funded in party by the National Science Foundation under Cyber Trust grant CNS-0627513 and by the Army Research Office contract no. DAAD19-02-1-0389 to Carnegie Mellon University's CyLab.

Abstract

People value their privacy; however, they typically do not make the protection of their privacy a priority. Privacy is oftentimes not tangible, complicating the efforts of technology users to express and act according to their privacy needs. Additionally, people may not be fully aware of the risks they are subjecting themselves to once they use the Internet for financial transactions, or create profiles on online social networks. Companies post privacy policies inform people about their informational practices; but, this information is extremely difficult to use and typically not considered in users' decision-making processes.

Privacy concerns have also had an impact on users' adoption of new technologies that share personal information. A plethora of mobile location-finding technologies applications have become available over the last two decades, but the products and services offered by the technology developers may not comprehensively address the privacy implications and privacy concerns surrounding their use. The design considerations for these products may not provide the necessarily amount of control or risk mitigation for users to ensure that their location information is not misused.

In this thesis, I focus on the impact of salient privacy information on privacy concerns and behavior in two contexts: online shopping and the use of a mobile-location sharing technology. I examine several case studies focusing on the evolution of privacy attitudes after people use specific technologies. Based on the examination of the use of a location-sharing system, I highlight several design considerations for mobile-location application developers to ensure they address their usersÕ privacy concerns. I use the results of online surveys and user studies to provide concrete information on the impact of feedback on the comfort with using location-sharing technology. This research shows that users will pay a premium to purchase from websites that offer better privacy policies IF that privacy information is made visible and understandable. This research points to the importance of control in the management of privacy concerns. Whether it be mandated by legislation, or recommended in industry standards or design standards, offering users control in the form of understandable privacy policy information, or control over the disclosure of personal information by technology, is essential.

Contents

List of Figures

List of Tables

Part I

Overview

Chapter 1

Introduction

Privacy concerns can have a significant impact on technology and policy. The adoption of a new technology often depends on how much the new technology pushes or changes social norms, how comfortable people are with these changes, and the context of use for the technology. For example, people have become alarmed when radio frequency identification tags (RFID) are used to track goods and purchases [80, 88]; but when global positioning (GPS) location tracking in cellular phones is proposed for children (for example, by Disney), it has received a much warmer reception [78]. Even policy changes with regard to existing technologies can generate ire. The outrage over changes to a social networking site's Terms of Service (Facebook) which seemed to give ownership of users' photos to the site forced the site to revert to its previous policies [106].

People value their privacy; however, they typically do not make the protection of their privacy a high priority. Privacy, is intangible, complicating the efforts of technology users to express and act according to their privacy needs. Additionally, people may not be fully aware of the risks they are subjecting themselves to once they use the Internet for financial transactions, or create profiles on online social networks. Companies post privacy policies inform people about their informational practices; but, this information is extremely difficult to use and typically not considered in users' decision-making processes.

Privacy concerns have also had an impact on users' adoption of new technologies that share users' personal information. A multitude of mobile location-finding applications have become available over the last two decades, but the products and services offered by the technology developers may not comprehensively address the privacy implications and privacy concerns surrounding their use. The design considerations for these products may not provide the necessarily amount of control or risk mitigation for users to ensure that their location information is not misused. These applications have yet to see a critical mass of adoption and use.

In this thesis, I focus on the impact of salient privacy information on privacy concerns and behavior in two contexts: online shopping and the use of a mobile-location sharing technology. I examine several case studies focusing on the evolution of privacy attitudes after people use specific technologies. Based on the examination of the use of a location-sharing system, I highlight several design considerations for mobile-location application developers to ensure they address their users' privacy concerns. I use the results of online surveys and user studies to provide concrete information on the impact of feedback on the comfort with using location-sharing technology. This research shows that users will pay a premium to purchase from websites that offer better privacy policies if that privacy information is made visible and understandable. This research points to the importance of control in the management of privacy concerns. Whether mandated by legislation or recommended in industry or design standards, offering users control in the form of understandable privacy policy information, or control over the disclosure of personal information by technology, is essential.

1.1 Research Questions

The following questions have guided the research in this dissertation:

- What are people's privacy concerns when they shop online and use applications that allow their locations to be displayed on an online social network?
- How do concerns regarding personal location evolve as people become accustomed to the new technologies that display or broadcast their location?
- What is the impact of an interface that allows users to define the restrictions they wish to place on the disclosure of their location?
- Will the prominent display of privacy information cause users to take the level of privacy protection offered by retailers into account when making online purchasing decisions?
- What is the impact of the timing of privacy information when consumers are making purchasing decisions?
- What is the relative value that people place on the level of privacy protection provided by a company compared to the premium that they would have to pay to obtain that

level of protection?

- When using a search tool that displays privacy icons rating how well the site matches the users' defined privacy preferences, will users choose to visit sites that better match their privacy preferences?

1.2 Research Overview

Overall, the problem of invisible privacy drives the research in this thesis. By making privacy more salient or prominent through awareness, notification, and control, users will be better equipped to make decisions regarding their personal information. I focus on the areas of location-sharing technologies and consumer privacy as offered by websites. The varied nature of personal information in these areas combined with the similarity of privacy concerns allows me to provide broad recommendations on how policymakers, online organizations, and technology developers can better adopt methods to make privacy information more salient for both their benefit and the benefit of the user.

This thesis presents several studies that examine the use of location-sharing systems with feedback and varied rule interfaces. These studies advance our understanding of users' perceptions of the risks and benefits of location-sharing technologies as well as the importance of the context of use on the privacy concerns that surround these technologies.

The second half of this thesis provides empirical evidence of the significant impact of salient privacy information on purchasing patterns. When privacy information is presented alongside search results, people will pay a premium to purchase from sites that offer better privacy. Similarly, privacy indicators placed in a search engine interface can increase website visitation rates for sites with high privacy.

1.2.1 Mobile Location Privacy Concerns Study

While new location-sharing technologies and applications are being developed at a rapid pace, there is a lack of background and research that deals with the perceptions or specific concerns surrounding the use of location-sharing applications. I evaluate the privacy controls offered by a sample of these applications and conduct an online survey of American Internet users to evaluate users' perceptions of the likelihood of several location-sharing use scenarios along with the magnitude of the benefit or harm of each scenario (e.g. being stalked or finding people in an emergency). While the majority of respondents had heard of location-sharing technologies (72.4%), they do not yet understand the potential value of these applications, and they have concerns about sharing their location information online. Most importantly, participants are extremely concerned about controlling who has access to their location. Generally, respondents feel the risks of using location-sharing technologies outweigh the benefits. Respondents felt that the most likely harms would stem from revealing the location of their home to others or being stalked. People felt the strongest benefit were being able to find people in an emergency and being able to track their children. Additionally, I find that while existing commercial location-sharing applications' do not offer their users a diverse set of rules to control the disclosure of their location, they do offer a modicum of privacy.

1.2.2 Location-Sharing Feedback Study I (Locyoution)

The human computer interaction literature cites feedback as a essential design consideration in designing for privacy in ubiquitous computing environments. I investigated the effect of feedback, that is, knowing who has requested one's location, on users' comfort level using Locyoution, a location-sharing system. In this system, users could create time-based rules specifying when they could be located. Locyoution users interface with the system via Facebook, an online social network. Participants, divided into two conditions: a group without feedback, and a group with feedback, used Locyoution for a month. In general, after using Locyoution, participants concerns about their privacy were reduced. Participants with feedback became more comfortable with being located by friends and strangers. Additionally, the results of the study suggest that peer opinion and technical savviness positively contributed to the continued use of a mobile location technology.

1.2.3 Location-Sharing Feedback Study II (Locaccino)

To followup to the Locyoution study, I examined the impact of feedback on users' levels of comfort using Locaccino, the redesigned interface to Locyoution. The Locaccino interface limited location requests to users' Facebook friends, and also provided users with additional options for rules defined by time, group, and location. Participants (divided into two conditions, a group *without feedback* and a group *with feedback*) used Locaccino for a period of a month. We conducted qualitative interviews with a small sample of users to better understand users' perceptions of Locaccino. The results of this study indicate that contrary to the previous study, providing users with feedback, by and large, had no impact on comfort levels of using the system and on patterns of usage with the system, suggesting that the fundamental shift in the system design of Locaccino, limiting access to “friends" and increasing the expressiveness of rules interface, mitigated privacy concerns.

1.2.4 Online Privacy Concerns Study

To understand the types of concerns people had related to their privacy when shopping online, I conducted a survey which quantified the perceived likelihoods and risks associated with those privacy concerns. Based on the results of the survey, I found that an interface used in the study called Privacy Finder addresses the highest rated concerns of the participants. Similar to previous studies, I find that most people have concerns when they are on the Internet and when they shop online, but most do not read privacy policies in their entirety. People tend to notice the presence of privacy policies more often than read them.

1.2.5 Privacy Information Purchasing Study

To determine the impact of salient privacy information on online purchasing patterns, I conducted a user study to examine the relationship between privacy premiums, levels of privacy, and the privacy-sensitivity of the product. Participants were divided into three conditions: no privacy information, irrelevant information, and privacy information. Using a search engine interface, people searched for and purchased a privacy sensitive item and a non-privacy sensitive item. The results were ordered in such a way that the site with the highest privacy level sold the products at the highest price, forcing users to pay a premium for privacy. The results of this study show that users will pay a premium to purchase both privacy-sensitive and non-privacy sensitive items when presented with privacy information.

1.2.6 Privacy Premium Survey

In the Privacy Information Purchasing study, the privacy premiums between the privacy-sensitive and non-privacy sensitive items are different. To standardize the comparison of the privacy premiums between the two products, I conducted an online survey to estimate the maximum premium that participants would be willing to pay to purchase from a website with a high privacy level. Participants viewed screen shots of search results and product prices for a privacy-sensitive and a non-privacy sensitive product. They then picked the site they would have purchased from. The results of this study inform the design of the next privacy information-focused purchasing study.

1.2.7 Privacy Information Timing Purchase Study

To examine the impact of the timing of the presentation of salient privacy information on online purchasing decisions, participants purchased privacy and non-privacy sensitive products using the Privacy Finder search engine interface. The timing of privacy indicators tested were the following: not at all (instead, users were presented with irrelevant indicators in the search engine interface as the control); alongside search engine results; in a frame above the destination website; or on an interstitial webpage after clicking a search result and before viewing the destination website. Vendors collaborated with this study, setting the prices for the products based on a premium survey completed prior to the study. Participants who viewed the privacy indicators in the search engine interface were the most likely to pay a premium for high privacy when purchasing privacy-sensitive items.

1.2.8 Privacy Finder Usage Study

To build on the body of research presented here that privacy information can have a significant impact on purchases, I conducted a field study to determine the impact of salient privacy information on search result browsing patterns. I recruited users for Privacy Finder, the P3P-enhanced search engine and tracked their searches, their search results, and the sites they visited. By comparing the visitation rates to sites with and without privacy information, I found that users were significantly more likely to visit sites with high privacy indicators, regardless of the search result ranking. I also observed that privacy indicators act as a draw, increasing the visitation rates of sites further down on the search results page.

In Section II, I present the work related to the privacy implications of mobile location-sharing technologies. The privacy and consumer choice studies are presented in section III. Policy recommendations are made in the conclusions IV.

Chapter 2

Background and Related Work

2.1 Information Salience

The concept of salience has been extensively investigated in psychology. in general, something that is salient is “prominent" and “enters thought more readily" [72]. Salient information, attitudes, or beliefs occupy people’s attention [72] or is easily brought to mind [110]. Salience also refers to the accessibility of knowledge that can be used to categorize information [26]. This research is guided by the salience hypothesis, where salient cues guide future actions [110] (consumer decision-making), and the hypothesis that salience plays an important role in knowledge activation [56]. We see that it is appropriate to refer to the “salience of privacy information" in this research (the term coined by Acquisti, Loewenstein, and John [66]) to examine the impact of usable privacy information on consumer decision-making.

2.2 Privacy Concerns

2.2.1 Online Privacy Concerns

Having access to and using the Internet has become a way of life for people in the United States (so much so that it is beginning to be considered a public utility [3]). The majority of Americans (80%) now use the Internet, spending an average of 17 hours online per week. Of those people online, two-thirds also make purchases online. Almost all of these people also have concerns about their privacy when purchasing things on the Internet [75]. When asked, most Americans say that their right to privacy is “under serious threat," [30] and express concern about companies collecting their personal data [4, 54, 30, 28, 117, 34, 74, 82]). These concerns may impact user behavior: based on survey responses, 64% of people indicated that they “decided not to purchase something from a company because they weren’t sure how their personal information would be used" [28]. While most people realize that they are concerned about their privacy, they are unsure of what to do to protect it.

2.2.2 Location-Based Privacy Concerns

By 2009, at least 87% of the U.S. population owned cellular phones [2]. The proliferation of mobile devices and mobile Internet devices (including laptops) along with federal E911 requirements and the ubiquity of GPS-capabilities in mobile devices has spurred the development of location-sharing applications [95]. These technologies, also referred to as *mobile location* technologies, *social mobile* applications or simply *location-based services*

(LBS), typically allow users to share their real-time or historical location information online.

Another application for mobile location-enabled devices is sharing real-time location information with friends, family, and colleagues. These types of technologies are best used in a social network setting. These sites allow users create profile, contact lists, and to traverse a list of connections [42]. As mobile location-finding technologies become more popular, developers have begun offering products and services that may not comprehensively address the privacy implications of such technologies [59]. In a Harris Interactive Poll, 70% of respondents felt that being able to “determine the location of persons on your contact list" was an invasion of privacy [55]. As of now, location-based technologies are still on the cusp of becoming the next great thing. While several “friend-finding" location-based products for cellular phones have been commercially available since 2006 (specifically services and products being offered by Loopt and Helio), it is only recently (early 2008) that technology providers have started offering technology platforms on which others can build location-finding applications. These include several cellular phone development platforms, including the iPhone SDK and Google’s Android SDK, and Yahoo’s Fire Eagle location-sharing service. It is still to be seen how these services will be received by the general public.

As these technologies are developed, the ability to define and control the privacy afforded by location-aware devices is imperative. Additionally, users’ privacy concerns and needs may change as they realize the full capabilities of the technology. People have significant privacy concerns when dealing with broadcasting their location [79, 20, 18]. In fact, is it these privacy concerns may be one of the top reasons for the slow adoption of location-based services (LBS) [67].

2.3 Dimensions of Privacy Concern

Understanding privacy concerns is a topic treated in the marketing and information science literature. These concerns can be grouped into several categories. Smith, et al. [100] 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 (see also [105]). Similar dimensions also apply to information privacy concerns the arise from online marketing and during online purchasing. In the online marketing situation, the dimensions of concern are reframed. Malhorta et al. describe the *collection* of personal information, the *control* over the use of personal data, and the *awareness* of privacy practices and uses of personal information [77]. The information privacy categories of control and awareness encompass the previous categories of unauthorized secondary use, improper access, and errors. Focusing on online purchasing behavior, the dimensions of concern defined by Brown and Muchira [25] become *unauthorized secondary use*, *errors* in personal information, and the *invasion of privacy*. Consumers place most importance on the invasion of privacy that occurs when people receive unsolicited communications.

Survey data indicates that online consumers place the highest importance on awareness of what will be done with personal information and how they can have direct control over their information [77]. In many instances, consumers have little control over the practices of the organizations or businesses that are collecting their information. Where consumers do have control is over the selection of the organizations or businesses with which they choose to share their information, and the type of information they choose to provide. When concerns are elicited by the merchant's behavior, the individual may lose trust in the merchant [29]. Milne and Gordon [86] present proper treatment of consumer information as an “implied social contract" with the customer. When a breach of confidentiality between the organization and the individual occurs, such violation of trust may entitle the victim to compensation [102]. On the other hand, the guarantee of fair information practices can counterbalance consumer's concerns about information sharing [40].

These dimensions of privacy concern listed also apply to scenarios beyond online marketing. As new technologies are developed, we see that the same types of privacy concerns continue to exist. In the context of location privacy, there are still issues related to the collection, awareness, and control of this type of personal information. As with personally identifying information on the Internet (credit card information, behavioral patterns), a user's location information is being collected, stored, and analyzed. For example, the mobile marketing industry is hoping to boost ad spending on mobile devices to $28.8 billion in the next 5 years [14], and several companies have already begun to experiment with location-based mobile advertising [22].

2.4 Invisible Privacy

Privacy, especially on the Internet, is very difficult to quantify. Most people can visualize closing the shades or being alone on a deserted island, but it is much more difficult to make privacy something with substance when the setting consists of IP addresses, cookies, web browsers, and latitude and longitude coordinates. One method industry and the government have taken to address these concerns is to recommend that businesses post privacy policies to convey their privacy practices [58]. Despite the large number of privacy policies posted online [84], privacy information remains invisible to Internet users: privacy policies have not been effective at making privacy information accessible. Privacy policies are difficult to read [117], few people make the effort to read them [64, 85, 90, 112], and the policies themselves are difficult to understand [16, 41, 57, 64]. A study by Sherman et al. asserts a graduate school education is required to even read typical privacy policies [97]. 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 [112, 117]. While individuals may be aware that a company or organization has a privacy policy, they still lack enough information to make informed decisions.

Similarly, in location-sharing applications, one typically has no knowledge of who is requesting their location information, or what is happening with that information. There is an issue of social translucency and control that is relevant to privacy in online social networks (OSN). One way that OSNs could make privacy more visible is by providing feedback to the user. The human computer interaction research community has looked at the question of feedback in ubiquitous computing environments. Feedback has been found to be one of the major principles that should be considered when designing new ubiquitous computing systems to mitigate privacy concerns [21, 60], yet comprehensive methods of feedback are restricted by the timing, perceptibility, obtrusiveness, intrusiveness, and cost of those mechanisms [21]. New technologies and interfaces have made it easier to provide more comprehensive feedback.

With new web interfaces, users can audit the actions the system has taken on their behalf and monitor how people use the system. Feedback also provides social pressure which should help to avoid abuses of the system. Looking at online social networks, we see that several online social networks do not provide feedback (Facebook and MySpace), but others have found it to be a useful feature in system design for creating ties between users. Online social networks Friendster and Orkut, have added "Who's Viewed You" features with mandatory reciprocity. Several online dating sites offer feedback features, e.g. "Who's viewed me" on Match.com[1] and Yahoo! Personals[2]) or "My Stalkers" on OkCupid.com[3].

To address users' privacy concerns in the use of location information, CTIA, the International Association for the Wireless Telecommunications Industry,[4] has issued Best Practices and Guidelines for LBS providers. These guidelines are meant to help LBS providers protect user privacy and rely on *user notice* and *consent* [1]. Generally, mobile providers provide their statements regarding notice and consent in their posted privacy policies or terms of service, rending this privacy information invisible.

---

[1] Match.com. `http://match.com/help/helpdtl.aspx?sec=35`

[2] Yahoo! Personals. What is Who's Viewed Me? `http://yahoo.personals.com`

[3] OkCupid.com. Your OK Stalkers. `http://www.okcupid.com/stalker`

[4] The CTIA Wireless Association. `http://www.ctia.org/`

2.5 Previous Privacy Research

2.5.1 The Valuation of Privacy

Over time, surveys have consistently indicated that people are concerned about their personal data and how companies will use that information. Evidently, those concerns hinder certain consumers from making online purchases. A 2005 survey conducted by Privacy and American Business (P&AB), for instance, 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 [28]. On the other hand, consumers have also been found to be willing to provide personal information for small discounts or rewards. A 2002 Jupiter Research study found that 82% of online shoppers were willing to give personal data to new shopping sites in exchange for the chance to win $100 and that 36% would permit their World Wide Web surfing habits to be tracked in exchange for $5 discounts [111]. In an experimental investigation, [104] found evidence that even privacy concerned individuals are willing to trade-off privacy for convenience and discounts. Similar dichotomies have been found in other privacy scenarios, such as consumer grocery cards and online social networks [7, 9].

In fact, the difficulties that companies in the privacy sphere have met trying to find a market for their products [27] suggest that while these concerns exist, many consumers are reluctant to pay for privacy protections or technological solutions.

Several researchers have further investigated how individuals make a tradeoff between privacy and monetary or intangible benefits, trying to determine the drivers of consumer privacy valuations. Hann et al. [53] tried to quantify the value individuals ascribe to website privacy protection, and found that “among U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49-44.62.” Chellappa and Sin [31] found evidence of a tradeoff between consumer valuation for personalization and concern for privacy. Huberman et al. [61] used a second-price auction experimental setup to study the monetary value of private information (such as an individual’s weight) to individuals. They found that information considered more “abnormal” or “undesirable” had a greater impact on what price was demanded to reveal that information. In a contingent valuation survey of the value assigned to enforceable property rights to their personal information, [94] found that survey participants expressed high sensitivity to privacy, but only 47% of them would be willing to pay for those property rights (an average of NZD 55.40 or USD 28.25). [62] used a field experiment in Singapore to study the values of various privacy assurance measures. They also found that privacy statements and monetary incentives could both induce more information disclosures. Similarly, Danezis et al. [43] used a second-price auction setup to obtain an estimate of value that people attach to their location information. They found that the median bid that users would want to be paid to allow their location information to be used was 10 GBP or USD 18.70, and those who traveled more frequently outside of Cambridge valued their location privacy more.

A debate has therefore emerged in the literature as to whether the co-existence of individual privacy concerns and willingness to make a tradeoff privacy for even small benefits may be evidence of inconsistent behavior, or, more simply, rational decision making and between-subject variance in privacy sensitivities [5, 8, 9, 99, 108, 118]. That literature has highlighted several factors that may affect individual privacy attitudes. These factors include variability in individual privacy sensitivities, bounded rationality, behavioral or cognitive biases, such as immediate gratification or optimism bias [5], and information asymmetry [13]. Information asymmetry, in particular, plays a double role in privacy valuations and decision-making. To use an example from the context of online shopping, before a consumer completes her first purchase at an online merchant, the merchant may have limited information about the consumer's taste, reservation price, identity, and so forth (see [11, 109]). However, after the purchase, the consumer has incomplete information regarding how the merchant will use the personal information revealed through the transaction [10]. Such incomplete information may affect individual behavior in different ways: it may make the consumer more likely to engage in a certain transaction (because she does not realize its potential privacy risks); but it may also make it less likely that a consumer will complete a transaction (because the increased risk and uncertainty of transacting with merchants whose privacy policies are not known decreases the willingness of consumers to complete such transactions).

2.5.2 Studies of Privacy in Location-Based Applications

Many previous studies of location-sharing applications have employed a variety of methods to examine the usage of such systems and privacy concerns raised by these systems. The Experience Sampling Method (ESM) has been employed by several researchers to determine how much information people would share and to what degree of detail [33], the social context of location-disclosures [70], and the context in which people are willing to share their location information [15]. Similarly, diary studies and small laboratory experiments have been conducted [20, 35, 89] to examine the usefulness and invasiveness of the technology. Deployments of such systems have typically involved small groups of participants who were members of an existing social group where the requestee responded via SMS with their location information [63, 101] or had their location provided automatically when their phone was on [19]. Other deployments involved groups who may already be aware of or have access to each other's location information, such as family members using the Whereabouts Clock [24]. While users are willing to share their locations when presented with a request for that information [33, 70, 96], past work strongly suggests that users have concerns over who is trying to find them and the context in which that person is requesting a location [24, 33, 63, 70, 76, 101]. Others have examined control mechanisms for mobile applications, finding that users will create groups of contacts for permission control [60, 89].

2.6 Privacy Indicators

2.6.1 P3P

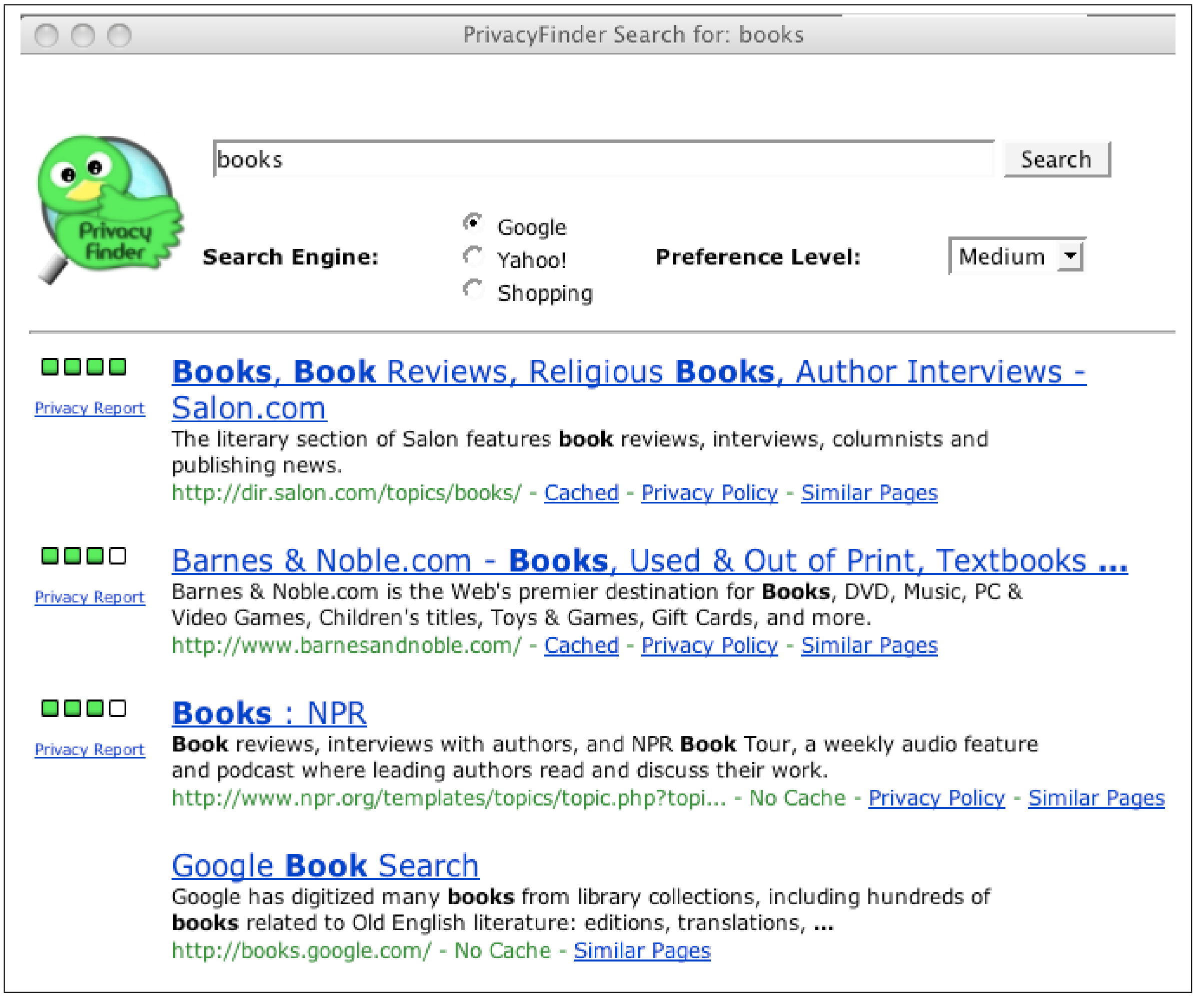
The World Wide Web Consortium (W3C) developed the Platform for Privacy Preferences (P3P) to make privacy policies more usable. P3P is a standard machine-readable format for privacy policies that standardizes the vocabulary in which companies can specify their data practices [37]. A company can go through is "natural language" privacy policy and create a corresponding P3P policy in extensible Markup Language (XML). Once this process is complete, the company can post its P3P files online to be read by P3P-enabled web browsers and P3P “user agents” [37]. These P3P user agents (built into web browsers or stand alone software programs) then parse the computer-readable privacy policies simplified formats which may or may not be accompanied by a visualization to help the user comprehend the privacy policy [39].

2.6.2 Privacy Finder

The Carnegie Mellon Usable Privacy and Security Laboratory (CUPS) 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.

Privacy Finder builds directly on the Google and Yahoo! search engine services, and "consists of four main architectural components: a policy acquisition module, a search engine integration module, an APPEL evaluation engine, and a caching daemon." Together, these components "acquire, maintain, and present a view of the P3P policies of sites returned by user search queries" [38]. The Privacy Finger interface is shown in Figure 2.1. 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 and reports.

When Privacy Finder displays the search results, they are annotated with privacy indicators or “privacy icons" that graphically represent how well a website’s P3P policy matches



books

Search Engine: ● Google ○ Yahoo! ○ Shopping

Preference Level: Medium

🟩🟩🟩🟩 Privacy Report

Books, **Book** Reviews, Religious **Books**, Author Interviews - Salon.com

The literary section of Salon features **book** reviews, interviews, columnists and publishing news.

http://dir.salon.com/topics/books/ - Cached - Privacy Policy - Similar Pages

🟩🟩🟩☐ Privacy Report

Barnes & Noble.com - **Books**, Used & Out of Print, Textbooks **...**

Barnes & Noble.com is the Web's premier destination for **Books**, DVD, Music, PC & Video Games, Children's titles, Toys & Games, Gift Cards, and more.

http://www.barnesandnoble.com/ - Cached - Privacy Policy - Similar Pages

🟩🟩🟩☐ Privacy Report

Books : NPR

Book reviews, interviews with authors, and NPR **Book** Tour, a weekly audio feature and podcast where leading authors read and discuss their work.

http://www.npr.org/templates/topics/topic.php?topi... - No Cache - Privacy Policy - Similar Pages

Google **Book** Search

Google has digitized many **books** from library collections, including hundreds of **books** related to Old English literature: editions, translations, **...**

http://books.google.com/ - No Cache - Similar Pages

Figure 2.1: Privacy Finder search engine interface

the privacy preferences specified by the user. The icons represent a five-point privacy “meter" (see Table 2.1). The meter is composed of a set of four boxes that are shown as green (filled) or white (empty) based on an algorithm that accounts for the number of privacy preference mismatches. Thus, a site that violates most of the user’s preferences will have zero or one box filled, while a site with only a few mismatches might have two or three filled boxes. Sites without P3P policies are not annotated with a privacy icon.

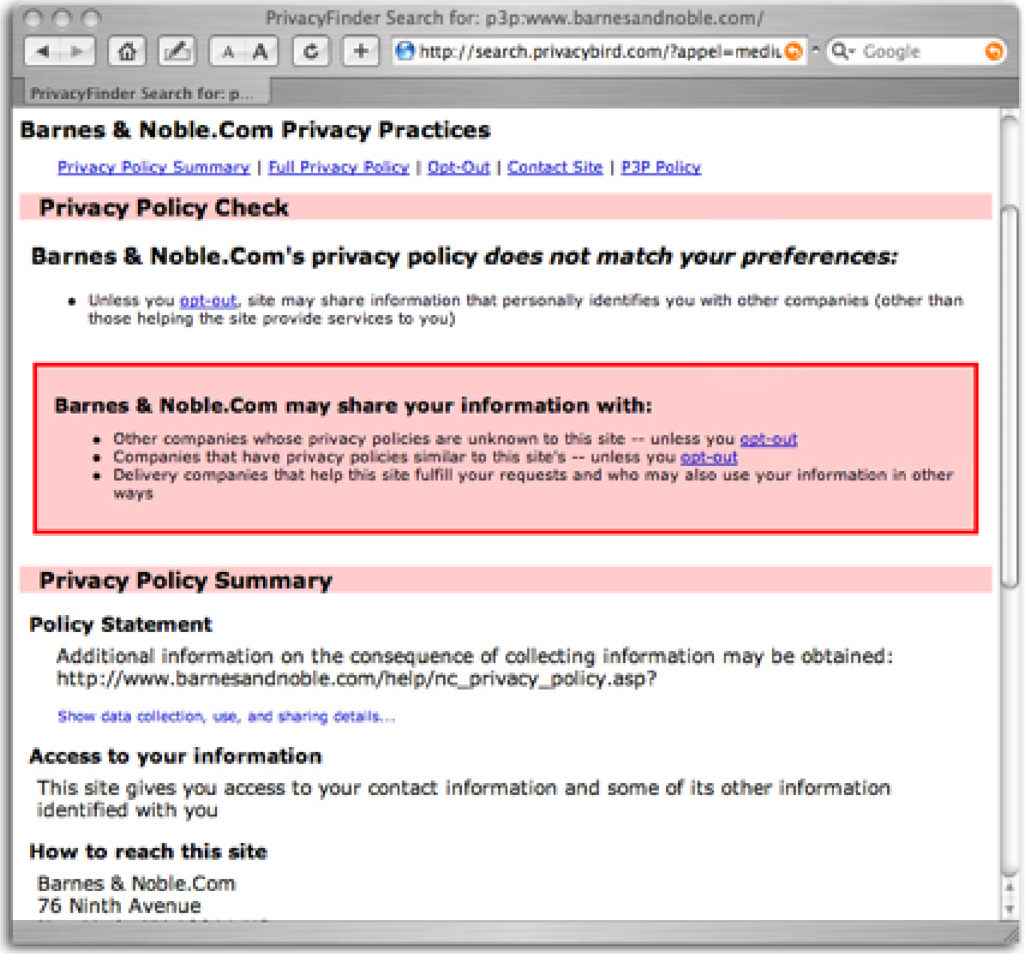
Privacy Finder provides a link to the privacy report for each P3P-enabled website. The

Icon	Site
🟩🟩🟩🟩	Matches privacy preferences
🟩🟩🟩☐	
🟩🟩☐☐	↓
🟩☐☐☐	
☐☐☐☐	Does not match privacy preferences

Table 2.1: Privacy Finder’s privacy indicators

privacy report includes a “Privacy Policy Check" section that highlights the specific areas where the policy does not match the user’s privacy preferences as shown in 2.2. The privacy report has been designed to present the privacy information that is “of greatest concern to users" in a simplified format [39].

The privacy information and reports are intended to provide a risk communication to consumers, allowing them to make “informed, independent judgments" [87] about the websites they visit. By providing this privacy information in an Internet search engine interface while people are actively seeking web pages, Privacy Finder further reduces the privacy information asymmetry that makes it so difficult for people to act consistently with their privacy preferences. In turn, by adapting their information systems to produce machine-readable privacy policies, corporations can ensure that their policies will become more accessible to visitors and consumers.


PrivacyFinder Search for: p3p:www.barnesandnoble.com/
http://search.privacybird.com/?appel=mediu
Google
PrivacyFinder Search for: p...

Barnes & Noble.Com Privacy Practices

Privacy Policy Summary | Full Privacy Policy | Opt-Out | Contact Site | P3P Policy

Privacy Policy Check

Barnes & Noble.Com's privacy policy *does not match your preferences:*

- Unless you opt-out, site may share information that personally identifies you with other companies (other than those helping the site provide services to you)

Barnes & Noble.Com may share your information with:

- Other companies whose privacy policies are unknown to this site -- unless you opt-out
- Companies that have privacy policies similar to this site's -- unless you opt-out
- Delivery companies that help this site fulfill your requests and who may also use your information in other ways

Privacy Policy Summary

Policy Statement

Additional information on the consequence of collecting information may be obtained: http://www.barnesandnoble.com/help/nc_privacy_policy.asp?

Show data collection, use, and sharing details...

Access to your information

This site gives you access to your contact information and some of its other information identified with you

How to reach this site

Barnes & Noble.Com
76 Ninth Avenue

Figure 2.2: Privacy policy summary generated for BarnesandNoble.com

2.7 Technology Adoption in Ubiquitous Computing Environments

To understand the factors that impact the acceptance or adoption of various technologies, the information systems field has developed a technology acceptance model (TAM) [44]. These models typical focus on the usefulness and the ease-of-use of technologies in a business environment (i.e. phone tree voicemail system). Spiekermann [103] has expanded upon the traditional user acceptance model to study ubiquitous computing (UC) technologies. Ubiquitous computing broadly refers to “a vision of environments and people augmented with computational resources which provide information and services when and where desired" [103]. Location-sharing technologies fall within this definition of UC: location information is automatically pulled for the user and displayed for others.

Spiekermann’s [103] examination of RFID technologies has defined several additional factors for consideration in the acceptance of UC technologies. These factors include control, helplessness, peer opinion, technical savviness, and privacy. In the acceptance of user-based privacy enhancing technologies (PET) for RFIDs, the usefulness of the PET, the perception of helplessness regarding the use of RFIDs, and information control properties of the PET were found to be significant factors in users’ attitudes towards privacy-enhancing technologies for RFIDs.

Part II

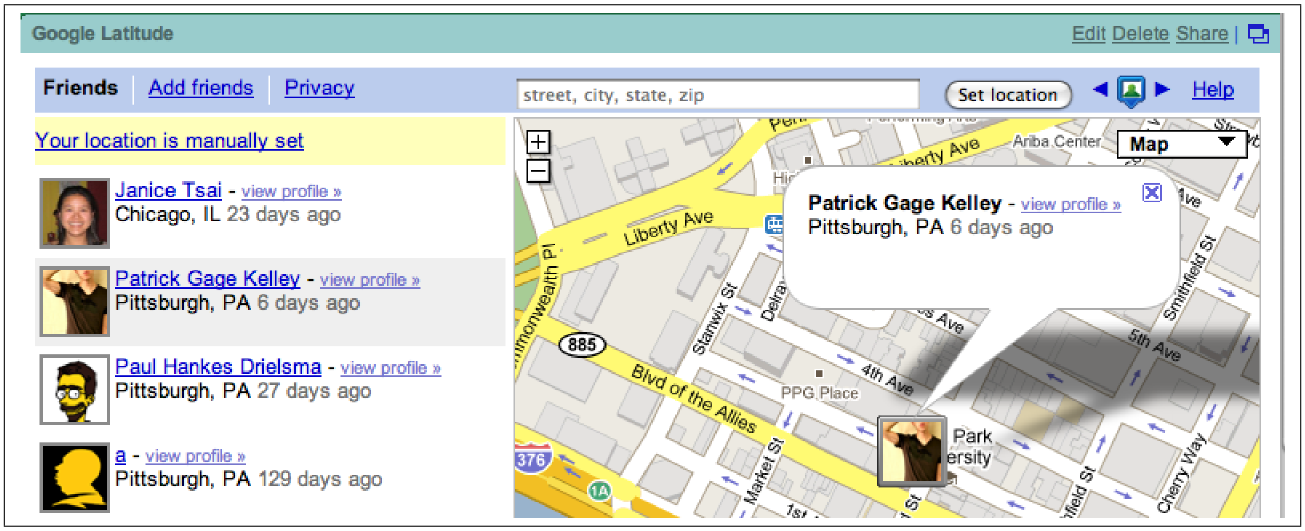
Privacy Implications of Mobile Location Technologies

Chapter 3

Mobile Location Privacy Concerns Study

This chapter is largely a reproduction of a paper co-authored with Patrick Gage Kelly, Lorrie F. Cranor, and Norman Sadeh [115]. This work is funded in party by the National Science Foundation under Cyber Trust grant CNS-0627513 and by the Army Research Office contract no. DAAD19-02-1-0389 to Carnegie Mellon University's CyLab. Additional support has been provided by Microsoft through the Carnegie Mellon Center for Computational Thinking, FCT through the CMU/Portugal Information and Communication Technologies Institute, and through grants from FranceTelecom and Nokia.

While new location-sharing technologies and applications are being developed at a rapid pace, there is a lack of background and research that deals with the perceptions or specific concerns surrounding the use of location-sharing applications. I evaluate the privacy controls offered by a sample of these applications and conduct an online survey of American Internet users to evaluate users' perceptions of the likelihood of several location-



Your location is manually set

Janice Tsai - view profile »
Chicago, IL 23 days ago

Patrick Gage Kelley - view profile »
Pittsburgh, PA 6 days ago

Paul Hankes Drielsma - view profile »
Pittsburgh, PA 27 days ago

a - view profile »
Pittsburgh, PA 129 days ago

Patrick Gage Kelley - view profile »
Pittsburgh, PA 6 days ago

Figure 3.1: The web interface for Google Latitude

sharing use scenarios along with the magnitude of the benefit or harm of each scenario (e.g. being stalked or finding people in an emergency).

3.1 Locating Technologies

The location-information shared by LBS may be text-based (e.g. “Andrew has been located at 5000 Forbes Ave., Pittsburgh, PA”), or it may be map-based, where the user’s location is represented as a dot on a map as illustrated in Figure 3.1 and Figure 3.2. To display location information, users can manually enter a street address or longitude and latitude coordinates. Today, location information is more frequently acquired through automated means.

The following locating technologies are typically used to determine users’ locations:

- **GPS:** The Global Positioning System (GPS), locates a user through a device that is

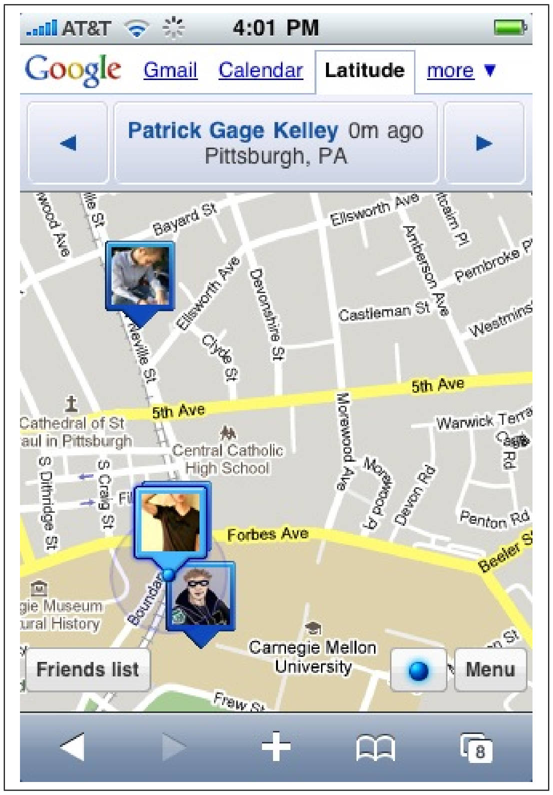


Figure 3.2: The iPhone interface for Google Latitude

in communication with a constellation of satellites. Triangulation by multiple satellites locates the device, making GPS the most accurate method for finding locations [95]. However, drawbacks include the lack of user-accessible GPS capabilities in most personal cell phones and the scarce availability of built-in GPS technology in commercial laptops. Additionally, GPS can be battery intensive and inconsistent or unavailable indoors.

- **Wireless positioning:** As urban areas become blanketed with both personal and public WiFi access points, users can be mapped according to the location of these access points. Through the process of "war-driving" access points, and mapping each broadcasting point to a GPS location [71], researchers and companies such as Skyhook Wireless[1] have created large databases with high location accuracy. While these locations are not always as precise as GPS, more people have wireless devices and location information can be pinpointed indoors.

- **Cellular identification:** At any given time, a mobile phone is likely in signal range of upwards of three cell phone towers, allowing a location to be triangulated if the locations of the cell towers are known. Some companies have partnered with telecom companies to use cellular data. One such company, AirSage[2] analyzes wireless signaling data to model traffic patterns. Loopt, a location-sharing service also leverages a cellular partnership with AT&T to provide always-on location information based on a user's iPhone [50].
- **IP Location:** Devices connected to an Internet network are provided with an IP address. IP addresses are limited in number; and based on the range, can be associated geographically [93]. (See the IP-to-Country Database.[3]) IP location is mostly used as a fallback when none of the above methods are available. The resolution of such lookups is commonly mapped to an area as large as a city.

3.1.1 Development Platforms for Locating-Technologies

Locating technologies are available for mobile phones, laptops, and internet-enabled mobile devices. There are three common ways for applications to pull location information:

---

[1] Skyhook Wireless. `http://www.skyhookwireless.com/`

[2] AirSage. `http://www.airsage.com`

[3] IP-to-Country Database. `http://ip-to-country.webhosting.info/`

- **Installed Software:** Users download and install software onto their cell phones or computers. Software determines the user's approximate location by one of the methods listed above and stores that data in a database or sends it to a location-sharing application. This transmission of coordinates may be automatic (e.g. a location ping is sent every 5 minutes) or it may require a "push" action to be initiated by the user (e.g. the user clicks a "Find me now" button).
- **Web browser:** In lieu of requiring the user to run a separate piece of software, several companies have developed location-finding web browser plug-ins. Applications that use this technology allow users to visit a website to be located, typically according to the users' wireless or IP location, based on an installed plug-in, such as Skyhook's web toolbar Loki.[4]
- **Location Broker:** APIs, (e.g. Yahoo!'s FireEagle[5] and Google Latitude[6]) allow developers to create applications that pull the user's location from a central provider. This allows application developers to entirely avoid any of the location lookup technologies, relying on a third party to provide location information.

3.2 Privacy Controls in Location-Sharing Applications

We evaluated 89 applications, social networks, and APIs to evaluate their privacy controls. See the Appendix for a list of the applications. Our privacy and location-based services

---

[4] Loki. `http://loki.com/`

[5] FireEagle. `http://fireeagle.yahoo.net/`

[6] Google Latitude. `http://www.google.com/latitude/apps/badge`

data is available online for download.[7]

3.2.1 Method

We used a user-contributed online list of location-based services[8] as our directory of sites. In general, the sites on this list are social in nature. We found its completeness to be unparalleled across the web. We removed from consideration any sites that were not location-based services, or sites that were offline or defunct (n = 10). This leaves us with a final set of 89 applications.[9] We did not consider "surveillance technologies."

To create our dataset, we completed a number of steps. First, we first visited the website for each application. We read the "About" page, frequently asked questions (FAQ), "Help" pages, and any other documentation available to search for explanations of their privacy controls. Additionally, we evaluated web interfaces, Facebook applications, and screenshots and descriptions of the iPhone application in the iTunes App Store. We evaluated the following features of these applications:

- **Date of launch:** While many of the current location-based services have been relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public, or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.

---

[7] Evaluation of Location-Sharing Application Privacy Controls. `http://cups.cs.cmu.edu/LBSprivacy/`

[8] A list of Location Based Social Networking sites. `http://bdnooz.com/lbsn-location-based-social-networking-links/`. Last visited August 10, 2009.

[9] Note: One of the applications included on the list, Locaccino, was developed by the authors.

- **Privacy Policy:** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service).
- **Privacy Controls:** We noted any ability that allowed users to control access to their location information.
- **Notice:** Some systems notify users when others request their location, or make an activity log available to allow users to see who has requested and received their locations.
- **Immediately accessible privacy settings:** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled “Privacy” would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.

3.2.2 Data Analysis

We constructed a dataset[10] based on our collection of the features listed above. In this section, we present the results of our analysis.

---

[10] Evaluation of Location-Sharing Application Privacy Controls. `http://cups.cs.cmu.edu/LBSprivacy/`

System Characteristics

The primary purpose of the majority of these applications was for tracking friends or finding new ones. Other highlights included sites geared towards location-based dating, travel planning and sharing, and information seeking (e.g. finding local "hot spots"). One site even allows users to tag speed traps.

Of the 89 applications surveyed, 63 are available for use on mobile phones. Of those phone-based applications, the iPhone was the most popular development platform (40 applications). Application developers also created products for the Blackberry (32), phones that use the Android OS (21), or other phones (34). These numbers include services that developed a mobile formatted web version of their application and are not mutually exclusive. For example, a single service may have an iPhone application, a Blackberry application, and an Android application.

The architectures of the location-sharing applications fell into two categories:

- **Open:** Users can be found by friends and strangers.
- **Closed:** Users may only be requested by "friends" on the system. In this case, users much have already granted the requester access (e.g. by accepting a friend request).

Of the surveyed applications, five did not allow users to request other users' location information; but allowed users to seek information about places or landmarks; and two are location-sharing APIs. Of the remaining sites, 29 are closed systems, and 52 are open systems.

Rate of Creation

The development of location-sharing applications has steadily increased over time as shown in Figure 3.3. Several new technologies may have spurred the development of location-sharing technologies. These include the launch of Yahoo's FireEagle platform (Q1 2008) and the iPhone SDK[11] with its Core-Location framework (Q3 2008).

The rate at which location-based services were introduced to the market increased from 5 per quarter at the end of 2006 to 14 per quarter at the end of 2008. After the economic downturn in 2008 the rate of introduction slowed, but new services continue to be introduced in 2009 at a rate of at least 8 per quarter. This overall growth leads us to believe two things. First, the development-side technologies are in place for location-based services and social networks to be created, and there are not unsolvable technical issues in the way of growth. Second, there do not seem to be strong market leaders who are prohibiting others from entering the market. Even with large players like Google, and established brands like Loopt, we have not seen any one of these technologies spread to a large section of the populace (however, finding active user data for any of these services has proven to be difficult).

Privacy Controls

Due to the sensitive nature of real-time location information and the existence of guidelines recommending clear notice to users, one would expect all location-sharing applications to detail their policies for the collection and use of personal information. Instead, we found

---

[11] iPhone Dev Center. `http://developer.apple.com/iphone/`

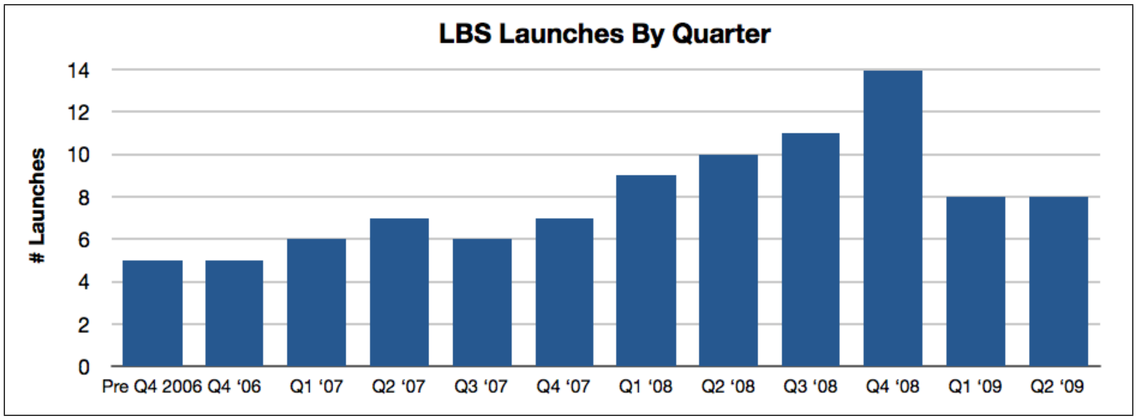


Figure 3.3: The number of location-sharing applications launched each quarter (includes 89 applications evaluated in our study and 7 defunct applications).

Category	Yes	No	Unknown	Not Applicable
Privacy Policy	66.3% (59)	33.7% (30)	-	-
Privacy Controls	76.4% (68)	16.9% (15)	1.12% (1)	5.62% (5)
Accessible Privacy Settings	16.9% (15)	75.3% (67)	2.25% (2)	5.62% (5)

Table 3.1: An overview of the proportion of applications that have privacy policies, privacy controls, and explicit privacy settings.

only 66% of the applications had privacy policies at all. For those services that did have privacy policies, the majority collect and save all data (e.g. locations, personal information entered into one's profile, and identifying web information such as one's IP address) for an indefinite amount of time. Only one, Mologogo[12] explicitly stated that it deletes GPS data after one month. Another interesting exception is Google Latitude which stores only the most recent location update.[13]

Our review of location-sharing applications reveals that the majority do have some form of privacy controls (76%). However, the majority of those privacy controls are not easily accessible from the main page or home page of the application itself. For the applications we

---

[12] Mologogo. `http://www.mologogo.com/`

[13] Privacy (Google Latitude). `https://sites.google.com/a/pressatgoogle.com/latitude/privacy`

reviewed, over 70% required users to visit or click multiple screens before they reached the privacy settings (see Table 3.1). This lack of immediately accessible privacy controls may be a result of the small amount of screen real estate available to application developers, especially in the case of mobile phones. For example, there was one case (Rummble[14]), included in the “Yes” category for accessible privacy settings in Table 3.1, where the web interface for the system had a link to the privacy controls, but the iPhone interface did not.

The types of privacy controls for the location-sharing applications are the following:

- **Blacklist:** Users are able to block specific individuals from viewing their location. (Found in 15.7% (14) of services.)
- **Friends Only:** This whitelist-based control restricts access to users denoted as a “Friend.” By default, closed systems are considered friends only. (Found in 49.4% (44) of services.)
- **Granularity:** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. “Andrew is in Pittsburgh, Pennsylvania.”) (Found in 11.2% (10) of services.)
- **Group:** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the “college friends” group to view my location.) (Found in 12.4% (11) of services.)
- **Invisible:** This feature may also be termed the “Private,” “Only me,” or “No one” setting. Users continue to send location data, but their locations are not divulged. (Found in 33.7% (30) of services.)

---

[14] Rummble. `http://www.rummble.com/`

- **Location-based rules:** This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as “Work” or select an area on a map, and their location information is revealed to anyone who requests them when they are at that location. (Found in 1.12% (1) of services.)
- **Network:** This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location. (Found in 12.4% (11) of services.)
- **Per-request permissions:** Users must specifically review each location request, and decide whether or allow or deny the request prior to the location being revealed. (Found in 2.25% (2) of services.)
- **Time-based rules:** Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm). (Found in 1.12% (1) of services.)
- **Time-expiring approval:** Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is “live.” During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible. (Found in 2.25% (2) of services.)
- **No restrictions:** Anyone is able to view the user’s location. (Found in 16.9% (15) of services.)
- **Not Applicable:** Privacy controls do not apply. (Valid for 5.62% (5) of services.)

- **Unknown:** We were unable to find information about the privacy controls. (1.12% (1) service.)

In general, we see that the "Friends Only" and "Invisible" restrictions are the most prevalent. Of the 89 applications we reviewed, only four provided explicit notice to the user regarding who had requested their location. Aka-Aki,[15] Locaccino,[16] and Mobiluck[17] provide request logs to the user so they can view "Who's Viewed Me," Sniff[18] sends out a text message notification providing the name of the person making the request, and HeyWay[19] requires the user to explicitly approve or reject each location request (providing the name of the requester making the request). The native Loki browser plug-in explicitly asks the user if an application is making a request can access that information, but does not provider the name of the person making the request. Only one specific application Locaccino[20] had time-based and location-based rules.

3.3 Location-Sharing Risk/Benefit Analysis

We conducted an online survey to understand the magnitude of the risks and benefits associated with location-sharing services.

---

[15] Aka-Aki. `http://www.aka-aki.com/`

[16] Locaccino. Note: the authors of this paper were also involved in the development of this application. `http://www.locaccino.com`

[17] Mobiluck. `http://www.mobiluck.com`

[18] Sniff. `http://www.sniffu.com/`

[19] HeyWay. `http://niftybrick.com/heyway.html`

[20] Locaccino. `http://www.locaccino.org`

3.3.1 Method

For an individual user to accept a technology, an acceptable balance of personal risk and benefits must be established [48]. To understand these risks and benefits, we investigated the perceived-risk attitude or the expected value of location-sharing risks and benefits towards the use of location-sharing technologies. This evaluation takes into account the willingness or likelihood of engaging in the activity as a function of its expected benefit or harm [23]. We conducted an online survey to capture users' perceptions of how likely certain scenarios would be if they used location-sharing scenarios and the magnitude of benefits or risks related to each scenario.

Recruitment

In April 2008, we solicited participants to complete a survey to examine their personal perceptions about location-sharing technologies. Online announcements were posted on the "Volunteers" section of craigslist.com for major metropolitan areas of the United States and in online sweepstakes websites, recruiting individuals over the age of 18. The survey was available online for two weeks. We raffled a $75 Amazon.com gift certificate as the incentive for participation.

Demographics

The final survey sample consisted of 587 respondents. Although 655 people completed the survey, respondents who completed the survey in under 4 minutes were eliminated from the final dataset. Due to the number of questions in the survey, we believed that anyone who answered in under 4 minutes was simply clicking through the survey, rather than reading and responding to the questions. Participants' ages ranged from 18 to 79 years of age (M = 35.7), and 61% were female. The respondents were fairly well educated, with 43.8% indicating that they had college degrees and 29.1% having graduate degrees. In general, most people (72.4%) had heard of technologies that allow people to share their locations with others.

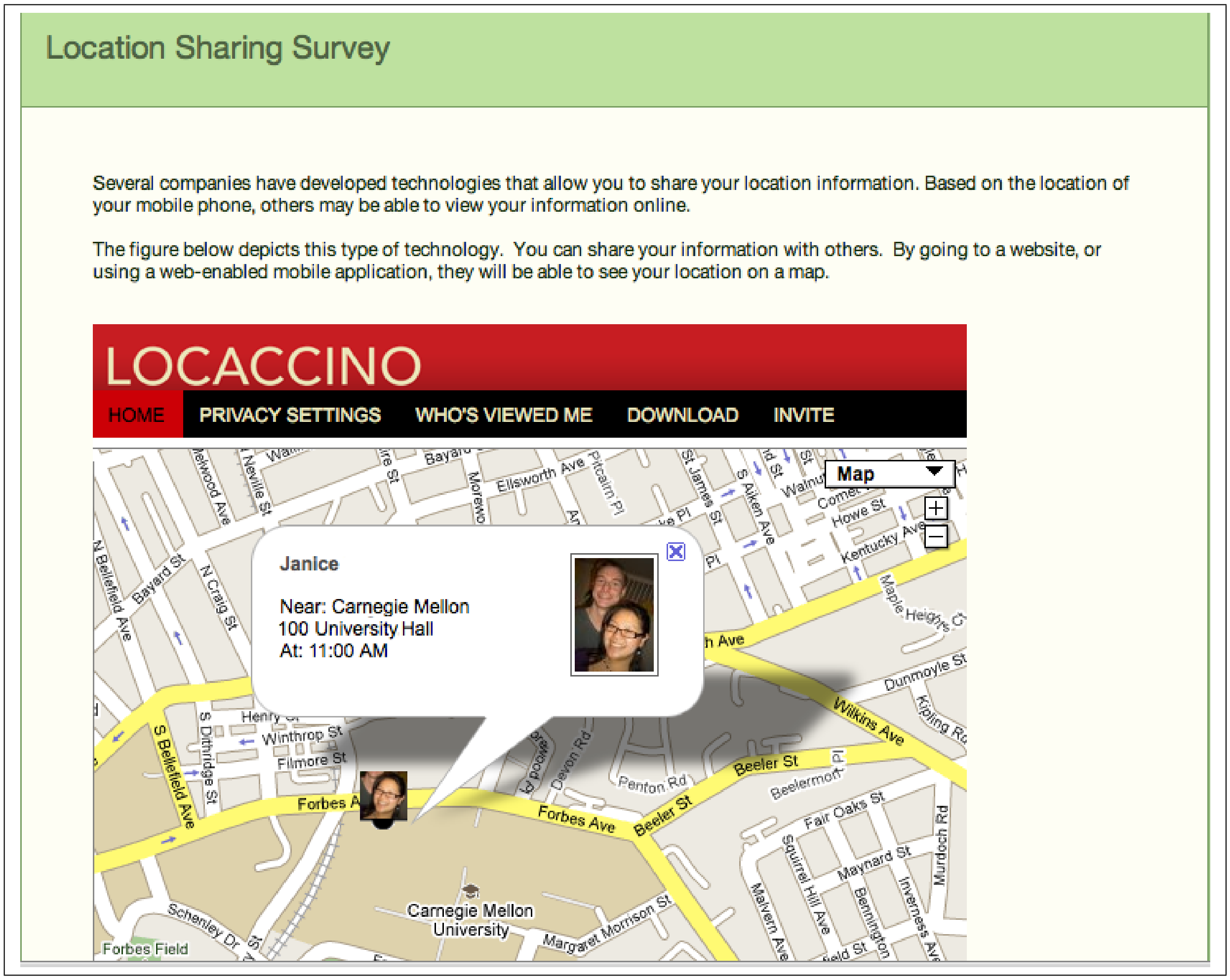
3.3.2 Survey Data Analysis

Technology Use

At the beginning of the survey, an example of an online-location sharing technology was presented to the study participants. A screen shot of of a map with a thumbnail of a person's picture pinpointed on the map was displayed, indicating that the person had been located with this technology (see Figure 3.4). Participants were asked to list some benefits and risks or dangers associated with this technology.

Some examples of benefits listed by our respondents are the following:

- Give out directions quickly to friends and family.
- Able to track loved ones and opportunity to surprise someone for a special event.
- People you know can find you, parents can track their kids, facilitates a rendezvous.
- Serendipitous encounters.



Location Sharing Survey

Several companies have developed technologies that allow you to share your location information. Based on the location of your mobile phone, others may be able to view your information online.

The figure below depicts this type of technology. You can share your information with others. By going to a website, or using a web-enabled mobile application, they will be able to see your location on a map.

Janice

Near: Carnegie Mellon
100 University Hall
At: 11:00 AM

Figure 3.4: The example of a location-sharing interface presented to our survey participants

- Remote awareness of friends and relatives.

Some examples of dangers listed by our respondents are the following:

- Anyone could know exactly where you are - there is no privacy - anyone could find you at any given time.
- If someone intends to do you harm, they would find you easily.

- An unwanted person will find you and stalk you. It is not safe. You have no control.
- Location history could be harvested for stalking or marketing.
- People could find out if no one was home.

Respondents were asked a series of 7-point Likert scale questions asking them to rate the usefulness of location-sharing technologies (ranging from *not useful* (1) to *extremely useful* (7)), their privacy concerns surrounding their use of these technologies (ranging from *not concerned* (1) to *extremely concerned* (7)), and the risk of using these applications (ranging from *the risk far outweighs the benefit* to *the benefit far outweighs the risk*). These questions were asked both at the beginning and end of the survey to determine if participating in the survey altered users' opinions.

The results reveal that people's first impression of location-sharing technologies is that they are mostly not useful. After taking the survey, which included various usage scenarios, people's opinions changed slightly, and they found the technology slightly more useful. They also became more concerned about allowing others to view their locations at the end of the survey. Participants' attitudes about the risk of using location-sharing technologies slightly outweighing the benefits did not change: they felt that the risk still outweighed the benefits. See Table 3.2 for mean values and paired t-test p values.

In the survey, we also asked participants about how concerned they were about controlling access to their location on a scale of *not concerned* (1) to *extremely concerned* (7). We found that participants were extremely concerned about having control (M = 6.17).

We also asked participants to rate the likelihood of the use of location-sharing tech-

Item	Before	After	t statistic	p value
Usefulness	3.72	3.94	-3.91	$<$**0.001**
Concern	5.15	5.42	-4.66	$<$**0.001**
Risk	3.27	3.33	-1.01	0.31

Table 3.2: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful*) (7), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), and the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the beginning and end of the survey. The degrees of freedom for the paired t-tests is 586.

Item	M	t statistic	p value
You	3.84	-1.84	0.07
Family	3.67	-3.78	$<$**0.001**
Friends	4.30	4.05	$<$**0.001**
Company/Employer	3.63	-4.52	$<$**0.001**

Table 3.3: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)). The responses are compared in a t-test to the midpoint (4). The degrees of freedom for the t-test are 567.

nologies by him or herself, their family, their friends, or their company or employer. Based on a 7-point Likert scale ranging from *very unlikely* (1) to *very likely* (7), we find that people think it is unlikely that their families and employers will use location-sharing technologies. As for themselves, they are neither likely nor unlikely to use the technologies, but think that they friends are more likely to use these types of applications. The responses to this question and their comparison to the midpoint of the scale are summarized in Table 3.3.

Gender Differences

Dividing participants by gender, we see that men find location-sharing technologies slightly more useful than women do, but men still find these technologies neither useful nor useful.

Item	Female	Male	t statistic	p value
Usefulness	3.77	4.20	-2.78	**.006**
Concern	5.60	5.14	3.73	$<$**0.001**
Risk	3.07	3.72	-4.19	$<$**0.001**
Likeliness of Use	3.56	4.26	-3.8	$<$**0.001**

Table 3.4: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful* (7)), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the end of the survey, and the likeliness of use by the respondent. The degrees of freedom for the two-sample t-tests is 585.

Women are also much more concerned with allowing others to view their locations, tend to feel that the risk of using these technologies far outweighs the benefit, and do not find it likely that they will use these technologies. These responses are detailed in Table 7.1.

Scenarios

Participants rated the likelihood of the occurrence of the scenarios below on a Likert scale from *very unlikely* (1) to *very likely* (7). Scenarios were divided into risks or benefits. For each risk, participants were asked to rate each item from a scale from *not harmful at all* (1) to *extremely harmful* (7), and to rate the benefits on a scale from *no benefits at all* (1) to *great benefit* (7). The responses are detailed in Table 3.5 and Table 3.6.

There were several scenarios in which people would be extremely likely to benefit from such services: finding people in an emergency, finding information based on location, and finding their children. Based on the survey results, people also seem to realize that these applications will likely open them up to receiving advertisements based on their location, being intruded upon, and accidentally revealing the location of their homes.

Scenario	Likelihood	Benefit
Finding people in an emergency	5.64	5.97
Finding information based on your location	5.29	4.99
Keeping track of the location of children in your family	5.17	5.18
Checking people's locations to make sure they are ok	4.98	5.05
Finding nearby friends for social activities	4.76	4.36
Using people's locations to coordinate a meeting	4.67	4.34
Keeping track of elderly relatives	4.66	5.11
Keeping track of where you've been	4.65	3.84
Coordinating family activities	4.59	4.39
Finding a coworker who is running late for a meeting	4.42	4.03
Coordinating ride sharing or carpooling	4.38	4.29
Having fun with locations	4.35	3.47
Recruiting people to participate in activities	4.01	3.83
Finding new people with similar interests	3.49	3.46

Table 3.5: Benefits-based location-sharing scenarios and their likelihood and magnitude of benefit ratings based on survey results, ordered by highest likelihood.

Level of Privacy Concern

We sought to determine the level of privacy concerns that people perceive when they are sharing their information online by asking several privacy scale questions. These privacy scale questions are based on an instrument developed by Malhotra et al. to measure Internet Users' Information Privacy Concerns (IUIPC) [77]. The IUIPC scale defines several groupings of concern, including control, awareness of privacy practices, collection of information, errors, unauthorized secondary use, improper access, and global information privacy concern; and consists of 27 questions. Based on a pilot test where we correlated the use of Facebook, an online social network, and the use of its privacy settings, we selected a sampling of 6 questions. Based on these questions, we calculated a "Privacy score" for each respondent. This score is an average of the ratings of the following six statements presented to the users, rated on a 7-point Likert scale, ranging from *strongly*

Scenario	Likelihood	Harm
Being bothered by ads that use your location	5.27	4.68
Having people intrude on your private space	5.15	5.51
Revealing the location of your home	5.11	5.93
Being found by someone you don't want to see	5.10	5.56
Being found when you want to be alone	5.07	5.08
Revealing activities you are participating in	4.83	4.17
Being stalked	4.75	6.32
Having the government track you	4.62	5.38
Being judged based on your location	4.35	4.50
Having your boss spy on you	4.21	5.15

Table 3.6: Risk-based location-sharing scenarios and their likelihood and magnitude of harm ratings based on survey results, ordered by highest likelihood.

disagree (1) to *strongly agree* (7). The higher the privacy score, the more concerned the person is about their privacy.

Participants were asked to rate the following statements:

- It is very important to me that I am aware and knowledgeable about how my personal information will be used. (IUIPC Awareness)
- I'm concerned that online companies are collecting too much personal information about me. (IUIPC Collection)
- Online companies should have better procedures to correct errors in personal information. (IUIPC Errors)
- Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information. (IUIPC Unauthorized secondary use)
- Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers. (IUIPC Access)

- I am concerned about threats to my personal privacy today. (IUIPC Global Concern)

To determine if this scale was internally reliable, we compute a Cronbach's α score for this set of questions. This statistic allows us to determine if the items, together, measure a consistent viewpoint. A set of items with a Cronbach's α score of above 0.70 is considered to be reliable. We found this 6-item scale for assessing users privacy concerns regarding online companies to be reliable, with a Chronbach's α of 0.85.

To determine if the privacy score had any relation to users' use and perceptions of location-sharing technologies, we examined their correlations. We see that the higher the privacy score, the more likely it is that users will feel that the risks of using location-sharing technologies outweigh the benefits (Risk After, r(586) = -0.23, p <.0001); that they would be less likely to use such technologies (r(586) = -0.12, p = 0.004); and feel that this technology is not useful (Usefulness After, r(586) = -0.11, p = .007). Additionally, users with higher privacy scores were older (r(586) = 0.23, $p < .0001$), more concerned about privacy (Concern After, r(586) = 0.41, $p < .0001$), and more concerned about controlling access to their location(r(586) = 0.39, $p < .0001$).

Expected Values of Risks and Benefits

To examine the ranking of the scenarios, we computed an expected value for the risk variable by multiplying the likelihood perceptions by the magnitude of the risk (harms) or benefit. This value allows us to compare within the sets of scenarios that are considered harms and those that are considered benefits.

Ranking	Scenario
1.	Finding people in an emergency
2.	Keeping track of the location of children in your family
3.	Finding information based on your location
3.	Checking people's locations to make sure they are ok
3.	Keeping track of elderly relatives
4.	Finding nearby friends for social activities
4.	Using people's locations to coordinate a meeting
4.	Coordinating family activities
5.	Coordinating ride sharing or carpooling
5.	Discovering that a friend from out of town is visiting
6.	Keeping track of where you've been
6.	Finding a coworker who is running late for a meeting
7.	Recruiting people to participate in activities
7.	Having fun with locations (e.g. games, pranks)
8.	Finding new people with similar interests

Table 3.7: The relative rankings of benefits obtained from the use of location-sharing technologies.

Within each set of harms and benefits, the expected value for the risk (or benefit) of each was compared to the other harms or benefits with paired t-tests to determine which scenarios are significantly distinct from each other ($p < 0.05$). The relative rankings for the benefits and risks as determined by their expected value are summarized in Table 3.7 and Table 3.8.

Evaluating each expected benefit, one sees that, by far, the most significant benefit is being able to find people in an emergency. The next distinct benefit is being able to track one's children. Finding information based on one's location, checking to see if people are ok, and tracking relatives are the third set of distinct benefits. The least valued expected benefit of location-sharing technologies is finding new people based on one's location.

The greatest expected harms derived from the use of location-based technologies are revealing one's home and being stalked. People perceive that being found by people one

Ranking	Scenario
1.	Revealing the location of your home to people you do not want to give your address to
1.	Being stalked
2.	Having people intrude on your private space
2.	Being found by someone you don't want to see
3.	Being found when you want to be alone
3.	Having the government track you
3.	Being bothered by ads that use your location
4.	Having your boss spy on you
5.	Revealing activities you are participating in
5.	Being judged based on your location

Table 3.8: The relative rankings of risks related to the use of location-sharing technologies.

wants to avoid and having others intrude on one's personal space are the next set of situations associated with these technologies. Being found when one wants to be alone, being tracked by the government, and receiving ads based on one's locations are the third set of distinct harms. It seems that people are the least bothered by the risks of being judged based on one's location and revealing activities that one is participating.

Analysis of participants with children

One potentially useful scenario for location-sharing technologies is keeping track of children in one's family. We asked participants to list the number of children they had, and divided our participants into two categories: those who have children and those who do not. The group with children includes those with adult children. Demographics are summarized in Table 3.9. We see that having children does have an impact of one's perceptions of these technologies.

Participants with children rated location-sharing technologies significantly more useful

Item	Without Children	With Children
Gender	Fem: 218, Male: 147	Fem: 140, Male: 82
Avg. Age	30.9	43.7

Table 3.9: Participants characterized by whether or not they have children or do not have children.

Item	Without Children	With Children	t statistic	p value
You	3.67	4.11	24.01	$<$**0.001**
Family	3.32	4.26	28.36	$<$**0.001**
Friends	4.27	4.36	26.52	$<$**0.001**
Company/Employer	3.48	3.87	26.21	$<$**0.001**

Table 3.10: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)) for people without children and with children. The degrees of freedom for the t-test are 585.

at the beginning of the survey as compared to participants without children ($M_{WithChildren}$ = 3.93 vs. $M_{WithoutChildren}$ = 3.59, t(585) = -2.17, p = 0.03). After taking the survey, both groups felt the same about location-sharing technologies being neither useful nor not useful ($M_{WithChildren}$ = 4.08 vs. $M_{WithoutChildren}$ = 3.85, t(585) = -1.5, p = 0.13).

When asked about the likelihood of use of these types of technologies, participants with children were significantly more likely to feel that they, their families, friends and employers would be likely to use these technologies as compared to people without children. See Table 3.10 for details of survey results and t-tests.

Examining the scenarios responses, we see that participants with children derived greater expected benefit from the following scenarios: checking people's locations to make sure they are ok, coordinating family activities, keeping track of the location of children in your family, keeping track of elderly relatives, and finding new people with similar interests. Those with children also had a greater amount of expected risk from being bothered by

Item	Without Children	With Children	t statistic	p value
Okayness Checking	25.0	29.9	-4.06	$<$**0.001**
Coordinating Family Activities	20.5	26.1	-4.65	$<$**0.001**
Tracking Children	26.1	34.6	-6.18	$<$**0.001**
Tracking Relatives	24.2	29.9	-4.12	$<$**0.001**
Finding New People	13.0	16.0	-2.8	**0.005**
Bothered by Ads	24.7	27.7	-2.35	**0.02**
Tracked by the Government	25.3	28.0	-1.98	**0.05**
Revealing One's Activities	20.1	22.4	-2.08	**0.04**

Table 3.11: Participants' expected benefits and risks based on if they have children or if they do not have children. The values were calculated by multiplying the likelihood ratings of each secenario with its rated risk and benefit. Degrees of freedom for the two-sample t-tests are 585.

ads that use their location, being tracked by the government, and revealing activities they are participating in. These differences are detailed in Table 3.11.

For respondents with children, being able to track their kids becomes the top benefit, tied with being able to find people in an emergency. Even when we control for age and gender, we find this to be the case.

3.4 The Ability of LBS Applications to Address Users' Perceived Risks

As location-based services proliferate in numbers but not in users [36, 79], we examined the ability for these applications to address users' privacy concerns. The number of applications has been increasing and companies have developed platforms that make it easier for others to create applications that leverage location information. Based on the results of our survey, we see that people do not yet understand the value of these location-sharing technologies, and people are still concerned about their privacy when sharing their locations online. In general, people still believe that the risks of location-sharing outweigh the benefits.

Based on our analysis of the risks associated with these technologies, we now examine the existing privacy controls of these technologies and investigate the ways in which these controls can address users' major concerns. We also suggest additional methods of addressing users' concerns.

3.4.1 Addressing risks with privacy controls

To determine if privacy controls are effective in location-sharing technologies, we first examine users' greatest expected risks.

As enumerated in Table 3.8, we see that the top ranked expected risks are the following:

- Revealing the location of your home to people you do not want to give your address to
- Being stalked
- Having people intrude on your private space
- Being found by someone you don't want to see
- Being found when you want to be alone.
- Having the government track you.
- Being bothered by ads that use your location .

Below, we examine how location-based applications' privacy controls address these concerns.

Blacklist: With blacklists, users are able to block specific people with whom they do not wish to reveal this location. This restriction allows users to protect against revealing the location of their homes, block known stalkers and people they do not wish to see. If users are active in managing and updating their blacklists, they may also reduce the ability to having people intrude on their space, and avoid being found when they want to be alone. Unfortunately, in the last two cases, users must spend the effort and time to add people to a blacklist, and must remember to remove people from the blacklist once they want to be found again.

Friends Only: By solely allowing all friends to access users' locations, this protects users from being stalked (users may remove their stalkers from their friend lists). Unfortunately, this control does not protect from being found by friends when one wants to be alone or being found by someone who is a friend, but whom you may not wish to see. To deal with these concerns, users may manage their friend lists by adding and removing friends as they see fit.

Granularity: Allowing the location-sharing application to only provide general information (e.g. neighborhood, city, or state) about one's location mitigates the risks (except for being bothered by ads and and being tracked by the government). Unfortunately, by only providing a wide range of possible locations, this also negates the benefits provided by location-sharing applications.

Group-based rules: Allowing people access to your location by dividing them into groups mitigates several privacy concerns. These group-based rules allow users to protect the location of their homes, to hide themselves from stalkers, and to avoid people they do not want to see. Based on how large one's group is and how active they are in assigning people to groups may also reduce, but not eliminate the risks of having people intrude on their private space and being found when they want to be alone.

Invisible: By going invisible, the user reduces the risks listed above except for that of being bothered by location-based ads and government tracking. The user can significantly reduce the risk of being stalked or of being found by people they don't want to see, but they also reduce the benefits of these services. To most effectively deal with the risks, they must be very active in turning invisible mode on and off, which places a significant burden on the user.

Location-based rules: Defining access by location allows the user to effectively protect the location of his home or spaces in which one needs private space or alone time. These rules may also block known stalkers at locations they do not wish to reveal. By continuously updating these rules, users may effectively address most of the risks, but this requires users to regularly update their rules.

Network: A network is typically larger than a group (e.g. the Carnegie Mellon network). This may make it easier for users to define rules, but may not be an effective means in protecting them from the risks listed above. By defining network based rules, one prevents the general public from locating them, but may not keep stalkers within their network from finding them, or it may not prevent others from finding the location of their home, or preserving their personal space and alone time.

Per request permission: Requiring users to approve of each location request reduces the risks listed above except for that of being tracked by the government and being bothered by ads. Unfortunately, this method requires that users be interrupted, and this may become too burdensome on the user.

Time-based rules: Basing restrictions on time allows users to create restrictions to protect the locations of their homes (assuming they are home at regular times). Time-based restrictions can also protect users from being intruded upon, being found, and allows them to be be alone at certain times of day or days of the week.

Time-expiring approval: Allowing users to specifically permit others to locate them mitigates most risks (excluding government tracking and being served with advertisements based on their location). Unfortunately, allowing users to be the only ones to "push" location information also negates most of the top benefits of location sharing (e.g. one would not be able to find someone in the case of an emergency when they need to wait for the user to make his location available for a small period of time).

No restrictions: Having no rules allows users to be located by anyone. This opens them up to all the benefits as well as the risks of using location-sharing technologies.

We see that the rules that allow users to mitigate the greatest risks are the following:

- Blacklist
- Granularity
- Group-based rules
- Location-based rules

- Time-based rules

Each of these rules alone, including the burden on the user, does not address the largest expected risks of using location-sharing technologies. We find that location-sharing technologies offer limited flexibility in their privacy controls. It is rare that systems give users the ability to specify expressive rules to control the sharing of their location information. Furthermore, there are no commercially available systems that offer anywhere near as powerful a control set as one could imagine: with the ability to specify rules based on specific users and groups of contacts, to control access based on time and location, to return locations at varying granularities, and to become invisible or obfuscate locations in extreme situations. There is one system, Locaccino, developed by the authors at Carnegie Mellon, that offers time, location, and group based rules, as well as invisibility. A combination of all of these rules would be the most effective in addressing users' privacy concerns.

Another factor that has been mentioned briefly is user burden. In some cases, it would be possible for the user to toggle being invisible on and off all day, based on that day's events. Unfortunately, in our experience, people easily forget to do this. Once the location-sharing software is up and running, it is easier to leave it running; otherwise, once people go offline or invisible, they are likely to leave the software in that setting. Similarly, in systems that do offer a myriad of privacy controls, methods must be developed to help users create rules based on their daily schedules, and regular and irregular interactions with others.

3.4.2 Discussion and Limitations

By defining the relative value of users' expected risks and benefits regarding the use of location-sharing services, we develop an understanding users' privacy concerns. We see that, in general, industry guidelines do not address these concerns, and the privacy controls in existing applications do not comprehensively address these concerns. In this paper, we have provided recommendations for sets of privacy control that may assist developers in addressing users' privacy concerns.

Based on the current perceptions of benefits and harms of location-sharing technologies at this time (noting that perceptions of risks in this area may evolve or shift), the primary risks can be addressed or mitigated by the design of the location-sharing technology. Based on the current restrictions offered by location-sharing technologies, we find that these risks may not be addressed, in full, by the current palette of available privacy controls. Instead, location-sharing applications may want to consider making more expressive privacy controls available to their users. With more expressive controls, people may become more comfortable with sharing their location information and find more value in these services. Additionally, future work must be done to determine how to reduce user burden. A balance must be found between expressiveness and usability or with offering users complex and detailed privacy controls and making these controls easy to use.

Another matter to consider is that of users' evolving privacy concerns. Currently, we find that users' still do not find location-sharing services useful. This may be due to the lack of usage in general. Without a critical mass of users, current users are unable to reap the benefits of being able to find their friends or to track family members. As more and more people adopt these types of technologies, and peer opinion about these technologies becomes more favorable, the level of concern that people feel may diminish. Additionally, we find that it is younger people or people with children who are more interested in location-sharing applications and are more likely to adopt these services.

New technologies continue to be introduced. One limitation of this study is the number and type of location-sharing applications we have reviewed. We did not consider technologies where the person being requested had no knowledge of the fact that they are sharing their location information or no control over the ability to disable these technologies. These technologies include ones that allow you to “spy" on a spouse, monitor your employees, or track your children. The privacy of people being tracked in these situations is typically not a consideration, and these people have no access to any privacy controls, whatsoever.

Chapter 4

Location-Sharing Feedback Study I (Locyoution)

This chapter is largely a reproduction of a paper co-authored with Patrick Gage Kelly, Paul Hankes-Driesma, Lorrie F. Cranor, Jason Hong, and Norman Sadeh [116]. This work is funded in party by the National Science Foundation under Cyber Trust grant CNS-0627513 and by the Army Research Office contract no. DAAD19-02-1-0389 to Carnegie Mellon University's CyLab. Additional support has been provided by Microsoft through the Carnegie Mellon Center for Computational Thinking, FCT through the CMU/Portugal Information and Communication Technologies Institute, and through grants from FranceTelecom and Nokia.

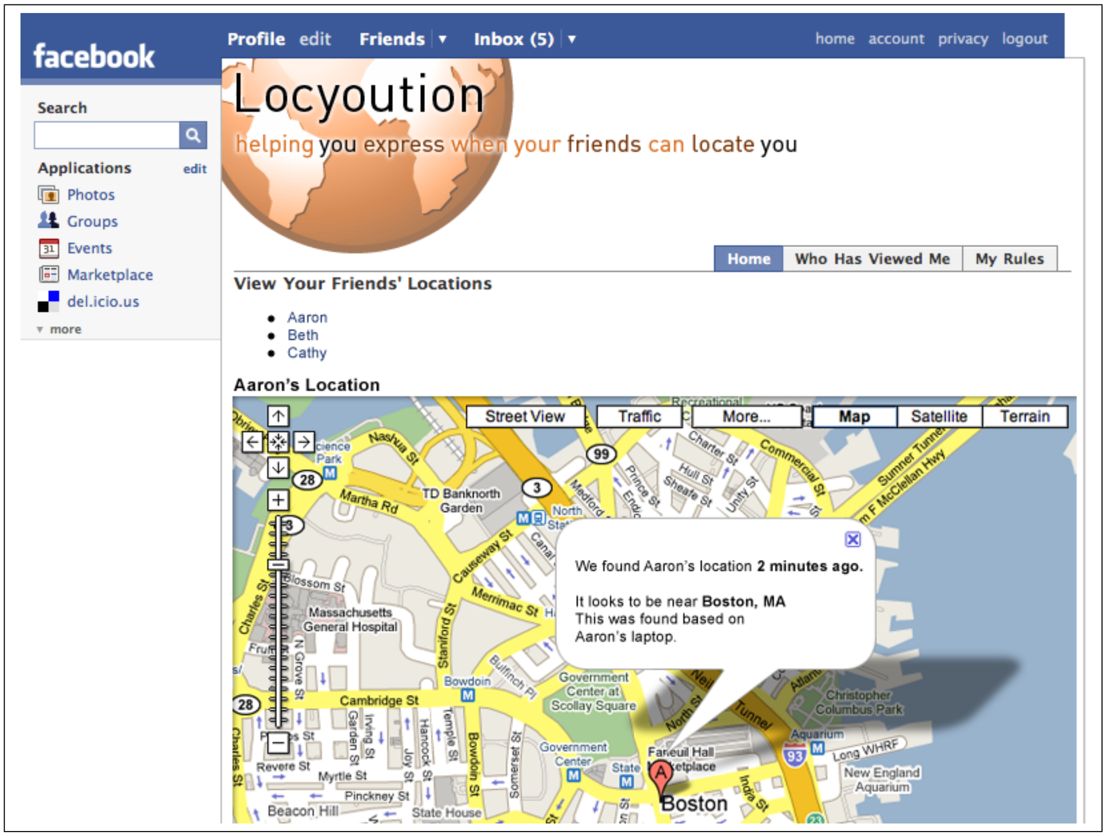
Due to the impact of privacy concerns on the use of location-sharing technologies, I investigated the role of feedback, or knowing who has requested one's location, on users' levels of comfort with using Locyoution, a location-sharing system. In this system, users could create time-based rules specifying when they could be located. Locyoution users interface with the system via Facebook, an online social network. Participants were recruited to use Locyoution for a month, and were divided into two conditions: a group without feedback (the control), and a group with feedback. Participants' privacy concerns were reduced after using the mobile location sharing system. Participants with feedback became more comfortable with being located by friends and strangers. Additionally, the results of the study suggest that peer opinion and technical savviness contribute most to whether or not participants thought they would continue to use a mobile location technology.

4.1 Technology

Locyoution is our Facebook interface for a mobile location-sharing application developed by the CMU Mobile Commerce Lab built on PeopleFinder [96] technology. It consists of two main pieces of technology: software that users install on their laptops and an application that is added on Facebook. By using Facebook, we leverage a social network of which participants are already a part [83, 91].

In Locyoution, the user interaction primarily occurs with the Facebook application. We refer to participants in this study as Locyoution users. Locyoution benefits from iterative improvements to the PeopleFinder system based on feedback collected from several other pilots of the technology over the previous two years [96].

PeopleFinder determines a user's location based on the WiFi access points in range, leveraging technology created by Skyhook Wireless. The Skyhook database provided generally accurate information for the city and covered the majority of the city. We also maintain



Locyoution

helping you express when your friends can locate you

View Your Friends' Locations

- Aaron
- Beth
- Cathy

Aaron's Location

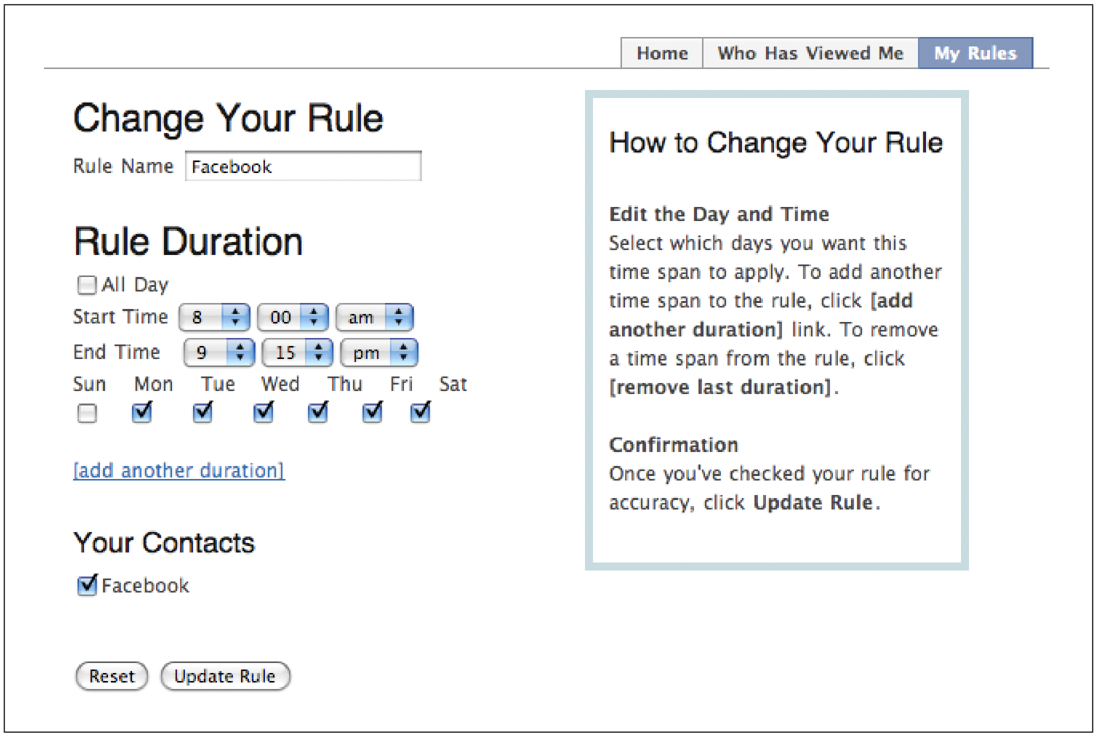
We found Aaron's location **2 minutes ago.**

It looks to be near **Boston, MA**
This was found based on
Aaron's laptop.

Figure 4.1: The Locyoution "Home" interface, displayed in Facebook. It shows, by default, the user's own location, and presents a list of friends using Locyoution. This allows users to quickly query their friends locations without having to navigate to each of their Facebook profiles individually.

a database of the buildings and room numbers of all WiFi access points on the university campus. When the Locyoution user is on campus, the building and room number information is listed on the user's map.

When people wish to check a Locyoution user's location, they must go to that user's Facebook profile and click on the icon for the Locyoution application. They then are able to view a map of that user's exact location (address, city, and state), subject to the rules that the user has defined.



Change Your Rule

Rule Name: Facebook

Rule Duration

☐ All Day

Start Time: 8 : 00 am

End Time: 9 : 15 pm

Sun	Mon	Tue	Wed	Thu	Fri	Sat
☐	☑	☑	☑	☑	☑	☑

[add another duration]

Your Contacts

☑ Facebook

How to Change Your Rule

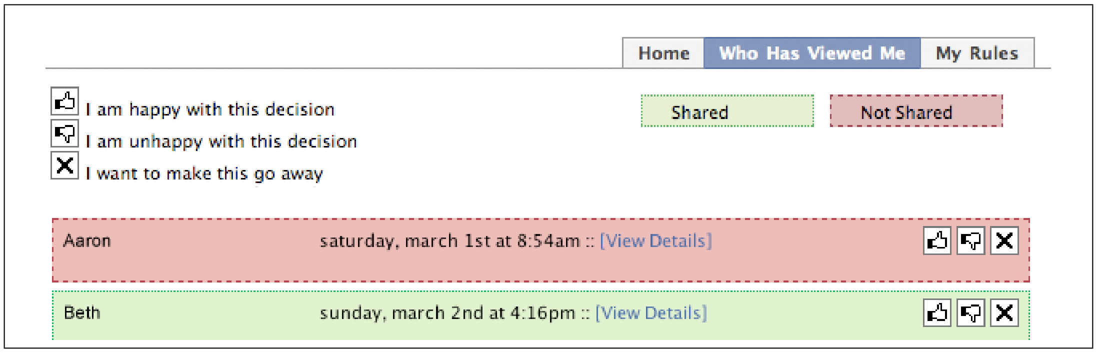
Edit the Day and Time
Select which days you want this time span to apply. To add another time span to the rule, click **[add another duration]** link. To remove a time span from the rule, click **[remove last duration]**.

Confirmation
Once you've checked your rule for accuracy, click **Update Rule**.

Figure 4.2: The Locyoution "My Rules" interface

4.1.1 User Interface

The Locyoution Facebook interface consists of three main areas. The first area, “Home,” is viewable by Locyoution users as well as by anyone on Facebook. The other two areas, “My Rules” and “Who Has Viewed Me,” are only viewable by Locyoution users. Locyoution users are provided with a username and password so that they authenticate with the system once they add the Facebook application, linking their laptop software with their Facebook account.



👍 I am happy with this decision
👎 I am unhappy with this decision
☒ I want to make this go away

Aaron saturday, march 1st at 8:54am :: [View Details] 👍 👎 ☒

Beth sunday, march 2nd at 4:16pm :: [View Details] 👍 👎 ☒

Figure 4.3: The Locyoution “Who Has Viewed Me" interface.

4.1.2 Home Screen

After the installation of the Locyoution software and Facebook application, the user is presented with the Locyoution home screen on Facebook, as shown in Figure 4.1. This screen has four elements. Common across all interface areas are the first two elements: the Locyoution title bar and logo, followed by a set of tabs. These tabs, in the Facebook style, allow for navigation between pages. The final two elements, which appear only on the home screen, are the Friends with Locyoution list and the map. The Friends with Locyoution list is the user’s friends who have the Locyoution application installed; and, thus, can have their locations queried.

The map shows the location of any person that a user selects from their list. If they have not yet located another user, it will show them their own current location. Locyoution allows a small degree of plausible deniability. Location requests can be denied for two reasons: the locatee is offline, or has a rule that does not allow for the disclosure of his or her location. If the request is not a success, the user is presented with a message which simply indicates that the requestee’s location is not available at that time.

4.1.3 Rules Screen

From the tabbed navigation area, Locyoution users can return Home or to go edit or view their rules via the “My Rules” tab. The Rules interface (Figure 4.2) allows users to control when others can view their location.

Rules in Locyoution are solely time-based rules, e.g. Only show my location between 9 am and 6 pm on Mondays and Wednesdays. Users can define rules based on specific days of the week and a combination of times of the day. Participants may also add additional durations to rules.

When a location request is made, that request is passed to the server, and if the request falls within the allowable period, the map location is passed back to be displayed on the Home screen; otherwise, the “unavailable” message will be displayed on the Home screen.

Due to limitations at the time of the study, we were unable to allow users to create group-specific rules. While Patil and Lai have found that people like defining permissions by group [89], being able to use Facebook, a social community with which that they are already familiar, was worth the tradeoff of group rule-defining functionality. Facebook has recently added functionality to define settings and permissions based on “Friend Lists."

4.1.4 Who Has Viewed Me

The final tab in the Locyoution interface allows users to see who has viewed their location as a history or audit log, as shown in Figure 4.3. When a Facebook user clicks on the Locyoution map graphic on a Locyoution user’s profile page, the identity of the requester is recorded. Additionally, the time of the request, the Locyoution user's location, and the system's decision are stored.

Users can view the location requests made of them, and each request is colored green or red based on whether or not their location was displayed to the requester. Locyoution users can also indicate their satisfaction with the decisions of the system by clicking the "Thumbs Up" or "Thumbs Down" buttons, styled after Facebook's system wide user satisfaction mechanism.

4.1.5 Facebook Privacy Settings

Facebook itself also provides a comprehensive set of controls for users to protect their privacy. Users are able to change the privacy settings for their applications to restrict who is able to view the application on their profile page. Users of Locyoution can restrict the Facebook application privacy settings to "My Networks & Friends," "Some Networks (which the user selects) and Friends," or "Friends Only." For actual usage of this feature see Table 4.3. The default setting for Locyoution allowed all networks & friends to access Locyoution.

4.2 Locyoution Study

We examined the use of Locyoution in a field investigation. Participants, solicited from a university population, were asked to install and use Locyoution over a period of four weeks. The study consisted of four phases: a pre-study questionnaire, Locyoution installation and troubleshooting, Locyoution deployment, and an exit survey. In Phase 1, participants completed a questionnaire and study consent forms. In Phase 2, participants were provided with a Locyoution username and password, and installation tutorials. We provided assistance to anyone who had difficulty installing the software and viewing their location. In Phase 3, participants were asked to use Locyoution. Usage patterns of Locyoution were determined by examining server logs. Finally, in Phase 4, participants completed an exit survey on their experience with Locyoution.

To determine the impact of feedback on the privacy attitudes and adoption of our mobile location application, participants were divided into two conditions:

No Feedback condition: Participants did not receive information about who had requested their location (n = 30).

Feedback condition: Participants were able to view their location disclosure history (n = 26).

4.2.1 Method

We recruited participants from a university population, offering a $20USD online gift certificate as compensation for completion of the study. We posted flyers around campus, and advertised on university mailing lists. We realized that there was a significant potential for participant attrition due to the nature of the study (a field investigation with a relatively “hands-off" approach), and thus recruited a large number of participants. After respondents completed the pre-study survey, we invited 123 users to participate in our study.

To mimic real world usage, participants were provided with online instructions for participation, no physical meetings or lab sessions were conducted. Participation involved downloading and installing the Locyoution software and adding the Facebook application. Users were also provided with a username and password so that they could link their laptop software to their Facebook account.

In the course of the study, we disqualified 6 users for not completing all pre-study requirements and 1 due to a operating system related incompatibility. Additionally, 16 users dropped out: 3 people were unable to get the software to work, 3 people did not have wireless on their laptops, 2 people were too busy to use Facebook, 2 people were too concerned about their privacy to use the technology, and 6 people declined participation for indeterminate reasons. Of the remainder, 75 users added the Facebook application. From this group, 64 were able to successfully use the software and Facebook application. Of those, 56 participated in our active data collection phase of the study. The results discussed in this paper are based on the data analysis of these 56 participants. In our user population, 32.1% were graduate students and the mean age was 22.4 years of age. In the No Feedback condition, 50% of those users were female, and in the Feedback condition, 61.5% are female.

4.2.2 Data Analysis

The duration of the study was 4 weeks: the first two weeks consisted of installation and troubleshooting, during which the majority of participants were away from campus for a week, and the final two weeks consisted of “normal" usage. We kept in touch with participants periodically, sending email reminders about using Locyoution. To the feedback

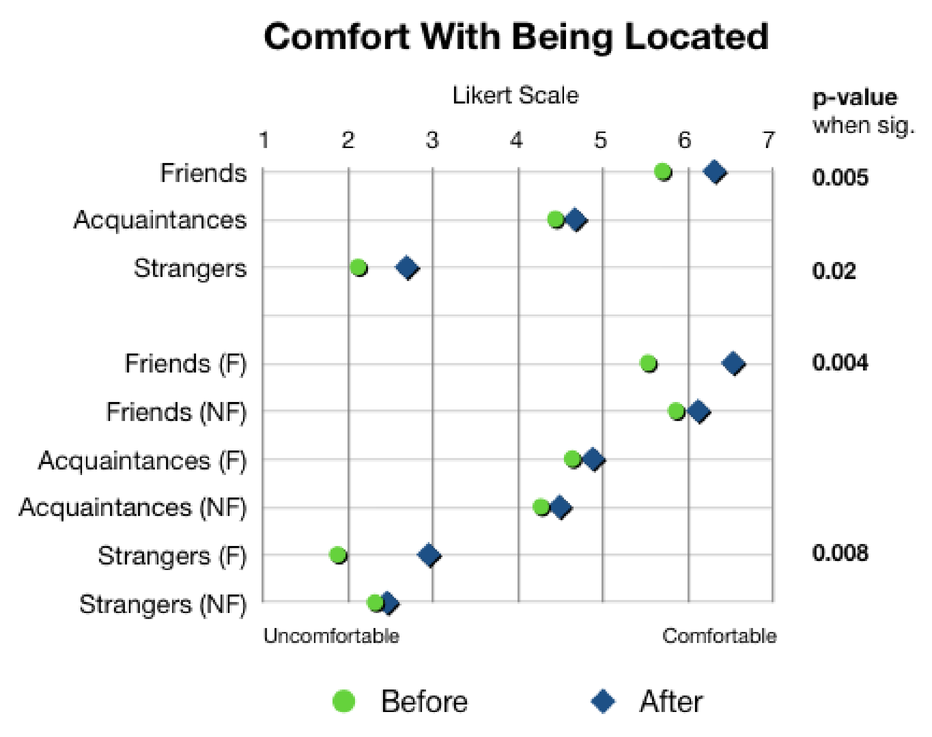


Figure 4.4: Survey results for comfort levels in location-finding. These results are based on a Likert scale from 1 to 7, ranging from not comfortable at all to fully comfortable. For the Feedback condition, participants were less uncomfortable afterwards with allowing themselves to be located by friends and strangers. This explains the statistical significance for both conditions combined (top section), where overall participants are more comfortable with displaying their locations to friends and strangers than they were prior to using Locyoution.

group, we sent information about the "Who Has Viewed You" feature of the application. Our data analysis covers the full 4 weeks of the study.

After the conclusion of the study, we analyzed the usage of Locyoution and the results of the pre-study and exit surveys. We examined differences between the conditions and their privacy attitudes, technology acceptance, and rule usage. In the next sections, we focus on the implications of privacy, feedback, and rule expressiveness.

4.2.3 Usage

A total of 233 requests were made to locate our 56 participants, or about 4 requests per participant. over the main two-week usage period. Of those requests, 43.4% were successful. Between the two conditions, there were no statistically significant differences between the proportion of requests where locations were returned to the requestees, Fisher's exact $p = 0.57$, with 44.9% of resuests being successful in the no feedback condition and 40.3% of requests being successful in the feedback condition.

4.3 Results

4.3.1 Privacy

Participants were asked about the level of concern they had with using a location-sharing application before and after they used Locyoution. We wished to study any differences in perceived privacy concerns before and after participants used the mobile location-sharing technology. In the surveys, users indicated their level of concern using a Likert scale from 1 to 7, ranging from no concern to extremely concerned. Prior to using Locyoution, participants indicated they had moderately high concerns for their privacy, M = 4.63 (99% CI = 4.04 - 5.21). After using Locyoution, the level of concern they had for their privacy (M = 3.96, 99% CI = 3.31 - 4.62) was reduced a statistically significant amount, t(55) = 2.21, p = 0.031. Based on these results, we see that users of Locyoution were concerned about their privacy prior to using the technology, and after a month of usage, participants' privacy concerns were slightly reduced.

	Before	After	t statistic	p value
Friends	5.71	6.32	-2.94	**0.005**
Acquaintances	4.45	4.70	-0.99	0.33
Strangers	2.12	2.70	-2.33	**0.02**

Table 4.1: Comfort levels of being located by certain groups of people before and after using Locyoution. Paired T-tests have a degree of freedom of 55 for each type of relationship. Mean values are based on a Likert scale from 1 to 7, ranging from not comfortable at all to fully comfortable.

To examine the impact of relationships on willingness to share location, participants were asked, prior to the study, about the level of comfort they thought they would have with friends, acquaintances, and strangers finding their locations anytime, at times they had specified, or at locations they had specified. As expected, participants were much more comfortable, in general, with friends finding their locations as compared to acquaintances, and acquaintances as compared to strangers. The differences between each of the types of relationships is statistically significant.

When comparing within each relationship type the period when their location information would be shared, we see that people are the least comfortable with allowing any of the groups to view their locations at anytime. For friends and acquaintances, participants indicated that they had the highest level of comfort sharing their locations using location-based rules. For strangers, participants were equally uncomfortable with allowing access using time-based rules or location-based rules.

At the end of the study, we again asked our participants how comfortable they had been with allowing friends, acquaintances, or strangers view their locations subject to time-based rules. See Table 4.1 for mean values and significance levels and Figure 4.4 for a graphical comparison. For the aggregate dataset, we found that participants, afterwards, were statistically significantly more comfortable with friends and strangers viewing their locations than they had been prior to using the system. While comfort levels for acquaintances also increased, this difference was not statistically significant.

Based on responses to the exit survey, we see the differentiation between privacy concerns in the Feedback and the No Feedback conditions. Participants with feedback were much more comfortable with being located by *friends* and *strangers*, compared to their perceived levels of comfort at the beginning of the study, based on results of paired T-tests by condition. We attribute the statistical significance for the aggregate dataset (Table 4.1) to the change in comfort levels to people in the Feedback condition. For participants who did not receive feedback, we observe that their comfort levels did not change after using the system. See Table 4.2 and Figure 4.4 for these results. Participants in the Feedback condition assumed they would be comfortable with being located by friends based on time-based rules. After using Locyoution, they became much more comfortable about being located by friends. Participants in the Feedback condition were not comfortable being located by strangers, even with time restrictions. After using the system, they became slightly less uncomfortable about being located by strangers at the time allowed by their rules.

In summary:

- People have privacy concerns about sharing their location, but experience with the system slightly reduced their privacy concerns.
- People who had received feedback become more comfortable with sharing their location information with friends and strangers.

	Cond.	Before	After	t statistic	p value
Friends	F	5.54	6.54	-3.14	**0.004**
	NF	5.87	6.13	-1.03	0.31
Acq.	F	4.65	4.89	-0.59	0.56
	NF	4.28	4.5	-0.81	0.42
Strangers	F	1.89	2.96	-2.90	**0.008**
	NF	2.33	2.47	-0.43	0.67

Table 4.2: Comfort levels of being located before and after using Locyoution by condition and relationship type, Friends, Acquaintances (Acq.), and Strangers. Paired T-tests have a degree of freedom of 25 for the Feedback condition and 29 for the No Feedback condition. Mean values are based on a Likert scale from 1 to 7, ranging from no concern to high concern.

- Users in the Feedback condition had a lesser degree of concern for their privacy after using the technology.

4.3.2 Feedback

Based on the pre-study questionnaire, participants were interested in knowing who had looked at their Facebook profiles, M = 5.02 (99% CI = 4.44 - 5.59), (based on a Likert scale from 1 to 7, from not interested at all to extremely interested), but were neutral about how they would feel if others knew they were looking at other people's profiles, M = 3.96, (99% CI = 3.31 - 4.62), (based on a Likert scale from 1 to 7 from not comfortable at all to fully comfortable). As one participant noted, "So, I'm interested in seeing who has seen me, but obviously, I'm concerned [about] them knowing if I looked up their locations." There is lack of reciprocity; wanting information for yourself, but not wanting others to have that same information.

At the end of the study, we surveyed the Feedback condition on their experiences and opinions of the "Who Has Viewed Me" feature. To the No Feedback condition, we presented screenshots of the “Who Has Viewed Me" interface to solicit their viewpoints on the future inclusion of such a feature. The majority of people in both conditions wanted feedback (76.9% of those who had it were happy they did and 83.3% of those who did not have it wanted it, Fisher’s Exact $p = 0.58$). Only one person in the Feedback condition would have preferred an opaque system.

We asked our participants if knowing who had viewed them made them or would have made them more willing to share their location with others. For those in the Feedback condition, having feedback made them more willing to share their location (84.6%). Fewer people in the No Feedback condition thought having feedback would make them more willing to share their location (56.7% were willing, 23.3% were not willing, and 20% were unsure). These differences were marginally significant, Fisher’s exact p = .09.

In summary:

- In general, people want to know who has been viewing them. But, for those who did not receive feedback, more people were unwilling or unsure if they would be more willing to share their locations with others.
- The desire to know who has been viewing one’s profile is compelling enough that participants would be willing to trade in an opaque system to have it.

4.3.3 Rule Expressiveness

To examine the impact and usability of rules, we asked people to rate the usefulness of time-based rules and to provide feedback on other types of rules. Participants, in general, indicated that they were able to easily create and define rules (M = 5.4, 99% CI = 4.79 - 5.9), they were confident that their rules represented their privacy preferences (M = 5.3, 99% CI = 4.73 - 5.77), and most were confident that the rules worked (M = 5.53, 99% CI = 4.87 - 5.43). When asked if time-based rules provided enough control (M = 4.95, 99% CI = 4.47 - 5.42), most agreed.

Users were also asked about their likelihood of using additional types of rules. We found that users say they are likely to use rules based on groups of people or friend lists, (M = 5.88 (99% CI = 5.48 - 6.27) and location based rules (M = 5.45 (99% CI = 4.86 - 6.03). Means are based on a Likert scale from 1 to 7 ranging from very unlikely to very likely. Users said they were less likely to use proximity, making one's location available to people within 1 mile of you, and granularity-based rules, displaying only the city or state of their current location, ($M_{granularity}$ = 4.34, 99% CI = 4.96 - 3.72; $M_{proximity}$ = 3.68, 99% CI = 3.13 - 4.23).

Another type of rule that several users requested was that of being able to “include/exclude specific people rather than networks." These whitelists or blacklists would allow users fine-grained control over who is able to see their location information. Having the ability to restrict a mobile location technology to actual, real friends, yet still use the convenient medium of Facebook may also have a significant impact on reducing privacy concerns and encouraging the continued use of such an application.

Examining participants' use of Facebook's application-based privacy settings, we see that the majority of participants (51.8%) used the default setting of allowing “All of their networks and friends" to view the Locyoution application in their profile. The other large

	Feedback	No Feedback
All Networks/Friends (Default)	57.7%	46.7%
Some Networks/All Friends	7.69%	3.33%
Only Friends	34.6%	50.0%

Table 4.3: The Facebook-based application privacy settings used by participants in the Feedback and No Feedback conditions. The differences in proportions are not statistically significant, Fisher's exact p = 0.22.

proportion of users (42.9%) changed this setting so that only “Friends" could use Locyoution to locate them. Differentiating by condition, a greater proportion of people in the No Feedback condition set their Facebook privacy settings to that of “Friends Only," but the differences in proportions are not statistically significant. See Table 4.3 for the proportions and privacy settings for each condition.

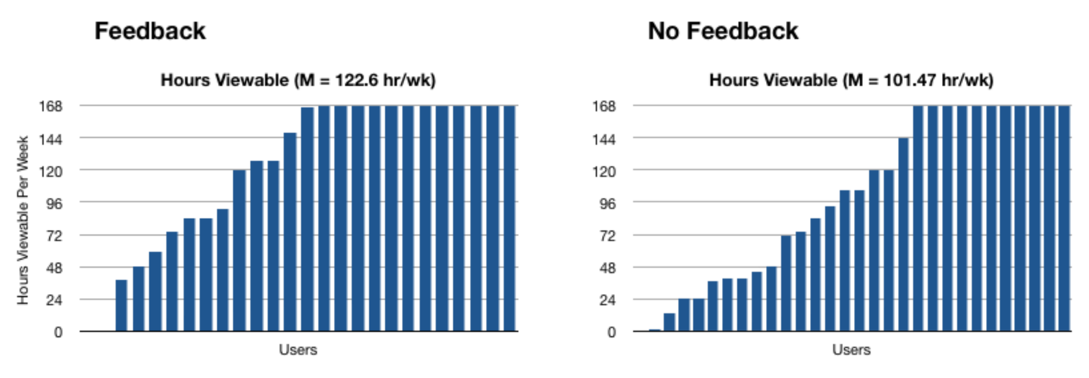


Figure 4.5: The number of hours per week that a user's rules allowed him or her to be viewable at the conclusion of the study are displayed above split by the Feedback and No Feedback conditions.

After the conclusion of the study, we examined the users' final rules, per condition, to evaluate how “open" the rules were in terms of number of hours that users allowed themselves to be found. The average number of hours that participants in the Feedback condition made themselves available (M = 122.7 hours) is greater than that in the No Feedback condition (M = 101.5), see Figure 4.5; but the differences in the one-sided T-test

(p = 0.096), are only marginally significant. It may be that people who have feedback made themselves available for a greater number of hours because they are more comfortable with the use of the system. Due to the “Who’s Viewed You" feature, they can see when, how often, and by whom they are being queried and adjust their rules accordingly.

- Users in the study seem to feel comfortable enough with the level of control they were given to actually use the system, while at the same time indicating that they wished they had access to more expressive rules.
- Participants were relatively happy with time-based rules, but feel that they would be likely to use location-based rules and group-based rules.
- Users of mobile location sharing systems may make their locations viewable for a greater number of hours (if using time-based rules) if they can see who has been checking their locations.

4.3.4 Technology Adoption

To explore what factors contribute to the continued use of location-based technologies, we included a series of questions in the pre-study survey and in the exit survey based on a model of technology adoption for privacy-enhancing technologies [103]. This allows us to determine participants’ general privacy attitudes, how technically savvy they were, their opinions on the ease of use of the technology, the importance of the perceived control they had with the ability to create rules, their sense of helplessness in the use and existence of such a technology, the opinion of their peers of mobile location technologies, and their opinion of new technology representing positive progress in the world. We conducted a logistic regression to determine whether people could continue to use the technology, based on these factors. The results of the regression are presented in Table 4.4.

	# items	Cronbach's α	Wald χ^2	p value
Condition	-	-	0.33	0.57
Control	1	-	0.02	0.89
Easy to Explain	1	-	0.57	0.45
Helplessness	4	0.82	2.32	0.13
Peer Opinion	2	0.71	9.2	**0.002**
Privacy Scale	6	0.86	1.34	0.25
Tech. Savviness	3	0.80	5.82	**0.016**
Tech. Progress	1	-	0.50	0.48

Table 4.4: Above, the technology adoption factors included in our pre-study and exit surveys are presented showing their influence in continued use of location-based technology. In the logistic regression model, the Wald's χ^2 degrees of freedom is 1 and n = 56.

The logistic regression model has a likelihood ratio χ^2 = 0.0001, indicating that the factors included in the model have a significant impact on whether or not people decide to continue using the mobile location-sharing technology. The model has a max rescaled R^2 of 0.57, indicating that the factors included in the model can explain about 57% of the variance in deciding whether to continue using the mobile location sharing technology. The two main factors of significance are peer opinion (p = .002), and technical savviness (p = 0.016). In the 7-point scale for peer opinion, for every 1-point increase, the odds of continuing use of the technology are increased by a factor of 4.44. Similarly, for every 1-point increase in the 7-point scale for technical savviness, the odds of continuing use are increased by a factor of 2.64.

- Peers have a significant impact on whether or not a user will accept and continue to use a mobile location-sharing technology.

- The more technically savvy someone is has an impact on whether or not a user will continue to use a mobile location-sharing technology.

4.4 Discussion

In this field experiment, we find that feedback can play a role in the adoption of mobile location-sharing technologies. Despite the success of existing OSNs or mobile location technologies that lack feedback, feedback has a role in the comfort of using such technologies. For designers of ubiquitous computing technologies, we offer the following insights to consider as they develop new technologies.

4.4.1 Context

The overall context may have an impact on whether or not feedback is necessary. In the case of real-time location requests, people desire social translucency due to the sensitive nature of this information. The interface and technical mechanisms in place in our mobile location-sharing technology allowed the system to provide to users details of who had viewed their locations. Subsequently, this information played a role in easing people's privacy concerns. In other contexts—for example, online profiles (Facebook), current music choices (last.fm), or the number of miles run (Nike Plus)—feedback may be less important.

4.4.2 Control

Designers should examine the types of controls and the amount of expressiveness that the controls provide. We find that people are willing and able to use rules to control access to their location information, and feedback does not cause users to lock down or severely restrict their information sharing, certainly a present fear of many OSNs, but may actually lead to more open policies. For future systems, mobile location-sharing technology developers may be well served by building disclosure history feedback into their systems as well as methods to define more expressive privacy preferences. Offering a diverse palette of rule types to govern the disclosure of personal location information empowers people to protect their own privacy, lessening concerns. While the top current OSNs do not have any system translucency, this initial work may address many of their reservations. Giving users more control over their privacy and knowing that this information is likely to make users more comfortable with the spectrum of people inquiring about their information are both positive for the OSNs.

4.4.3 Bells & Whistles

Designers should understand the customer they are trying to target. In addition to the technology acceptance model's tenets of perceived usefulness and perceived ease-of-use [44], other factors may influence technology adoption. We have seen that adoption of a mobile location-sharing technology depends highly on technical ability. While developers need to target the “bleeding edge," they must maintain a positive buzz about their services to keep users and their peers enthusiastic about location-based technologies. As OSNs continue to grow in features and population, we hope to see a balancing of the amount of social translucency and information users receive and their comfort in exploring and using the network.

4.5 Insights

This research presents the findings of a study examining the impact of control and feedback for sharing location disclosures. Based on a four-week field investigation of a mobile location-sharing application embedded in an online social network, our findings can inform the design of mobile social systems:

- Providing feedback to users about when and by whom they have been queried tends to make them more comfortable about sharing location information.
- Feedback is a desired feature in such a system and makes users more willing to share their location information.
- Users are able to use time-based rules to control access to their location information, and they feel that these rules accurately represent their privacy preferences.
- In addition to time-based rules, users also indicated that they are likely to use location-based and group-based rules.
- Users who have feedback are more likely to set rules that make themselves findable for a greater number of hours.
- Peers and technical savviness have a significant impact on whether or not a user will accept and continue to use a location technology.

4.6 Items for Future Research

While this was a successful deployment of a real-world location-sharing study, we were unable to capture the full range of user defined rule expressiveness due to the system's limitation of time-based rules only. We also see that real system usage of Locyoution was very low, making it difficult to analyze usage patterns. Additional research can be conducted to examine the impact and use of a rules that span a larger number of restriction types and how feedback affects system use.

Chapter 5

Location-Sharing Feedback Study II (Locaccino)

In a followup to the Locyoution study, we examined the impact of feedback on users' levels of comfort using Locaccino, the redesigned PeopleFinder technology. The entire premise of the Locaccino system was changed, switching from an open system, where strangers were permitted to view one's location, to a closed system, where location requests were limited to users' Facebook friends. In addition, the Locaccino system provided users with additional options for rules defined by time, group, and location. Participants (divided into two conditions, a group *without feedback* and a group *with feedback*) used Locaccino for a period of a month. Afterwards, we conducted qualitative interviews with a small sample of users to better understand users' perceptions of Locaccino. The results of this study indicate that contrary to the previous study, providing users with feedback, by and large, had no impact on comfort levels of using the system and on patterns of usage with the system. These finding suggest that the fundamental shift in the system design of Locaccino, limiting access to “friends" and increasing the expressiveness of rules interface, mitigated privacy concerns.

5.1 Technology

In the Summer of 2008, a fundamental shift occurred in the syntax and semantics of the PeopleFinder concept. Previously an open system, where users could be located by strangers, it was transformed into a closed system, where people were required to be connected to each other to request one’s location. As such, the PeopleFinder technology was completely overhauled. The new backend, frontend, and locater software were renamed and rebranded as *Locaccino*. Similar to Locyoution, users interact with two main pieces of technology: software that users install on their laptops or mobile phones (the Locaccino Locator) and an application that is added on Facebook (the Locaccino Facebook Application).

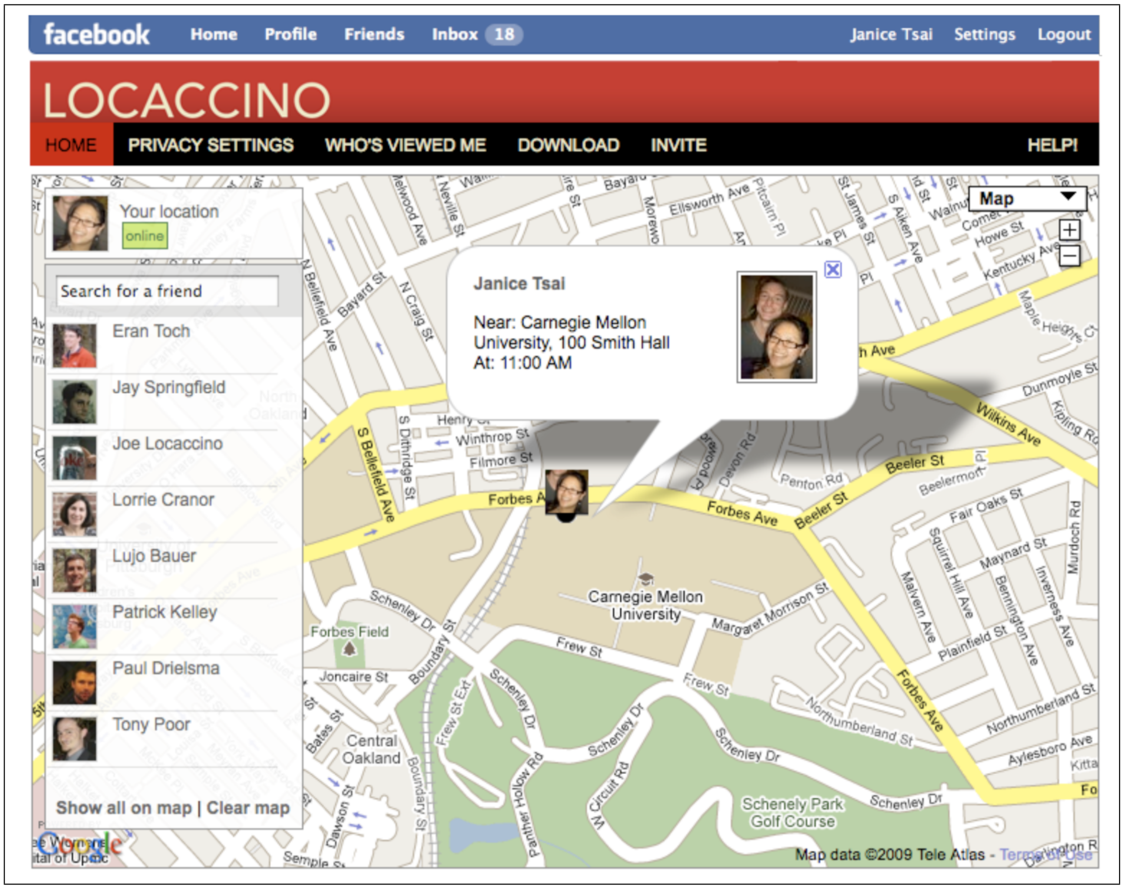
At the same time, several major changes occurred within Facebook that had significant impacts on the use and deployment of Locaccino:

- Profile pages were divided into a tabular format, rather than a single page. The majority of third party applications were moved onto a “Boxes" tab, reducing the visibility of those applications.
- Facebook launched “Facebook Connect," an authentication service that allows developers to use Facebook credentials rather than requiring the creation of a new

set of login credentials. Once a user downloads and installs the Locaccino Locator software, they are authenticated via Facebook Connect, linking their identity on the Locaccino Facebook application to the Locator software which sends out location updates.

The changes made to Locaccino include the following:

- Users interact with or find Locaccino by clicking on a webpage link to the application, by searching for the application on Facebook, or by adding a bookmark to Locaccino on their applications toolbar (the bottom left corner of their browser window when Facebook is open). A Profile box to the application is no longer available on the user's Profile page.
- Locaccino users can only be requested by people with whom they are "Facebook Friends," (in Locyoution, users could be requested by anyone with access to their Facebook Profile page). In Locaccino, one's list of Facebook Friends who are also Locaccino users is automatically pulled from the backend database and displayed on the Home page.
- The Locaccino ruleset was expanded in functionality. In addition to the time-based rules available in Locyoution, Locaccino users can also create group-based, network-based, and location-based rules (i.e. Allow my friends Rich and Julie (group) and people on the Carnegie Mellon University network (network) to view my location from 10 am to 3 pm (time) and when I am on campus (location)).



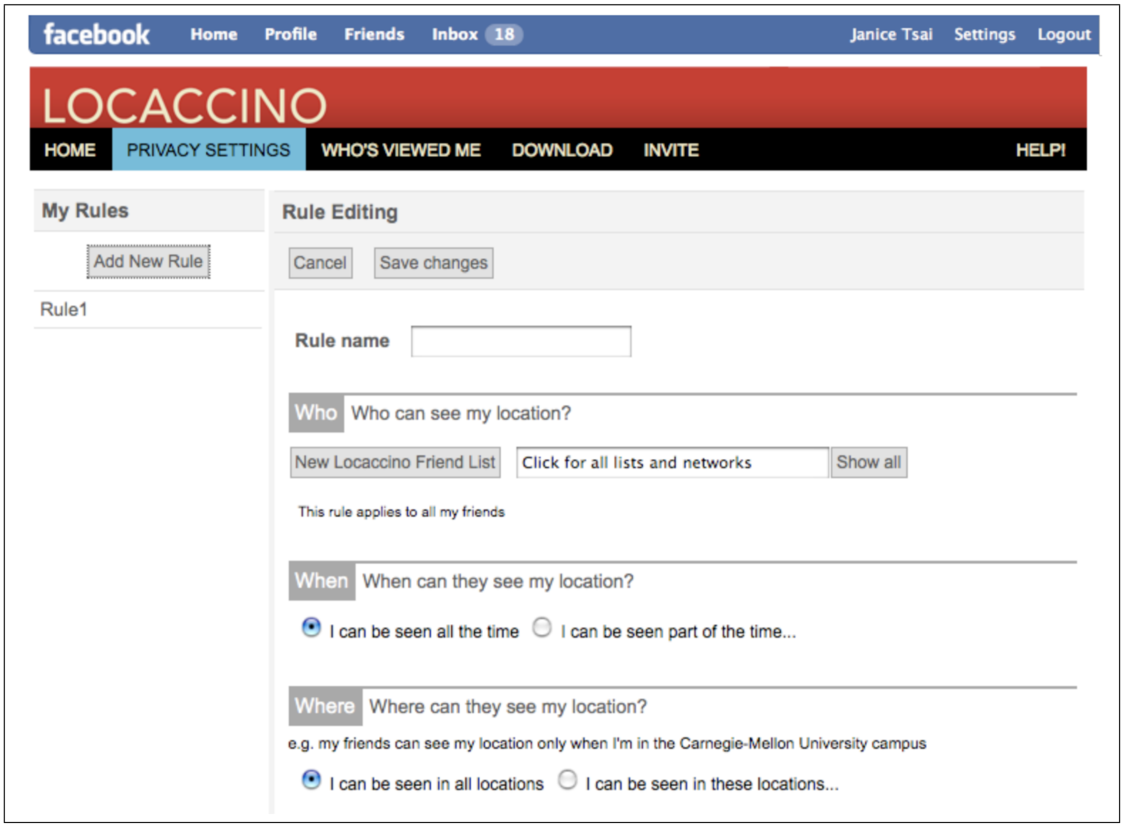
Janice Tsai

Near: Carnegie Mellon University, 100 Smith Hall
At: 11:00 AM

Figure 5.1: The Locaccino “Home" interface in Facebook. It shows, by default, the user’s own location, and presents a list of friends using Locaccino.

5.2 User Interface

The Locaccino Facebook interface consists of three main areas. The first area, “Home,” is viewable by Locaccino users as well as by anyone on Facebook. The other two areas, “Privacy Settings” and “Who’s Viewed Me,” are only viewable by Locaccino users (users who have downloaded the Locaccino Locator).



Who can see my location?

This rule applies to all my friends

When can they see my location?

● I can be seen all the time ○ I can be seen part of the time...

Where can they see my location?

e.g. my friends can see my location only when I'm in the Carnegie-Mellon University campus

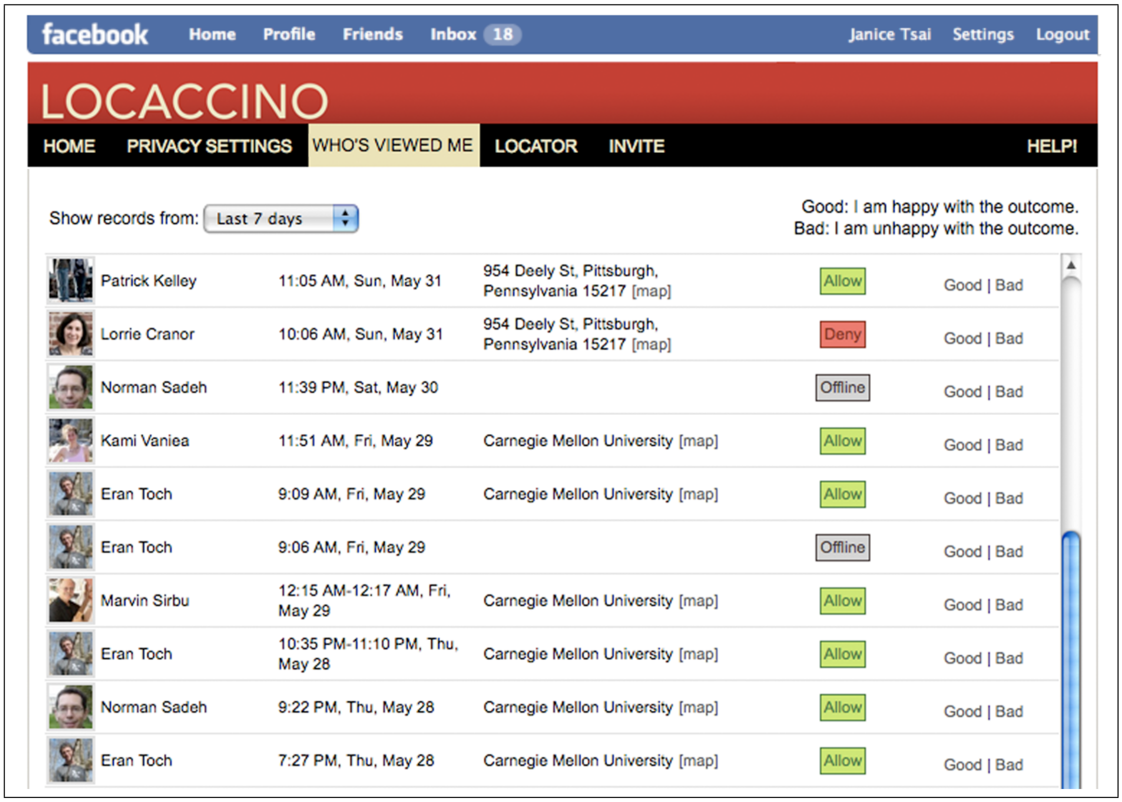
● I can be seen in all locations ○ I can be seen in these locations...

Figure 5.2: The Locaccino “Privacy Settings" interface, formerly “My Rules." The interface allows users to define *Who* can view them (group and network-based rules), *When* people can view them (time-based rules), and *Where* people can view them (location-based rules).

5.2.1 Home Screen

After the installation of the Locaccino Locator software and Facebook application, the user is presented with the Locaccino home screen on Facebook, as shown in Figure 5.1.

The Home page shows, by default, the user’s current location. If the user have Facebook friends who are Locaccino users, they can click on each individual friend to locate them, or click "Show All" to view all available friends on the map.



Show records from: Last 7 days

Good: I am happy with the outcome.
Bad: I am unhappy with the outcome.

Patrick Kelley	11:05 AM, Sun, May 31	954 Deely St, Pittsburgh, Pennsylvania 15217 [map]	Allow	Good | Bad
Lorrie Cranor	10:06 AM, Sun, May 31	954 Deely St, Pittsburgh, Pennsylvania 15217 [map]	Deny	Good | Bad
Norman Sadeh	11:39 PM, Sat, May 30		Offline	Good | Bad
Kami Vaniea	11:51 AM, Fri, May 29	Carnegie Mellon University [map]	Allow	Good | Bad
Eran Toch	9:09 AM, Fri, May 29	Carnegie Mellon University [map]	Allow	Good | Bad
Eran Toch	9:06 AM, Fri, May 29		Offline	Good | Bad
Marvin Sirbu	12:15 AM-12:17 AM, Fri, May 29	Carnegie Mellon University [map]	Allow	Good | Bad
Eran Toch	10:35 PM-11:10 PM, Thu, May 28	Carnegie Mellon University [map]	Allow	Good | Bad
Norman Sadeh	9:22 PM, Thu, May 28	Carnegie Mellon University [map]	Allow	Good | Bad
Eran Toch	7:27 PM, Thu, May 28	Carnegie Mellon University [map]	Allow	Good | Bad

Figure 5.3: The Locaccino “Who’s Viewed Me" interface. This interface allows users to see who has queried their location as well as the response provided.

5.2.2 Privacy Settings

Locaccino users can create and edit rules about their visibility in the Privacy Settings area of Locaccino. This interface (Figure 5.2) allows users to define access to their location information.

Rules can consist of three different types of restrictions:

- *Group (Who):* Group restrictions are created when users select specific Facebook Friends they wish all access to their location information. Group restrictions can also consist of Networks users wish to make their location information viable (i.e. anyone on the Carnegie Mellon University Facebook network). Users can create new groups by adding their Facebook friends or by utilizing their existing Facebook Friend Lists.

- *Time (When):* Users can define period of time (i.e. 9 am - 5 pm) and days of the week during which they wish to allow others access to their location information. Users can add multiple time-based restrictions onto a single rule. (i.e. Allow people to find me on Tuesday and Thursday. from 3 pm to 5 pm, and from 10 pm to 2 am from Thursday through Sunday.)
- *Location (Where):* In the Privacy Settings interface users can select a geographic area they wish to allow themselves to be found.

The default setting in Locaccino is to **deny** location requests. Unless a user creates rules, no one will be able to view the user's location.

5.2.3 Who's Viewed Me

The Who's Viewed Me tab in the Locaccino interface allows users to see who has viewed their location as a history or audit log, as shown in Figure 5.3. When a Facebook user clicks on an individual to be located on their Home screen, or Show All, the identity of the requester is recorded. Additionally, the time of the request, the requested person's user's location, and the system's decision (e.g. Allow) are stored.

Users can view the location requests made of them, and whether the request was allowed, denied, or if they were offline or hidden. Users can also view a map of where they were at the time of the request.

5.2.4 Facebook Privacy Settings

Due to the changes in the Facebook interface, Locaccino users typically no longer add Locaccino as a profile box, as they did in Locyoution. The default Facebook Application privacy settings allow users to bookmark Locaccino, or permit Locaccino to publish stories on the user's profile.

5.3 System Response

When a location request is made, that request is passed to the server, and if the request falls within the allowable provisions defined by the rules, the map location is passed back to the frontend to be displayed on the Home screen; otherwise, a "[Person being located] is unavailable" message will be displayed. The system response will be one of the following:

- *Deny:* The person requesting the user is not permitted access to the user's location information as defined by the user's rules. The "unavailable" message is displayed to the requester.
- *Disclose:* The person requesting the user is granted access to the user's location information. The map of the requestee's location is displayed to the requester.
- *Hidden:* The Locaccino Locator has an "Invisible" mode where the Locator continues to pass location information back to the server, but location information is blocked. When someone requests a "hidden" user, the "unavailable" message is displayed.
- *Offline:* The person being requested does not have any location information available

because their Locaccino Locator is not on, or is not transmitting location information. The person requesting a user's location is presented with the “unavailable" message.

5.4 Locaccino Study

Due to the limitations of the Locyoution study, we conducted the Locaccino study to examine the impact of rule expressiveness and feedback on Locaccino usage on a larger scale. In March 2009, participants solicited from a university population, were asked to install and use Locaccino over a period of four weeks. The study consisted of three phases: a pre-study questionnaire which directed users to instructions for Locaccino installation, Locaccino deployment and use, and an exit survey. In Phase 1, participants completed a questionnaire, installed the Locaccino Locator, added the Facebook application, and completed consent forms. We provided assistance to anyone who had difficulty installing the software and viewing their location. In Phase 2, participants used Locaccino for four weeks. Usage patterns of Locyoution were determined by examining server logs. Finally, in Phase 3, participants completed an exit survey on their experience with Locaccino. Any users who had previously participated in the Locyoution study were disqualified. After the conclusion of the Locaccino Study, we conducted qualitative interviews with a small sample of Locaccino users .

To determine the impact of feedback on the privacy attitudes and adoption of our mobile location application, participants were randomly divided into two conditions:

No Feedback condition: Participants did not receive information about who had requested their location (n = 57).

Feedback condition: Participants were able to view their location disclosure history (n = 85).

5.4.1 Method

We recruited participants from a university population, offering a $20USD online gift certificate as compensation for completion of the study. We posted flyers around campus, and advertised on university mailing lists. We realized that there was a significant potential for participant attrition due to the nature of the study (a field investigation with a relatively “hands-off" approach), and thus recruited a large number of participants.

To mimic real world usage, participants were provided with online instructions for participation, no physical meetings or lab sessions were conducted. Participation involved downloading and installing the Locaccino software and adding the Facebook application. Once participants added the Facebook application, they were required to click on a "Join the Study" button to officially register for the study, and to be randomly assigned to a condition.

As per study completion requirements, users were required to be online (have the Locator running on their laptops) an average of 5 hours per day over the 4 week period. Participants who were not active Locaccino Locator users were disqualified from the study.

5.4.2 Demographics

The final set of users included 142 individuals. The ages of the participants ranged from 18 to 71 years old (M = 30.2 years). Of all the respondents, 39.4% were female. Between the two conditions, there were comparative proportions of males and females (i.e. 40.0% female population in the feedback condition and a 38.6% female population in the no feedback condition.) The participants in our study were primarily students (51.4% Undergrads (73), 27.5% Masters students (39), and 12.0% PhD (17)). The remainder of our population was a mix of staff (7.03% (10)), faculty (0.7% (1)), and other (1.41% (2)).

5.4.3 Data Analysis

The duration of the study was 4 weeks, with rolling entrance into the study for the first two weeks of the study launch date. We kept in touch with participants periodically, sending email reminders about using Locaccino and keeping the Locator running. Our data analysis covers the full duration of the study.

After the conclusion of the study, we analyzed the usage of Locaccino and the results of the pre-study and exit surveys. We examined differences between the conditions and their privacy attitudes, technology acceptance, and rule usage. In the next sections, we focus on the implications of privacy, feedback, and rule expressiveness.

5.5 Results

5.5.1 Privacy

Similar to the previous study, we were interested in the impact of technology use on the level of concern that people had for their privacy. We also investigated the perceived usefulness of location-sharing technologies, and on the ability to control access to one's location. To capture levels of concern related to privacy and control we asked how concerned people were with allowing others to view their locations and about controlling access to who has access to their locations on a 7-point Likert scale ranging from not concerned to extremely concerned. We also asked how useful being able to share their location with other would be, ranging from not useful to extremely useful on a 7-point Likert scale.

Examining our users survey responses, we see that in general, after using Locaccino, users found it less useful than they thought it would be to share their location with others, and they became less concerned with controlling access to their location. People in the Feedback condition were still as concerned with their privacy after using the system as they indicated they were prior to the study, and those in the No Feedback condition became less concerned about their privacy, see Tables 5.1 for details.

In the pre-study survey, we asked for participants' stated comfort levels with being located by close friends, acquaintances, and strangers. Within each of these relationship types, users rated their comfort levels with sharing their locations *anytime*, *at times they had specified*, or at *locations they had specified*. We see that, in general, our users were most comfortable with their friends checking their locations, less so with acquaintances,

Item	Condition	Before	After	t statistic	p value
Concern	Feedback	3.94	3.88	0.22	0.82
	No Feedback	4.09	3.49	2.70	$<$**0.01**
Control	Feedback	5.40	5.00	2.10	**0.04**
	No Feedback	5.28	4.83	2.31	**0.02**
Usefulness	Feedback	4.28	3.51	3.73	$<$**0.001**
	No Feedback	4.27	3.47	3.43	**0.001**

Table 5.1: Survey results for people in the Feedback and No Feedback conditions. Paired T-tests for the Feedback condition have a degree of freedom of 84 for each category, and for the No Feedback condition a degree of freedom of 56 for each category. Mean values are based on a Likert scale from 1 to 7, ranging from not concerned to extremely concerned or not useful at all to extremely useful. Concern: how concerned are you with allowing others to view you location. Control: How concerned are you about about controlling access to who has access to your location. Usefulness: how useful is being able to share your location with others.

and not at all comfortable with strangers viewing their locations.

Within each relationship type, participants were the least comfortable being located at *anytime* than with being located with *location* or *time* restrictions. For acquaintances and strangers, people felt more comfortable with sharing their location information if they could specify location restrictions more so than with time restrictions. These results (in a paired t-test) were statistically significant for acquaintances and strangers and marginally so for friends. These comparisons are detailed in Tables 5.2

	Time	Location	t statistic	p value
Friends	6.07	6.19	-1.93	0.056
Acquaintances	4.71	4.99	-3.88	**0.0002**
Strangers	2.49	2.66	-2.68	**0.008**

Table 5.2: Comfort levels of being located by certain groups of people having time-based restrictions and location-based restrictions. Paired T-tests have a degree of freedom of 139 for each type of relationship. Mean values are based on a Likert scale from 1 to 7, ranging from not comfortable at all to fully comfortable.

In the exit survey, we asked participants how comfortable they had been with allowing close friends, acquaintances, and strangers to check their location. We compared these responses with the pre-study comfort rating users had provided about allowing these groups check their locations subject to time-based and location-based rules prior to using Locaccino. See Table 5.3 for mean values and significance levels.

Based on these survey responses, we see that people in the Feedback condition became less comfortable with being located by acquaintances as compared to how comfortable they thought they would feel with time-based or location-based rules. The comparisons for friends and strangers for time-based and location-based rules were not statistically significant. There were no significant differences in the No Feedback condition for the comfort with being located after using Locaccino with time-based or location-based rules.

	Cond.	Time	t statistic	p value	After	t statistic	p value	Location
Friends	F	6.08	0.29	0.77	6.07	-0.31	0.75	6.18
	NF	6.05	0.50	0.62	6.16	-0.27	0.79	6.21
Acq.	F	4.74	-3.36	**0.001**	4.01	-4.66	$<$**.0001**	4.94
	NF	4.66	-0.31	0.76	4.58	-1.59	0.12	5.05
Strangers	F	2.37	-1.49	0.14	2.08	-1.94	0.055	2.49
	NF	2.68	-0.59	0.56	2.53	-1.28	0.21	2.91

Table 5.3: Survey results for people in the Feedback (F) and No Feedback (NF) conditions regarding their comfort levels of being located before (time-based restriction (Time) and location-based restriction (Location)) and after using Locaccino (After) by condition and relationship type, Friends, Acquaintances (Acq.), and Strangers. Paired T-tests have a degree of freedom of 82 for the Feedback condition and 55 for the No Feedback condition. Mean values are based on a Likert scale from 1 to 7, ranging from not comfortable at all to very comfortable.

In general, based on open responses in the exit survey regarding “bad" things that happened to our participants as a function of their use of Locaccino, we find that only a few listed privacy concerns. Most participants had nothing bad happen (n = 85) or they complained about the software or user interface causing problems for them (n = 29).

Several (n = 10) felt nervous about their privacy, and nine participants were found by friends when they would have preferred not to have been bothered.

5.5.2 Feedback

Based on the pre-study questionnaire, participants were interested in knowing who had looked at their Facebook profiles, M = 5.28 (99% CI = 4.97 - 5.59), (based on a Likert scale from 1 to 7, from not interested at all to extremely interested), but were neutral about how they would feel if others knew they were looking at other people's profiles, M = 3.78, (99% CI = 3.37 - 4.18), (based on a Likert scale from 1 to 7 from not comfortable at all to fully comfortable).

At the end of the study, we surveyed the Feedback condition on their experiences and opinions of the Who Has Viewed Me feature. To the No Feedback condition, we presented screenshots of the Who Has Viewed Me interface to solicit their viewpoints on the future inclusion of such a feature. The majority of people in the No Feedback condition wanted feedback (82.46%). For the No Feedback participants who did not want feedback (n = 10, 5 females, 5 males), we see that they are concerned about others knowing they had viewed them. As one user put it, "I would probably not look at people's locations much if they could tell I've viewed their location. Too much opportunity to misinterpret intentions (e.g. i'm just bored vs. I'm a creepy stalker)."

After using Locaccino, people in the Feedback condition became more comfortable checking other people's locations (M = 4.40, 99% CI = 3.97 - 4.84), as compared to how comfortable they felt about having others know they were checking their profiles before the study (Comfort before (M = 3.87, 99% CI = 3.33 - 4.40), based on a paired t-test, t(83) = -2.49, p = 0.02 (means are based on a 7-point Likert scale ranging from not comfortable at all to very comfortable).

For people in the No Feedback condition, there were no differences between how comfortable they would be with having people know that they were viewing their profiles (M = 3.64, 99% CI = 3.00 - 4.29) and how comfortable they felt about viewing other people's locations if they had the Who's Viewed Me feature (M = 3.96, 99% CI = 3.38 - 4.55), t(55) = -1.20, p = 0.23.

We asked our participants if knowing who had viewed them made them or would have made them more willing to share their location with others. For those in the Feedback condition, having feedback made them more willing to share their location (60.71% were more willing, 14.29% were not willing, 25% were unsure). Similar proportions of participants in the No Feedback condition thought having feedback would make them more willing to share their location (57.89% were more willing, 17.54% were not willing, and 24.56% were unsure). There were no significant differences between the conditions, Fisher's exact p = 0.86.

One feature we are often asked about is the ability to have a "stealth mode" where users can view others, but avoid having others notified about their location requests. For example, one user provided us with extensive comments about this feature in the exit survey.

> There can be some more additions and customization options added like 1. Add a stealth mode while viewing others profile. This way your name will not

> show in their who viewed me tab. 2. Also provide the user option to disable viewing their profile in stealth mode. may be provide them only the number of hits on their location for the stealth mode in case they opt to show their location in stealth mode. The basic idea is sometimes the user may want to view someone's profile without being getting noticed by that user. But again this access would be validated by the rules engine and the settings individual may do.

5.5.3 Rule Expressiveness

To examine the impact and usability of rules, we asked people to rate the usefulness of rules. Participants, in general, indicated that they were able to easily create and define rules (M = 4.95, 99% CI = 4.64 - 5.25), they were confident that their rules represented their privacy preferences (M = 4.75, 99% CI = 4.44 - 5.04), and most were confident that the rules worked (M = 4.81, 99% CI = 4.51 - 5.10).

Rules can contain between zero and three restrictions. A rule without restrictions (Always) allows anyone to view that user at any time and in any location. The most common number of restrictions is 1. Table 5.6 provides details on the number of total restrictions by condition.

Examining the last active ruleset for each user, we see that, on average, people created 1.2 rules. In general, 78.9% (112) created 1 rule, 12.0% (17) created 2 rules, and 5.6% (8) created 3 rules, and 3.5% (5) did not create any rules. (Users without rules are not locatable.) The majority of rules have restrictions with group-based components (including

Type of Rule	Feedback	No Feedback
Group Only Rules	36.3% (37)	26.5% (18)
Time Only Rules	12.7% (13)	7.4% (5)
Location Only Rules	2.9% (3)	2.9% (2)
Group/Time Rules	7.8% (8)	11.8% (8)
Group/Location Rules	7.8% (8)	14.7% (10)
Time/Location Rules	3.9% (4)	2.9% (2)
Group/Time/Location Rules	7.8% (8)	7.4% (5)
Always (No restrictions)	20.6% (21)	26.5% (18)

Table 5.4: The percentage of rules based on rule type for each condition.

Type of Rule	Percentage
Group Only Rules	32.35% (55)
Time Only Rules	10.59% (18)
Location Only Rules	2.94% (5)
Group/Time Rules	9.41% (16)
Group/Location Rules	10.59% (18)
Time/Location Rules	3.53% (6)
Group/Time/Location Rules	7.65% (13)
Always (No restrictions)	22.94% (39)

Table 5.5: The percentage of rules based on rule type for each condition.

Network restrictions). Of our user population, 27.5% (39) used network-based restrictions in their rules. The next most common type of rule contains time restrictions, followed by location restrictions. The rules by condition are summarized in Table 5.4. No statistically significant differences existed between the proportion of types of rules between conditions.

5.5.4 Usage

A total of 4,866 requests were made to locate the 142 participants in our study, or an average of 34 requests per participant (or about 1 request per day). Our participants themselves made 7,758 requests of others (not including self-requests) (about 2 requests per day). (Note: We excluded requests for study participants made by the members of

# Restrictions	Feedback	No Feedback
0	20.6%	26.5%
1	52.0%	36.8%
2	19.6%	29.4%
3	7.8%	7.4%

Table 5.6: The percentage of rules based on the number of restrictions for each condition.

	Deny	Disclose	Hidden	Offline
Requests For	13.73% (668)	30.64% (1491)	3.80% (185)	51.83% (2522)
Requests Made By	12.06% (936)	19.49% (1512)	4.59% (356)	63.86% (4954)

Table 5.7: Requests made for study participants and requests made by study participants divided into the response received.

the research lab. These requests would have positively skewed the data for users who are Facebook friends with people on the project. We included all requests made by our participants.)

In the Locaccino interface, users are able to request friends individually by clicking on their names/icons, or users are able to request the locations of all of their friends at one time with the Show All feature. Excluding requests where users only had 1 friend to locate, we see that, participants made individual requests for 44.08% of all requests and Show All requests 55.92% of the time.

In general, for the majority of requests (made by people in our study and for people in our study), the person the user is trying to locate is offline. See Table 5.7 for the responses to all of the requests made by users in our study and the requests made by users in our study.

We find that there are no differences in usage patterns across study conditions. A summary of the means of the types of usage are presented in Table 5.8.

	Feedback	No Feedback	t statistic	p value
Individual Requests	4.31 (σ = 10.39)	5.77 (σ = 9.94)	-0.84	0.40
Show All Requests	7.60 (σ = 18.45)	4.07 (σ = 11.64)	1.28	0.20
Requests For	33.79 (σ = 52.25)	34.98 (σ = 49.58)	-0.14	0.89
Requests Made By	68.82 (σ = 166.5)	33.47 (σ = 77.87)	1.50	0.14
Locator Friends	6.20 (σ = 5.39)	5.46 (σ = 4.85)	0.84	0.40
Application Only Friends	2.41 (σ = 2.33)	1.98 (σ = 4.85)	1.07	0.29
Locaccino Visits	12.64 (σ = 26.78)	8.12 (σ = 16.22)	1.14	0.26

Table 5.8: The mean number of requests, friends, and visited for participants in the Feedback and No Feedback conditions. There were no statistically significant differences between the two conditions in two-sample t-tests.

One limitation in our analysis of the usage of Locaccino is the lack of use in the system. On average, each participant received about 1 request per day. Over the course of the study, people were online with the Locaccino Locator for about .5 a request per day. Due to these sample sizes, we are able to only detect only very large differences between the conditions. For example, in a power analysis where we wish to detect significant differences between the requests made for participants between the two conditions, with the current means (Feedback M = 33.79 and No Feedback M = 34.98), we would need a sample size of 32,490 requests (or approximately 229 requests per user) as compared to the 4,866 requests made of users in our study[1].

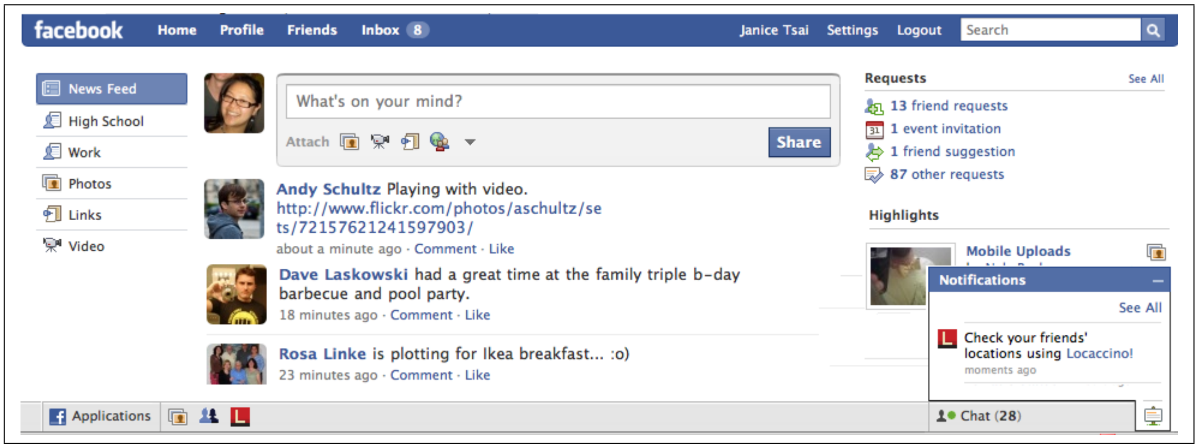
5.5.5 Facebook Notifications

In Facebook, application developers are able to send notifications to their users. These notifications appear as a small red flag in the bottom left-hand corner of the users' main Facebook page, as shown in Figure 5.4. During the study, we sent three notifications about using Locaccino to our study participants or to users who had located people in our study.

---

[1] Power analysis calculations were computed using G*Power 3[46].

We see that the notifications typically results in an increase in requests, with a significant increase as a result of the third notification. See Figure 5.5.



Andy Schultz Playing with video. http://www.flickr.com/photos/aschultz/sets/72157621241597903/
about a minute ago · Comment · Like

Dave Laskowski had a great time at the family triple b-day barbecue and pool party.
18 minutes ago · Comment · Like

Rosa Linke is plotting for Ikea breakfast... :o)
23 minutes ago · Comment · Like

Check your friends' locations using Locaccino!
moments ago

Figure 5.4: Facebook notification.

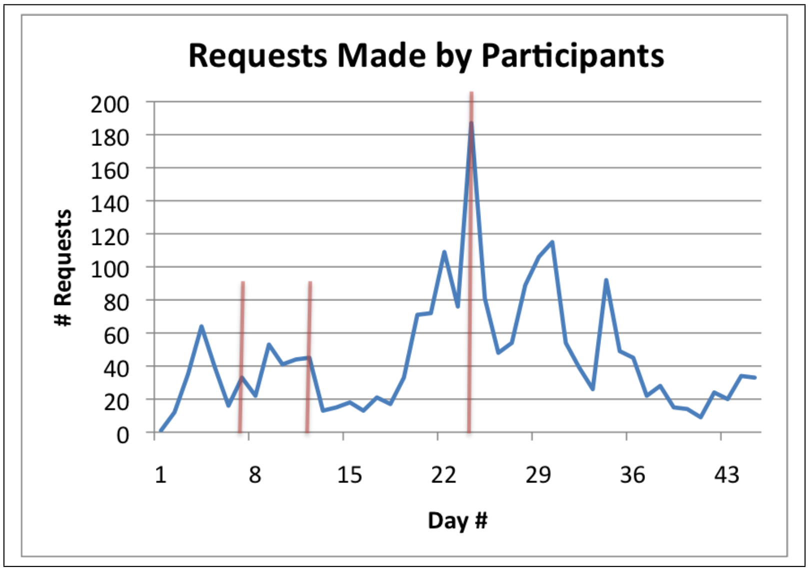


Figure 5.5: The chart of the requests made by study participants over the duration of the study. The lines indicate when Facebook notifications were sent to users.

5.5.6 Technology Adoption

To explore what factors contribute to the continued use of location-based technologies, we included a series of questions in the pre-study survey and in the exit survey based on a model of technology adoption for privacy-enhancing technologies [103]. This allows us to determine participants' general privacy attitudes, how technically savvy they were, their opinions on the ease of use of the technology, the importance of the perceived control they had with the ability to create rules, their sense of helplessness in the use and existence of such a technology, the opinion of their peers of mobile location technologies, and their opinion of new technology representing positive progress in the world. We conducted a logistic regression to determine whether people could continue to use the technology, based on these factors. The results of the regression are presented in Table 5.9.

	# items	Cronbach's α	Wald χ^2	p value
Condition	-	-	0.008	0.38
Control	1	-	1.32	0.25
Usefulness	1	-	6.11	**0.01**
Ease of Use	3	0.68	10.68	**0.001**
Helplessness	4	0.66	3.00	0.08
Peer Opinion	3	0.74	19.78	$<$**.0001**
Privacy Scale	6	0.82	1.18	0.28
Tech. Savviness	3	0.73	0.07	0.80
Tech. Progress	3	0.47	0.40	0.53

Table 5.9: Above, the technology adoption factors included in our pre-study and exit surveys are presented showing their influence in continued use of location-based application. In the logistic regression model, the Wald's χ^2 degrees of freedom is 1 and n = 139.

The logistic regression model has a likelihood ratio $\chi^2 < 0.0001$, indicating that the factors included in the model have a significant impact on whether or not people decide to continue using the mobile location-sharing technology. The model has a max rescaled

R^2 of 0.54, indicating that the factors included in the model can explain about 54% of the variance in deciding whether to continue using the mobile location sharing technology. The main factors of significance are the usefulness of the technology (p = 0.01), the ease of use of the technology (p = 0.001), and one's friends opinion of Locaccino (peer opinion) (p <.0001).

In the 7-point Likert response scales for usefulness, ease of use, and peer opinion, a 1-point increase on these scales leads to an increase in the odds of the adoption of location sharing technologies. For usefulness, for every 1-point increase, the odds of continuing use are increased by a factor of 1.63. Similarly, for every 1-point increase related to the ease of use of the technology, the odds of continuing use increase by a factor of 0.46. Finally, a 1-point increase in peer opinion would increase the odds of use by a factor of 3.86.

5.5.7 Data Analysis for Active Users

While we had 142 users in our study, only 127 would be considered active users (Feedback = 76, No Feedback = 51). Active users are ones who visited the Locaccino application and made location requests of others. The survey results and usage results for active users did not differ significantly from those presented above.

Technology Adoption for Active Users

When controlling for active users, we see that the factors that impact technology adoption are slighted altered. In the results of the logistic regression to model continued use of location-sharing applications, we see that helplessness becomes a significant factor. The model has a likelihood ratio $\chi^2 < 0.0001$, and a max rescaled R^2 of 0.62. In addition to helplessness (p =0.01), the other factors of significance include peer opinion (p <.0001), and the ease of use of the technology (p =0.0002). The usefulness of the technology becomes marginally significant (p <0.054). The results of the regression are presented in Table 5.10.

	# items	Cronbach's α	Wald χ^2	p value
Condition	-	-	0.54	0.46
Control	1	-	0.76	0.38
Usefulness	1	-	3.71	0.054
Ease of Use	3	0.73	13.79	**0.002**
Helplessness	4	0.69	6.70	**0.01**
Peer Opinion	3	0.74	20.03	$<$**.0001**
Privacy Scale	6	0.80	1.33	0.25
Tech. Savviness	3	0.72	0.34	0.56
Tech. Progress	3	0.47	0.04	0.84

Table 5.10: This table details the technology adoption factors for active users of Locaccino, modeling the continued use of location-based application. In the logistic regression model, the Wald's χ^2 degrees of freedom is 9, n = 125.

In the 7-point Likert response scales for ease of use and peer opinion, a 1-point increase on these scales leads to an increase in the odds of the adoption of location sharing technologies. For every 1-point increase related to the ease of use of the technology, the odds of continuing use increase by a factor of 0.33. A Finally, a 1-point increase in peer opinion would increase the odds of use by a factor of 6.05.

	Deny	Disclose	Hidden	Offline
Feedback	11	14	3	36
No Feedback	7	14	3	24

Table 5.11: Users divided info classifications based on the most frequent type of request response.

5.5.8 Data Analysis by Request Responses

To examine the impact of requests and their responses on system usage, we classified each of our users based on the most frequent request response: Deny, Disclose, Hidden, and Offline (e.g. A user with 10 total requests where 9 of those requests were offline would be classified as Offline.) (Note: This data includes requests for participants by users in the research group.) This classification by condition is detailed in Table 5.11.

Using an ANOVA to compare the usage means between each condition for each classification, we see that the most frequent type of response to requests for our users does not have an impact on usage. See Table 5.12 for details.

	Condition	Deny	Disclose	Hidden	Offline	F statistic	p value
Requests For	F	15.09	46.36	25.00	54.08	1.50	0.22
	NF	15.43	45.50	26.00	47.08	0.78	0.51
Requests Made By	F	49.36	133.21	30.00	90.67	0.51	0.68
	NF	27.29	36.86	133.33	31.88	1.41	0.25
Locator Friends	F	5.73	6.93	9.67	8.47	1.01	0.39
	NF	4.57	5.43	5.33	7.08	1.10	0.36
Rule Changes	F	1.27	1.79	2.33	2.53	1.65	0.19
	NF	1.29	2.57	1.00	2.13	0.87	0.47

Table 5.12: Information for people in the Feedback (F) and No Feedback (NF) conditions regarding their usage by classification along with ANOVA results.

5.5.9 Qualitative Interviews

We conducted several qualitative interviews to elicit an understanding of users' perceptions of use and privacy surrounding their participation in the Locaccino user study. We wished to understand why the results of this study were so different from the results of the Locyoution study, where participants with feedback became more comfortable with allowing certain groups to access their location information.

We conducted these interviews with two hypotheses in mind:

Hypothesis 1: A user interface that precluded being located by strangers resolved privacy concerns.

Hypothesis 2: Rule expressiveness mitigated privacy concerns.

A small sample of users was selected for semi-structured interviews conducted via phone in July 2009 (three months after their participation in the user study). Of the 24 people solicited for interviews, 10 responded (Feedback = 6, No Feedback = 4) and were interviewed. Users could be divided into two group: those who have no concerns for their privacy at all (n = 4), and those who had some qualms about sharing their location information (n = 6).

Our questions focused on several topics:

- Users' privacy concerns prior to using Locaccino.
- The evolution of those concerns (if any) due to their use of Locaccino.
- The features or attributes of Locaccino that may have made them more (or less)

comfortable.

- Differences in usage for a system run for research purposes by Carnegie Mellon as compared to a commercial enterprise.

To ensure that users remembered their experiences in the user study, each person was asked to recall their last rule in the Locaccino system.

Privacy Concerns

Several users expressed the concerns they had about sharing their location information. “I was worried that people could find me, and I would not be interested in having people finding me." Another user mentioned that they would only let people see their location if they were on their contact list, and that he’d be concerned if there was a way for someone not on his list to view him. The majority of the people that were interviewed indicated that they would not be comfortable with allowing everybody or strangers to view their locations. Another participant indicated that they would not be comfortable with even acquaintances viewing their locations. She made the distinction of acquaintances not being a part of the group she has granted access to, and would not feel comfortable with them knowing where she was. Hypothesis 1 is supported.

The Impact of Rules

Our interviews revealed that having rules or controls were an attribute that made users less concerned about using Locaccino. One made it very clear that since they knew that

Locaccino was a “privacy-based project" they were less worried about their participation in the user study. Users mostly echoed the sentiment that “the privacy settings were quite detailed, and I could exclude people so that if I didn’t want they wouldn’t see [me]" or that “Locaccino is cool because it has all the options." People had a good understanding from the beginning that they rules they set would restrict the disclosure of their location. As one user noted “I knew there were privacy controls so I could restrict who could see me and not." Hypothesis 2 is supported.

5.6 Discussion

This research presents the findings of a study examining the impact of control and feedback for sharing location disclosures. Contrary to our findings in the last study, we see that feedback, by and large had no impact on privacy concerns, usage patterns, or the creation of rules. The fundamental shift in the design of the system may have had an impact on our users and led to the difference in the importance of knowing who has viewed your location. Based on our qualitative interviews, we see that people’s privacy concerns were allayed by the design of the system, the controls provided to them allowed them to sufficiently limit who they made themselves available to. We revisit our original insights presented in Chapter 4, and find that they are still applicable and relevant.

Context

Context continues to play a role in whether or not feedback is necessary. In an open system, where strangers can request users' locations, feedback may be necessary to reduce the privacy concerns associated with the use of the technology. Being provided with Who's Viewed Me may help users ensure that their location information is only accessible to those who they want to have access. In a closed system limited to one's contact list or existing list of friends, or one in which the expectation for use of the system is "Friends Only," feedback may not be as necessary to allay fears. As one participant in the Locaccino study noted "Since they allow me, it [checking a friend's location] should not be an issue."

We find that people continue to want feedback, even if it does not impact the use of the location-sharing system. As one interviewee said about the Who's Viewed Me feature,

> [It's] certainly an interesting feature. As long as I have a working set of privacy rules, I don't need to know who's viewed me, or who can view me right now. [But,] no reason against the feature. Having the feature does not harm the usability of the software.

Control

Designers are encouraged to continue to consider the controls they offer and the expressiveness provided by those controls. In this research we see that expressive controls can reduce privacy concerns. The majority of the users in the Locaccino study were able to create rules, using the spectrum of controls that were made available to them. Based on our small sample of interviews, it seems that the rules had an impact on their impression of Locaccino. By providing users with a diverse palette of controls, it allows them to govern the disclosure of their location information.

Critical mass

Currently, it seems that technology developers have not yet found a way to present this technology to users so that they value the usefulness of location-sharing technologies. We see that after using our system, people found location-sharing technologies to be less useful than they thought they would be. In addition to the usefulness of location-sharing technologies, peer opinion continues to have an impact on the adoption of these technologies. This is connected to the issue of creating a “critical mass" of users or friends using the technology so that people have a reason for signing up and maintaining their use of these types of applications. Technology developers must also make an effort to expound on and communicate the usefulness of their products and ensure that their applications are easy to use.

5.7 Limitations and Future Work

This study suffered from a lack of usage of the application. From the exit survey results, we see that people still do not find location-sharing applications useful. This may be due to a lack of critical mass of adoption. For example, unless a Locaccino user can convince their friends or families to download the location-sharing software, and begin to use the

Facebook application, there is no reason for them to visit the application itself in Facebook, and no reason for them to even keep the application running if no one is checking for their locations. Based on the perceived benefits of location-sharing applications discussed in Chapter 3, we see that the greatest benefit is that of being able to find people in an emergency. If no one is running the location-sharing application, this benefit becomes moot.

Studies, such as this one, are typically very difficult to run. In a university environment, participants in the study who are in the same friendship groups, classes, or residence halls. may see each other so frequently, and know so much about each others daily activities and schedules that they do not need to use location-sharing services to find each other. Additionally, they may also have an non-standard and low level of privacy concern because they already expect others to know everything about them. In a non-university setting, people may not be using their laptops or be online as constantly as people in a college population, making themselves more difficult to locate. The less frequently someone is online, the less use others will find from using an application that rarely locates their friends.

Another limitation of this study was the addition of two significant changes of the system: the shift to a closed system, limited to Facebook Friends, and the addition of more complex rule expressiveness. While it seems that both of these factors may have had an impact on users' perception and use of Locaccino, we are unable to quantify the specific impact of each of these changes. Future work could isolate these factors to better understand the effect of each on privacy concerns. For example, future research studies could eliminate rules entirely and solely provide users with feedback or no feedback using an open and a closed system. This research design would allow researchers to pinpoint the value of a closed vs. open system and the impact of feedback in each. Other research directions could also focus on how to better increase the value proposition and usefulness of location-sharing systems.

Part III

Privacy and Consumer Choice

Chapter 6

Online Privacy Concerns Study

An online survey was used to understand the types of concerns people had related to their online privacy when shopping online. In this survey, I examined online privacy concerns and their perceived likelihoods and consequences. This survey was also used to evaluate various products to determine which purchases would raise significant privacy concerns. Based on the results of the survey, we see that the Privacy Finder interface addresses the concerns that participants rated the most likely. Similar to previous studies, we find that most people have concerns when they are on the Internet and when they shop online, but most do not read privacy policies in their entirety. Instead, they tend to notice the presence of privacy policies more often than they read them. It seems that people still find it difficult to get the privacy information they want, and instead, choose to bypass reading privacy policies, and just hope for the best.

6.1 Method

6.1.1 Recruitment

In September 2006, we solicited participants to complete an “Online Privacy Concerns” survey, administered via SurveyMonkey, an online survey creation and administration tool. 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.

6.1.2 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.

6.2 Data Analysis

6.2.1 Privacy Policies

We were also interested to see how participants' actions were linked to privacy concerns. To find out, we inquired about individuals' behaviors involving privacy policies. We asked participants if they had read the policy at the last online store they had purchased from, and how much of the policy they had read. With regard to how much of the privacy policy they had read, 46% responded that they had interacted with the policy in some way, where 8.3% of participants had clicked on the "privacy policy" link to verify that a policy existed, 29.4% reported that they had skimmed the policy, 1.5% had read the first paragraph, 1.8% read half of it, and 5.1% indicated that they had read the entire privacy policy.

We asked the following 7-point Likert questions to determine participants' general practices related to privacy policies:

- Do you generally notice whether or not a website you are visiting has a privacy policy? (Never (0) to always (6))
- How often do you read websites' privacy policies? (Never (0) to Always (6))

In a paired t-test, participants reported to be more likely to notice if a website has a privacy policy (M = 3.1) than they were to read them (M = 1.85), t(275) = 12.57, $p <$.0001. We also asked, on an 11-point Likert scale, "How bad is it if an online company you buy from doesnÕt have a privacy policy?" from (not bad at all (0) to extremely bad (10). We found that most respondents find that it is bad if an online company does not have a privacy policy, M = 7.3 (99% CI = 6.8, 7.7), t(275) = 13.3, $p < .0001$. It appears that while people may not often read privacy policies and only sometimes notice privacy policies, they find it important that an online store has a privacy policy.

6.2.2 Risk Beliefs

We sought to determine the level of risk that people perceive when they are sharing their information online, and in particular, when they are purchasing items on the Internet. In our sample, 65.2% indicated that they have general privacy concerns on the Internet and 68.5% have privacy concerns when they are shopping online.

Several risk belief questions were asked of the respondents. Based on these questions, we calculated a "Risk Score" for each person. This score is an average of the following four 7-point Likert scale questions asked in the survey:

- I feel safe giving my personal information to online stores. (Strongly disagree to strongly agree (reversed))
- Providing online stores with personal information involves too many unexpected problems. (Strongly disagree to strongly agree)
- I generally trust online companies with handling my personal information and my purchase history. (Strongly disagree to strongly agree (reversed))
- How concerned are you about threats to your personal privacy online in American today? (Not concerned at all to extremely concerned)

We assigned points to the responses, reversing the scoring for the questions marked with an asterisk so that the higher the score, the greater the feeling of concern or risk of being online. We found this 4-item scale for assessing whether the participants felt it risky to be online to be reasonably reliable, as measured through a Chronbach's α of 0.77.

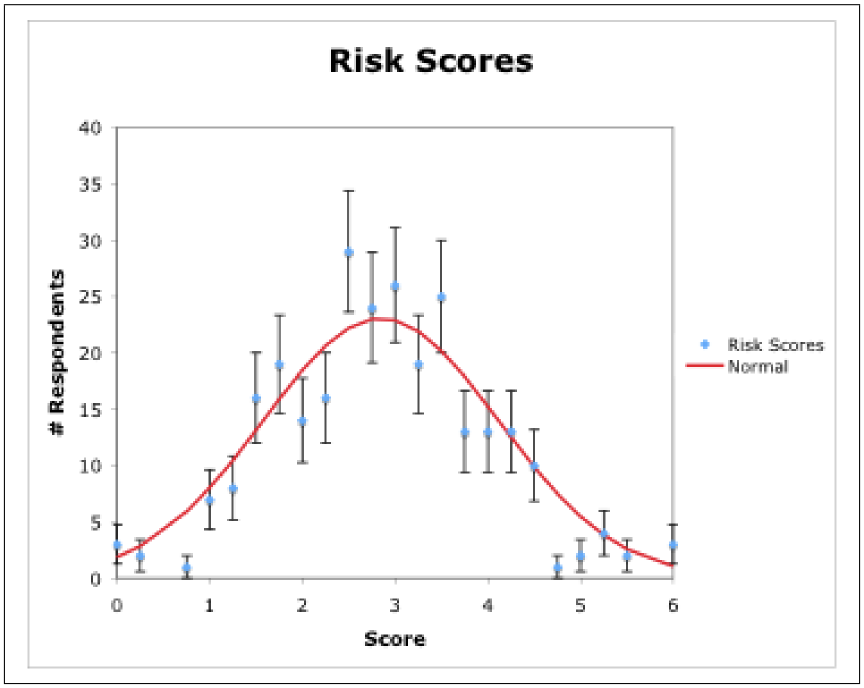


Figure 6.1: A histogram of the risk scores for the online concerns survey participants.

The histogram depicted in Figure 6.1 shows an approximately normal distribution for the risk scores. However, the PearsonÕs goodness of fit test fails to reject the null hypothesis that the data is normally distributed, where the 95% level (22 degrees of freedom) = 33.9 and χ^2 =26.4. The tails of the distribution contain people who have no regard for privacy and those who perceive a great deal of risk concerning their personal information online.

6.2.3 Concerns Scenarios

We asked participants to evaluate the likelihood of certain online scenarios and provide a rating on an 11-point Likert scale of how likely each scenario would be and also much “trouble” it would cause them if the scenario were to occur. We asked them to “think back to [their] last online purchase," and to “answer these questions considering that purchase and that online store." 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 youÕve 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)

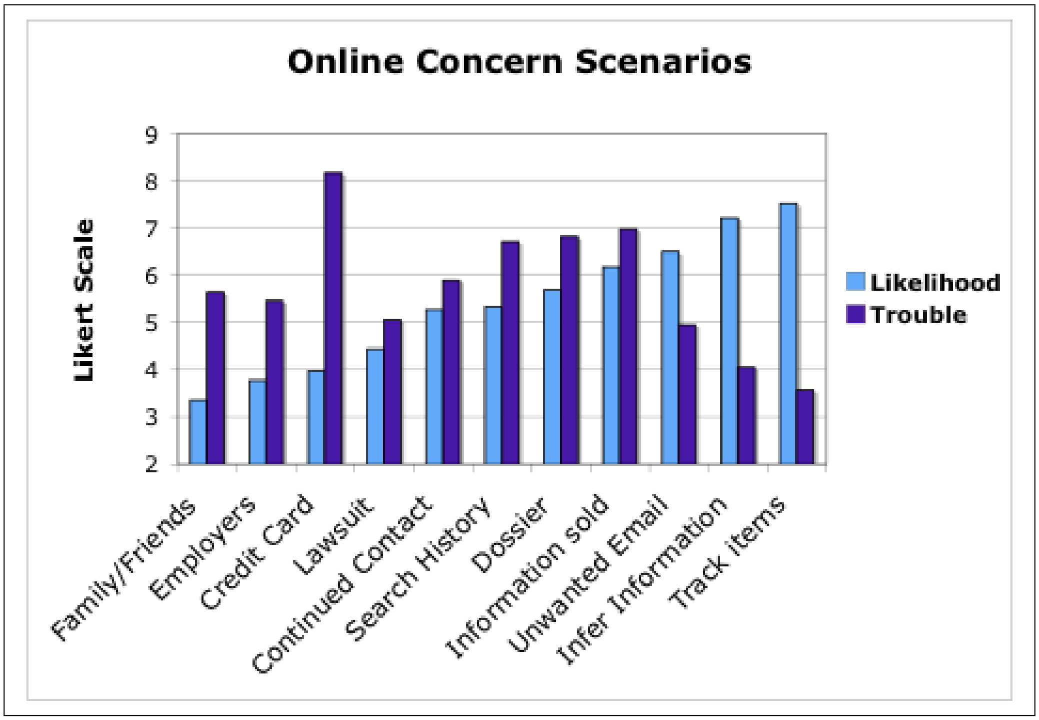


Figure 6.2: The online concerns scenarios and their trouble and likelyhood ratings.

The responses to the online concern scenarios are detailed in Figure 6.2. Based on participants' reports of their last online purchases, we can argue that many participants' answers probably were not based on a privacy concern raised by that particular purchase but instead reflect their privacy concerns when making typical purchases.

Respondents seem to be the least concerned with the scenarios that they found to be the most likely, including 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.

It seems that most people appear to realize that the websites they purchase from are tracking what items they click on to infer information about them. Some sites, like Amazon.com, make this obvious by recommending items to consumers based on their previous purchases the other items that people have clicked on. Of respondents who made their last purchase from Amazon.com, 73.8% rated both the tracking of information and the inferring of information with high likelihood (i.e., greater than a 5 on the Likert scale). In the entire sample, 79% rated the tracking of information with a high likelihood, and 77.5% rated the inferring of information high likelihood.

It is interesting to note that the survey participants found it more likely that their purchase history would be made available in a lawsuit than their purchase history being accessed by family or friends (M=4.4 and M= 3.4), t(275) = -6.6, $p <$ .0001. This seems surprising, especially if people share computers, email accounts, or passwords. Respondents also expressed the highest level of trouble related to the theft of their credit card numbers, M = 8.2 (99% CI = 7.8, 8.5), t(275) = 21.74, $p <$ .0001.

6.3 User Study Items

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 6.3 shows the list of items and their purchase likelihood scores.

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.

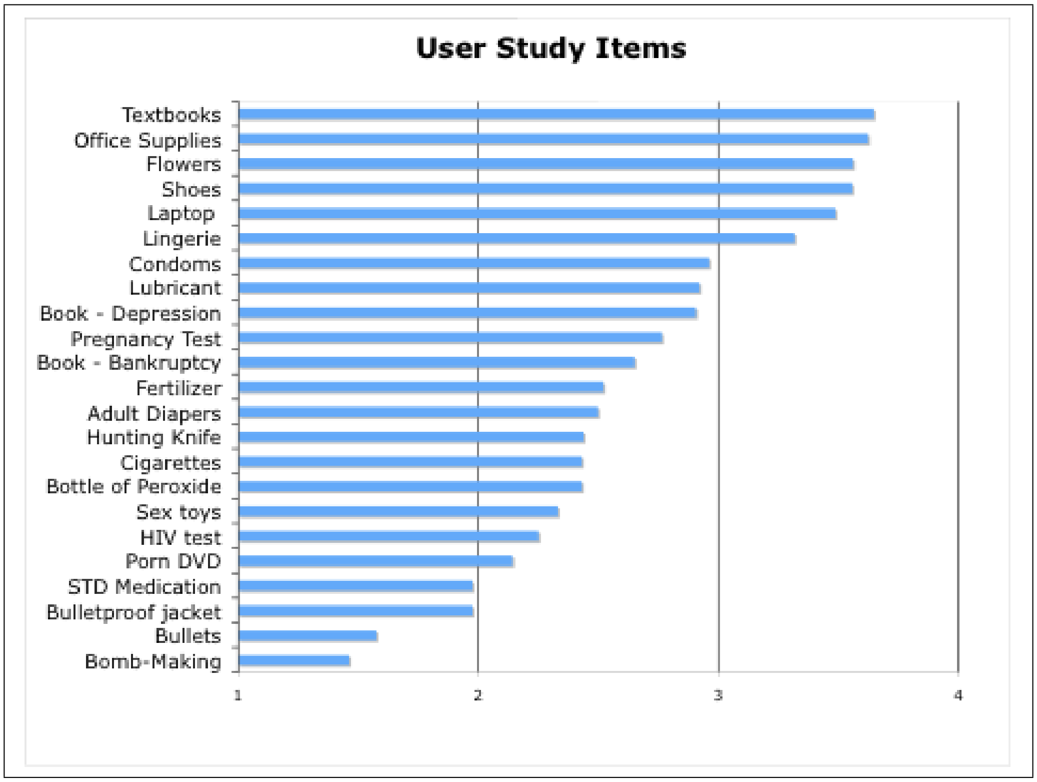


Figure 6.3: The user study items and levels of privacy-sensitivity.

6.4 Discussion

We examined online privacy concerns and risks to investigate the relationship between these concerns and privacy-protecting behaviors. The results are not necessarily representative of any particular population. However, they provide some general insights into attitudes about privacy. Similar to previous studies, we find that most people have concerns when they are on the Internet and when they shop online, but most do not read privacy policies in their entirety. Instead, they tend to notice the presence of privacy policies more often than they read them. It seems that people still find it difficult to get the privacy information they want, and instead, choose to bypass reading privacy policies, and just hope for the best.

It is interesting to see that people have generally realistic views of the relative likelihood of certain situations that could occur once their information is online. Most people seem to realize that the websites they purchase from are tracking what items they click on to infer information about them.

When asked about products that the participants would purchase in a user study, the post-9/11 political situation had an effect on responses. Items that people refused to buy dealt with items that could get them labeled as a terrorist; these items included bullets and a book on bomb-making.

Based on this preliminary survey, we find that P3P tools provide information that people find relevant to their privacy concerns. Our ongoing work will focus on conducting users studies to examine online purchasing behavior with the Privacy Finder P3P search engine. We aim to study whether, by lowering the barrier to finding privacy information, people may be able to make better and more informed decisions regarding the usage of their personal information online.

Chapter 7

Privacy Information Purchasing Study

> This chapter is largely a reproduction of a paper co-authored with Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti [114]. This work was supported in part by the National Science Foundation under grant CCF-0524189 and by U.S. Army Research Office contract no. DAAD19-02-1-0389 (Perpetually Available and Secure Information Systems) to Carnegie Mellon University's CyLab.

Previous privacy valuation studies have utilized several technique to elicit willingness-to-pay information. In this study, we focused on actual purchasing patterns, exposing users to the real risks of purchasing products online with the users' own credit cards. Participants were divided into three conditions: no privacy information, irrelevant information, and privacy information. Using a search engine interface, people searched for and purchased privacy-sensitive and non-privacy sensitive items. The results were ordered in such a way that the site with the highest privacy level also offered the products at the highest price requiring users to pay a premium for privacy. The results of this study show that users presented with privacy information will pay a premium to purchase privacy-sensitive and non-privacy sensitive items.

7.1 Experimental Design and Hypotheses

The Privacy Finder annotates search results with icons that represent a five-point privacy meter that represents how well a website's privacy policy matches the user's privacy preferences. The more the green boxes are filled, the better the match. We modified Privacy Finder for online shopping, submitting search queries via the Yahoo! shopping interface and returning search results annotated with product photographs and price information, as well as the privacy information described above.

	Female	Male	Mean Age
No Privacy Indicator	14	12	24.3 (σ = 7.08)
Irrelevant Information	11	8	32.4 (σ = 14.63)
Privacy Information	14	11	28.6 (σ = 9.71)

Table 7.1: Gender data for participants in each condition.

We randomly assigned participants to one of three experimental conditions. Gender and age information in available in Table **??**. Across all conditions, participants viewed the same set of search results in the same order. Sites were selected based on their privacy policies and the price of the product. Therefore, a site with 4 green boxes or high privacy indicator offered a high level of privacy protections regardless of whether or not participants were presented with privacy indicators in their set of search results. We compared participants' purchasing decisions in the following between-subjects design to gauge the impact of providing privacy information:

- *Condition 1 (control condition), No privacy indicator*: This group viewed search results without any annotations (as is the case with actual merchants in the status quo). Participants were given a version of the Search Engine Key that highlighted the type of data the search engine made visible: merchant names, product prices, photos, and so on. Search results during the experiment did not include any Finder icons. However, the natural language privacy policies were still accessible from the merchants' sites.
- *Condition 2 (control condition), Irrelevant information*: This group viewed search results annotated with icons representing irrelevant information. Participants were given a Search Engine Key that highlighted the presence of green box icons indicating a high or low Şrating calculated based on our analysis of the site's computer readable accessibility information for vision-impaired users. (Natural language privacy policies also remained accessible from the merchants' sites.)
- *Condition 3 (treatment condition), Privacy information*: Privacy icons and links to privacy reports were presented to this group. Participants in this condition were given a Search Engine Key that highlighted the presence of green box icons indicating a high or low privacy "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 (in addition to the baseline control condition of status quo information) to rule out

the possibility that the presence of an icon by itself would have as much influence on purchase decisions as the presence of privacy information. In previous studies, other content-free symbols (including credit card logos) have increased participants' willingness to trust certain sites [65].

The between-subjects design allowed us to test the following hypotheses:

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

Hypothesis 2: Participants in the privacy information condition will be more likely than those in the no privacy indicator condition to purchase from websites annotated with the four-green-boxes icon (the sites offering the best privacy policy).

For Hypothesis 1 and 2, when individuals are uncertain or ignorant of a merchant's privacy practices and the resulting potential for privacy issues, privacy concerns have little influence over the decision to make a purchase [6]. When merchants provide accessible privacy information, the consumer's utility function will give more salience and weight to privacy considerations; as a result, consumers in the privacy information condition should be more likely to purchase from merchants with better privacy policies.

In Hypothesis 2, we theorize that participants will be compelled to purchase from the site that offers the best privacy policy (four-green-boxes). This is not only because the privacy policy is available, but also because it is easy for the consumer to compare sites that offer high levels of privacy to those offering low and medium levels of privacy.

Hypothesis 3a: Participants presented with prominent privacy information (those in the privacy information condition) will be more likely than those in the no privacy indicator condition to pay a premium to purchase from sites that have better privacy policies.

Once salient information about privacy is provided and privacy considerations have a more significant role in the consumer's mind, one would expect some consumers to trade money for privacy. The decision to make this trade depends on the relative strength of their privacy and price sensitivities (see also [11]; and [109] for privacy models with price discrimination).

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

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

Hypothesis 4: Icons in the privacy information condition will affect purchase decisions more than icons in the irrelevant information condition.

This hypothesis is inspired by the literature on "institutional-based trust" that studies structures and situations that affect trust-based individual decision-making [81]. For instance, consumers often consider trust seals to be a proxy for merchant quality [92]. Hence, in the irrelevant information condition, the green icons visible through the interface may be interpreted as proxies of merchant quality regardless of their actual meaning (see also [65]). We wish to differentiate between the actual impact of privacy information and the impact of institutional-based trust; that is, we wish to rule out the possibility that consumers make decisions based solely on the presence of icons, regardless of their meaning. If Hypothesis 4 is supported, we will be able to conclude that our participants' purchasing decisions were affected more by privacy considerations than by the search engine interface itself.

7.2 The Study

7.2.1 Participant Recruitment

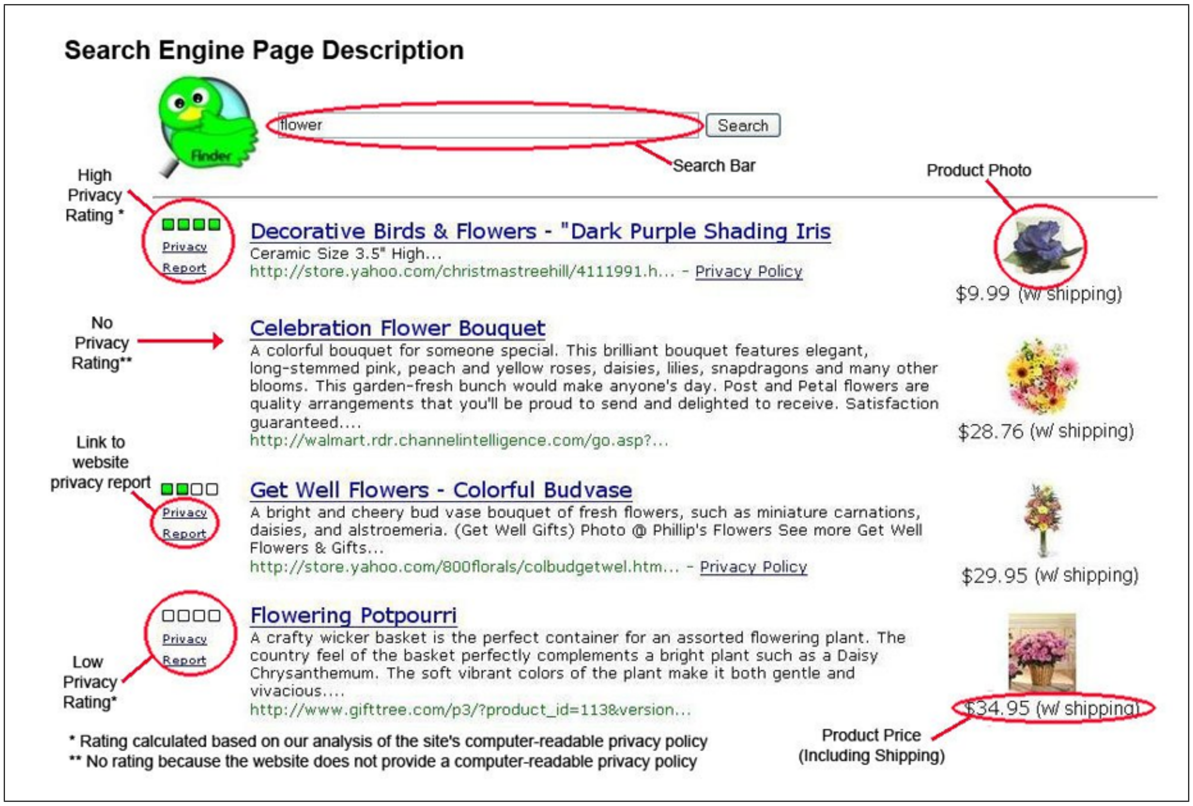
In October 2005 and November 206, participants were recruited from the general Pittsburgh population; there was no overlap between the participants in the online shopping experiment and the respondents to our online concerns survey. Participants were sought for an "Online searching and shopping study," with flyers posted around town, online in the Volunteers section of Craigslist, and via the Center of Behavioral and Decision Research at Carnegie Mellon. Participants had to be at least 18 years old, have a personal credit card to use during the study, and have experience shopping online. The flyer also advertised that participants would be paid to shop online using our money and would get to "Keep the change."

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 (α = 0.05, β = 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.

7.2.2 Screening Survey

Interested participants were directed to a preliminary survey online. We received 272 complete responses. Our study was designed to target individuals concerned with privacy rather than the population at large: we assumed that our search interface would be helpful to people with some online privacy concerns. We calculated a "risk score" for each participant and used it to screen out those who perceived online shopping to involve little or no privacy risk. 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 shopping session. Due to 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 they might consider when choosing a website for a purchase. These factors and their mean ratings are detailed in Section 9.4. Participants reported that they primarily base purchasing decisions on price, followed by return policy. Shipping speed, customer service, privacy policy, website design, and customer reviews were rated as equally important. We used participant ratings of these purchasing factors to determine which have minimal impact on purchasing decisions, an insight that we used to design the experimental conditions. The factor accessibility for sight-impaired users was found to have almost no impact on purchase intentions.



Search Engine Page Description

Decorative Birds & Flowers - "Dark Purple Shading Iris
Ceramic Size 3.5" High...
http://store.yahoo.com/christmastreehill/4111991.h... - Privacy Policy
$9.99 (w/ shipping)

Celebration Flower Bouquet
A colorful bouquet for someone special. This brilliant bouquet features elegant, long-stemmed pink, peach and yellow roses, daisies, lilies, snapdragons and many other blooms. This garden-fresh bunch would make anyone's day. Post and Petal flowers are quality arrangements that you'll be proud to send and delighted to receive. Satisfaction guaranteed....
http://walmart.rdr.channelintelligence.com/go.asp?...
$28.76 (w/ shipping)

Get Well Flowers - Colorful Budvase
A bright and cheery bud vase bouquet of fresh flowers, such as miniature carnations, daisies, and alstroemeria. (Get Well Gifts) Photo @ Phillip's Flowers See more Get Well Flowers & Gifts...
http://store.yahoo.com/800florals/colbudgetwel.htm... - Privacy Policy
$29.95 (w/ shipping)

Flowering Potpourri
A crafty wicker basket is the perfect container for an assorted flowering plant. The country feel of the basket perfectly complements a bright plant such as a Daisy Chrysanthemum. The soft vibrant colors of the plant make it both gentle and vivacious....
http://www.gifttree.com/p3/?product_id=113&version...
$34.95 (w/ shipping)

* Rating calculated based on our analysis of the site's computer-readable privacy policy
** No rating because the website does not provide a computer-readable privacy policy

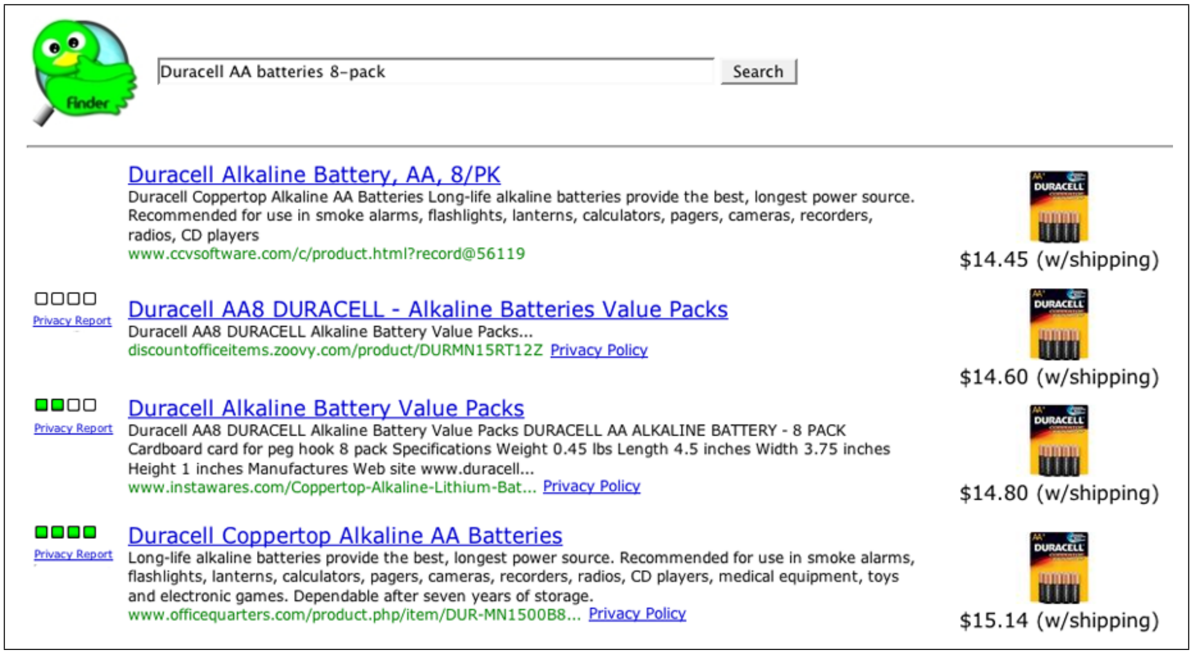
Figure 7.1: The search engine key provided to users in the privacy information condition.

7.2.3 Experiment Protocol

Participants were given an informed consent form when they arrived at our laboratory. After reading and signing the form, participants were given a search engine key. This key served as instructional material (see Figure 7.1), explaining the meaning of the icons and other user interface features. Participants in the three experimental conditions had nearly identical information, but the explanations of the icons differed. To reduce any framing and priming effects, Privacy Finder was renamed Finder, and participants did not see or have access to the privacy preference settings. Instead, based on the results of the online concerns survey, 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; a website's refusal to allow a user to remove their personal information from marketing lists; and the inability of users to view their own information on the site.

To familiarize participants with the interface and draw focus away from the purchasing tasks, participants across all conditions were asked to complete the same six search tasks; instructions for these tasks were provided one task at a time. Only the fourth and sixth tasks required participants to search for vendors selling a specified item (a pack of batteries and a sex toy, the order was randomized across participants) and use their credit card to actually purchase the product from the site of their choice. Participants were also asked to write down the website from which they had made their purchase along with the total price they paid. 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 perused websites.

We based our selection of the items participants purchased on the results of the online concerns survey (Section 6). We selected products that had an average cost of $15 per item, including shipping. These products also had to be available from a variety of real websites with diverse privacy policies. One item was an office supply product: an 8-pack of Duracell AA batteries; the other item was a vibrating sex toy, the “Pocket Rocket Jr." Participants used their own credit cards to pay for the products, which meant that their personal information was exposed to real merchants during the study. The websites were actual, real merchant sites, and they were chosen due to the very small likelihood that they would be familiar to the participants (to avoid confounding biases from brand effects). However, though the participants did not know it, we had preselected which merchant websites would appear during the users' searches for the online purchasing tasks. Purchasing either item (the batteries or the sex toy) forced individuals to reveal personal information (their credit card number) to unknown merchants; this arguably may have raised privacy concerns. However, one item (the sex toy) could be considered more personal and sensitive than the other, and may have therefore elicited greater concerns.



Duracell AA batteries 8-pack

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 Privacy Policy
$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... Privacy Policy
$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... Privacy Policy
$15.14 (w/shipping)

Figure 7.2: Search engine results interface for the Privacy Information condition..

7.2.4 Incentives and Reimbursements

We paid participants a two-part lump sum payment of $45 for their participation in the study. The participants kept the products and any money left over after the purchases were made. This design created a price incentive, encouraging participants to purchase from merchants with lower prices. To best capture the premium that participants paid for privacy, we ordered search results based on both privacy level and price across all conditions. The first item was the least expensive and was sold by a web site without a P3P policy (thus no privacy information was readily available). With each subsequent result, both the privacy level and the price increased, as shown in 7.2. Based on previous pilot studies, we found that participants were unlikely to browse beyond the first four search results. Thus, we did not focus on the specific order of privacy levels beyond the first four sites.

User study payments were made in two installments to prevent gaming the study (for instance, canceling the purchase after the study). At the end of the session, participants were given $10 in cash. Once the products shipped and the study participants sent us tracking numbers or product packing slips, they were mailed the remaining $35 payment.

Due to product availability and the fluctuation of product and shipping prices, we used marginally different sets of search results during the study while keeping both the price and privacy policy distributions fairly constant. The premium for high privacy batteries ranged from 3-5% of the product cost, while the premium for the sex toy ranged from 7-10%. Due to retailer problems that occurred during the purchasing tasks, as well as some participants' refusal to make some of the purchases, we continued to recruit participants until we had collected 48 complete responses for the study.

As stated above, participants paid for the products using their own credit cards and were later reimbursed a fixed amount. This means that both the privacy concerns (revealing personal information to a merchant site) and price incentives were real.

7.2.5 Exit Survey

Upon completion of the study tasks, participants completed an exit survey. We asked whether 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 whether those privacy policies influenced their purchasing decisions. This set of self-reported data was compared with and complemented the quantitative results of our experiment.

7.3 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 (even when those sites charged higher prices), while those in the control conditions generally made purchases from the lowest priced vendor. This indicates that individuals are likely to pay a premium for privacy when 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 merchant features, were less likely to take those indicators into consideration when making purchases. This demonstrates that the observed behavior cannot simply be attributed to an interest in purchasing from web sites labeled with attractive indicators.

% Purchases	Condition 1: No Privacy Indicator	Condition 3: Privacy Information	Fisher's Exact p
Battery	11.1% n = 2/18	77.7% n = 14/18	$<$.0001
Sex Toy	16.0% n = 4/25	66.7% n = 14/21	$<$.005

Table 7.2: A between-conditions comparison of the proportion of purchases made from sites corresponding to those annotated with icons in the privacy information condition. To test for significance between these proportions we used the Fisher's Exact test.

7.3.1 Meaningful Privacy Information

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

One of the goals of this study was to determine whether participants presented with salient privacy information would be more likely to purchase from sites with privacy indicators than participants who did not see that information. As shown in Table 7.2, we found that to be the case.

For both products, participants in the privacy information condition made a greater proportion of purchases from sites that displayed privacy icons. Participants in the no privacy indicator condition were significant less likely to purchase from the corresponding sites. These results indicate that people choose sites with better privacy policies when they are provided with privacy information in a more salient format.

Hypothesis 2: Participants in the privacy information condition will be more likely than those in the no privacy indicator condition to purchase from websites annotated with the four-green-boxes icon (the sites offering the best privacy policy). **- Supported**

When shopping for batteries, participants in the privacy information condition made significantly more purchases from the four-green-box “high privacy site" (47.4%) than participants in the no privacy indicator condition (5.6%), chi2 =10.6, df = 2, N = 53, p = 0.005. For the sex toy purchases, participants in the privacy information condition also made significantly more purchases from the high privacy site (33.3%) than participants in the no privacy indicator condition (0%), chi2 = 16.1, df = 2, N = 64, p = 0.0003.

7.3.2 Privacy Premium

Hypothesis 3a: Participants presented with prominent privacy information (those in the privacy information condition) will be more likely than those in the no privacy indicator condition to pay a premium to purchase from sites that have better privacy policies. **- Supported**

As stated previously, this experiment was also designed to determine whether individuals would be willing to pay a premium for enhanced privacy protection (though it is important to note that the goal of the study was not to quantify a specific premium for the selected products). When comparing the no privacy indicator condition to the privacy information condition, we found statistically significant privacy premiums of roughly 60 cents for both products, as detailed in Table 7.3. Note that, to achieve a realistic design, we relied on actual merchants' prices. 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 sex toy was replaced with a slightly more expensive result. All of

	Condition 1: No Privacy Indicator	Condition 3: Privacy Information	Premium	p value
Mean Price: Batteries	\$14.64	\$15.23	\$0.59	$<$0.001
Mean Price: Sex Toy	\$15.26	\$15.88	\$0.62	$<$0.001

Table 7.3: A t-test comparisons of mean prices paid in the no privacy indicator condition and the privacy information condition.

	Lowest Priced Battery Purchases	Lowest Priced Sex Toy Purchases
Condition 1: No Privacy Indicator	83.3%	80.0%
Condition 2: Irrelevant Information	75.0%	66.7%
Condition 3: Privacy Information	21.1%	28.6%
χ^2 Value	17.3	13.1
p Value	0.0002	0.002

Table 7.4: χ^2 test comparing the proportions of purchases made at the sites offering the lowest price for the batteries and the sex toy.

these changes were on the order of a few cents; we found no evidence that these changes impacted purchase decisions. Based on t-tests, we found that individuals shown privacy information were significantly more likely ($p < 0.001$ in both cases) to pay a premium to purchase from sites with better privacy policies. This effect was present for purchases of the privacy-sensitive item as well as the non-privacy sensitive item.

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

Examining the number of purchases made at the websites offering the lowest prices, we see that participants in the control conditions tended to purchase both items from the least expensive website, as denoted in Table 7.4.

	Condition 2: Irrelevant Information	Condition 3: Privacy Information	Fisher's Exact p
% of battery purchases	25.0% n = 4/16	77.7% n = 14/18	$<$.0001
% of sex toy purchases	27.8% n = 5/18	66.7% n = 14/21	$<$.005

Table 7.5: A between-conditions comparison of the proportion of purchases made from sites annotated with icons. To test for significance between these proportions we used the Fisher's Exact test.

	Condition 1: No Privacy Indicator	Condition 2: Irrelevant Information	Fisher's Exact p
% of battery purchases	11.1% n = 2/18	25.0% n = 4/16	$<$.0001
% of sex toy purchases	27.8% n = 4/25	27.8% n = 5/18	$<$.005

Table 7.6: A between-conditions comparison of the proportion of purchases made at sites with icons in the irrelevant information condition and the corresponding sites in the no privacy indicator condition.

7.3.3 The Impact of Icons

Hypothesis 4: Icons in the privacy information condition will affect purchase decisions more than icons in the irrelevant information condition. **- Supported**

When comparing the proportions of purchases made from sites with icons, we found statistically significant differences in purchase patterns between participants who were presented with privacy indicators and those who were presented with indicators representing irrelevant information (Table 7.5). Unlike the former, participants who saw icons associated with irrelevant information were not likely to purchase from sites annotated with green box icons. This implies that our results can be attributed primarily to the actual privacy signals carried by the icons.

	Condition 1: No Privacy Indicator	Condition 3: Privacy Information	Premium	p value
Mean Price: Batteries	\$14.64	\$15.23	\$0.59	$<$0.001
Mean Price: Sex Toy	\$15.26	\$15.88	\$0.62	$<$0.001

Table 7.7: Comparison of mean price paid for each product in the control conditions. Based on a t-test, there was no significant difference between the control conditions.

Additionally, as detailed in Table 7.6, we detected no statistically significant differences between the two control conditions' purchasing patterns. This table indicates that there was no significant difference between the no privacy indicator and irrelevant information conditions in terms of purchases made at sites with icons.

Similarly, when using a t-test to compare the average purchase prices of the no privacy indicator group with the purchase prices of the irrelevant information group, we did not find significant differences in the prices paid for each product, as shown in Table 7.7.

Figure 7.3 also clearly depicts the different purchase patterns between conditions. For both items, a greater percentage of purchases were made at four-green-box sites in the privacy information condition than in the no privacy indicator and irrelevant information conditions. The proportion of purchases made at sites with irrelevant icons is somewhat larger than the proportion made at sites with no privacy indicator; however, as noted above, this difference is not significant. More importantly, while we may have found that irrelevant icons motivate some participants to purchase from certain sites, we also found that the impact of such icons is far less than the impact of clearly annotated privacy information.

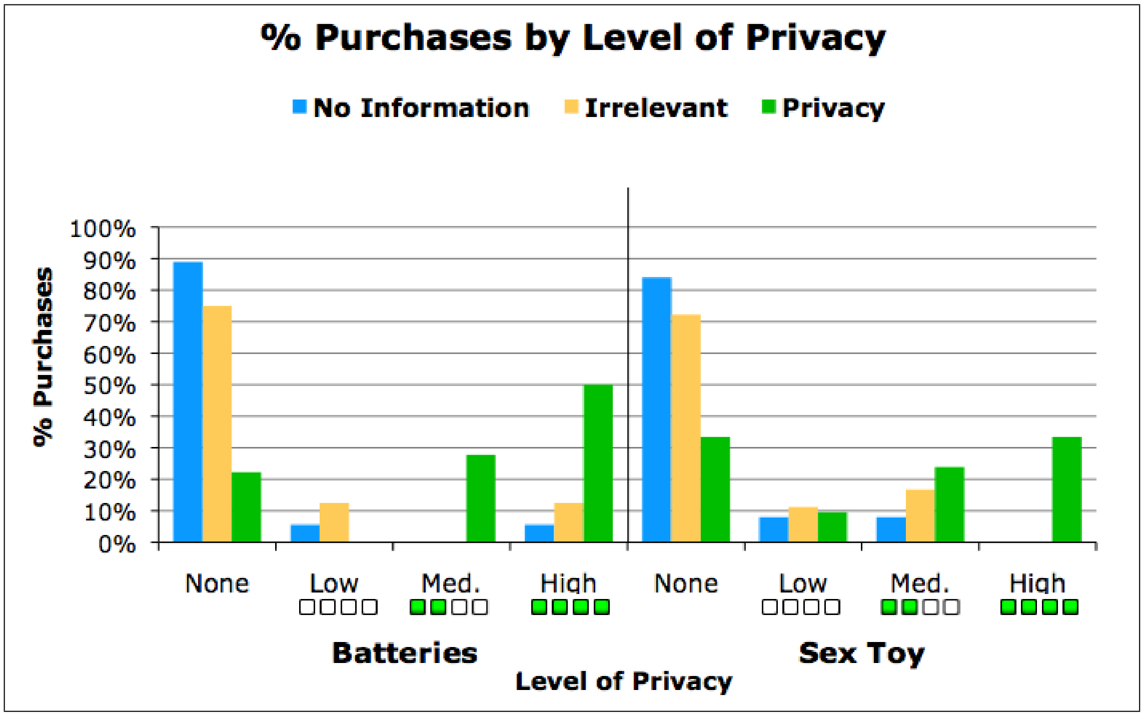


Figure 7.3: The percentage of purchases made for each product, by level of privacy, for each condition.

7.3.4 Other Results from the Exit Survey

In the exit survey, we asked whether the privacy icon (if seen) influenced participants' purchasing decisions, whether participants understood what the icon represented, whether they read any of the privacy policies, and whether those privacy policies influenced their purchasing decisions. Overall, the privacy icons served as an effective means for communicating privacy information. In the privacy information condition, 92% noticed the 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%).

Providing visible privacy information heightened privacy awareness for the batteries, an innocuous item. When asked in the exit survey about their battery purchase decision, participants in the privacy information were more likely to write in “privacy” or “privacy policy” when identifying the factor that most influence their decision than participants in the no indicator condition (32% vs. 0%; Fisher’s Exact p =.001).

These results indicate that once people were provided with salient privacy information, they chose sites they considered privacy protective; furthermore, they perceived differences in the level of privacy offered by sites annotated with the high, medium and low privacy icons.

7.4 Limitations

Our study was not designed to establish whether the premium consumers were willing to pay for privacy should be interpreted in absolute terms (roughly 60 cents) or relative ones (roughly 4% of the price of the goods in question). However, the literature in the areas of marketing and behavioral economics suggests a number of plausible inferences, which further experiments could help us validate. These fields of research indicate that consumers’ valuations are highly dependent on framing [69], relative changes in price, and relative comparisons ([68, 98]). As exemplified by Equation [1], participants in our experiment could assess the price charged by privacy protective merchants (for instance, $15.14 for a set of batteries) against two other reference points: 1) the value of protecting their privacy; and 2) the price charged by other (less protective) merchants. Since the benefits of privacy protection are often uncertain and intangible [10], we can expect that consumers are likely resort to relative comparisons when they try to determine the value of protecting their privacy, and therefore will assess privacy premiums in relative (percentage) terms. However, evidence also suggests that the willingness to pay for privacy is, ultimately, bounded [52]. With regard to the prices charged by other merchants, the literature suggests that, for low-price products, consumers pay more attention to price premiums expressed in percentage terms. For high-price products, however, consumers are more likely to be affected by price premiums expressed in absolute dollar amounts (see [98]). In the case of our relatively inexpensive user study products (batteries and sex toys), consumers may have perceived a 4% premium - around 60 cents - to be an acceptable amount to pay for privacy; however, if the price of the items increased, a percentage of 4% would become a larger and larger amount in absolute dollar terms - an amount capable of dissuading more consumers from paying for privacy. Combining these two lines of reasoning, we can expect the privacy premium to be a percentage of the absolute price of a good that decreases as that absolute price rises; furthermore, this premium is likely bounded in absolute dollar terms: a consumer purchasing a $20,000 luxury item may be willing to allocate $20 to make her transaction more confidential (this amount would represent more than the 60 cent premium in our scenario), but arguably not as much as $800 (the equivalent to our 4% premium). Future research will be necessary to pinpoint the exact trade-offs between price and privacy sensitivity.

Lastly, while our participants made purchases using their own credit cards, the purchases were made in a laboratory setting following a specific experimental protocol. This setting is not necessarily reflective of ordinary search activity. To better determine the impact of prominent privacy information in a more natural setting, we plan to conduct a field study in which participants are asked to use Privacy Finder over a period of months. This may allow us to measure the impact of privacy information on people's everyday searches.

7.5 Implications and conclusions

The goal of this study was to determine whether the availability and accessibility of privacy information affects individuals' purchasing decisions. In turn, investigating that question allowed us to discuss whether businesses can leverage privacy protection as a selling point. Our study focused on what occurs when a search engine prominently displays privacy ratings for web sites. We used a modified version of Privacy Finder to display the privacy policies of certain online shopping sites in a fashion that, arguably, reduces the information asymmetry that separates merchants and customers vis a vis the usage of the customer's data. Our experimental approach was designed to investigate the impact of more prominent and accessible privacy information on consumer purchasing behavior in a realistic setting; this approach differs from the current method of making privacy practices information available via privacy policies.

Our results offer new insight into consumers' valuations of personal data and provide evidence that privacy information affects online shopping decision-making. We found that participants provided with salient privacy information took that information into consideration, making purchases from websites offering medium or high levels of privacy. Our results indicate that, contrary to the common view that consumers are unlikely to pay for privacy, consumers may be willing to pay a premium for privacy.

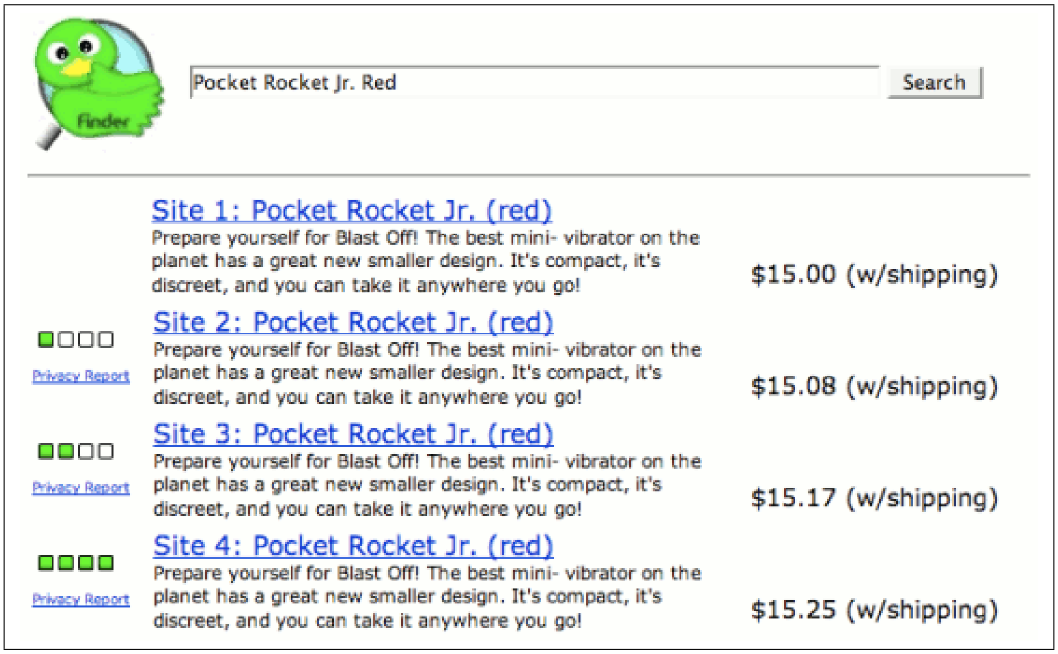
The results of this study suggest that future research needs to estimate the relationship between privacy and price sensitivity; in addition, researchers must work to achieve a more granular understanding of the behavioral and cognitive factors that influence a consumer's decision when privacy information is made more accessible. Our results also indicate that businesses may use technological means to showcase their privacy-friendly privacy policies and thereby gain a competitive advantage. In other words, businesses may direct their policies and their information systems to strategically manage their privacy strategies in ways that not only fulfill government best practices and self-regulatory recommendations, but also maximize profits. Specifically, if the adoption of P3P increases, businesses protective of customer privacy may be able to attract consumers by posting their P3P policies and signaling "good" privacy practices. Survey data indicates that online consumers greatly value insight into what will be done with their personal information and how they can control those processes ([77]). While consumers are often unable to control the practices of those who collect their information, they can control who they share their information with and the type of information they provide.

Chapter 8

Privacy Premium Survey

To standardize the comparison of the purchases of privacy-sensitive and non-privacy sensitive items, I conducted an online survey to estimate the maximum premium that participants would be willing to pay to purchase from a website with a high privacy level. Participant were presented with screen shots of search results and product prices (with shipping) for a privacy-sensitive and a non-privacy sensitive product and asked to rate from which site they would pick to make their purchase. The results of this study inform the design of the next privacy information focused purchasing study.

Search results without privacy indicators in Privacy Finder are sites where the website simply has not created a privacy policy. It provides no indication of how good of a privacy policy that site has. To investigate user's perceptions of results without privacy indicators, we divided participants into two conditions: one where the cheapest website did not have a privacy indicator, and the other where the cheapest website had the lowest privacy level.



Pocket Rocket Jr. Red

Site 1: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.00 (w/shipping)

🟩☐☐☐
Privacy Report
Site 2: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.08 (w/shipping)

🟩🟩☐☐
Privacy Report
Site 3: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.17 (w/shipping)

🟩🟩🟩🟩
Privacy Report
Site 4: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.25 (w/shipping)

Figure 8.1: Example screenshot used in the privacy premium survey.

8.1 Experimental Design

We recruited 676 Internet users through Craigslist and sweepstakes websites in June 2008. The majority of the respondents were female (74.3%) and highly educated (74.5% with college degrees or graduate education). The survey contained five pages of Privacy Finder screenshots (Figure 8.1). Each screenshot depicted four search results for identical products with identical descriptions. The search results only differed based on the privacy indicator placed to their left and the price information placed to their right. Both the price and privacy level increased with each subsequent search result. Thus, the websites with the highest privacy ratings also had the highest prices.

We assigned half the respondents to a between-group condition in which the cheapest website had no privacy indicator and the other half to a condition in which the cheapest

Indicator	Premium 1	Premium 2	Premium 3
☐☐☐☐	\$15.00	\$15.00	\$15.00
🟩☐☐☐	\$15.08	\$15.25	\$15.50
🟩🟩☐☐	\$15.17	\$15.50	\$16.00
🟩🟩🟩🟩	\$15.25	\$15.75	\$16.50

Table 8.1: The privacy premiums and associated privacy indicators used in the survey. The privacy indicator for the cheapest website was only displayed to half of the respondents.

website had the lowest privacy level. The product displayed in the search results alternated between the sex toy and pack of batteries that laboratory participants would be purchasing, with the order randomly selected. Respondents were given the following instructions:

> “Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.”

Respondents were exposed to two of three possible premiums for the highest privacy—denoted by four green boxes: \$0.25, \$0.75, and \$1.50. The premiums and associated privacy indicators are shown in Table 8.1. The privacy premiums were randomly assigned so that respondents saw the same premium for the first two pages (i.e. respondents saw the same premium for both products). The third page of the survey contained a control where one of the two products was randomly displayed with identical prices for each of the four search results. The privacy indicators varied so that we could examine whether participants would select the website with the highest privacy level in the absence of a premium.

The fourth and fifth pages followed the same protocol as the first and second pages, but participants were randomly assigned one of the two privacy premiums they had not already seen. However, we decided not to include these results in the analysis since we found evidence that participants' willingness to pay the subsequent premiums was highly dependent on the first premium to which they were exposed.

8.2 Data Analysis

We combined the two between-group conditions for the analysis when we discovered that the only difference occurred when respondents encountered the highest privacy premium: those selecting the batteries were significantly more likely to select the first website—the cheapest one—when the indicator was absent ($t_{239} = 2.175$, $p < 0.031$).[1]

The ideal privacy premium for our laboratory study is the highest one that survey respondents would be willing to pay for both products; the survey responses likely provided an upper bound because the respondents reported how much they *would* pay without actually having to pay that amount. Using ANOVA to compare the three privacy premiums for each of the two products we found no significant differences between the three premiums when respondents considered the sex toy: most respondents indicated they were willing to pay any privacy premium presented to them. However, when the privacy premium was \$1.50, respondents were more likely to purchase the batteries from cheaper vendors, and therefore unwilling to pay a premium for privacy ($F_{2,673} = 6.251$, $p < 0.002$). At the same time, respondents indicated they were still willing to spend \$0.25 and \$0.75 for increased

---

[1] For a privacy premium of \$1.50, users may purchase from a website with an unknown privacy policy (i.e. the cheapest website) if the item being purchased does not raise privacy concerns.

privacy when purchasing the batteries. We concluded a privacy premium of $1.50 would be too high for our laboratory experiment.

A pairwise t-test confirmed that a $0.75 privacy premium would still allow us to observe differences between the two products. Respondents indicated they were willing to spend significantly more money for the sex toy—in exchange for greater privacy—than for the batteries ($t_{214} = 5.226$, $p < 0.0005$). We concluded that a $0.75 privacy premium would be low enough that laboratory participants would consider paying it for both products, while still allowing us to observe differences in behavior between the two product purchases.

Due to the ambiguity surrounding websites without privacy indicators (one could select the cheapest site and hope that while it doesn't have a P3P policy, the website's natural language policy is a “good" one), we decided to provide a low privacy indicator (a indicator where all the boxes are not green) for the cheapest website in the following purchasing study.

Chapter 9

Privacy Information Timing Purchasing Study

This chapter is largely a reproduction of a paper co-authored with Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti [45]. Thanks to Daniel Rhim for his assistance carrying out this study. We are also grateful to the companies who participated: EdenFantasys.com, Instawares, Little Office Supply, NiteTimeToys.com, Office Quarters, On Time Supplies, SheVibe, and The Dirty Bunny. This work was supported in part by the National Science Foundation under grant CCF-0524189 and by U.S. Army Research Office contract no. DAAD19-02-1-0389 (Perpetually Available and Secure Information Systems) to Carnegie Mellon University's CyLab.

To examine the impact of the timing of the presentation of salient privacy information on online purchasing decisions, participants purchased privacy and non-privacy sensitive products using the Privacy Finder search engine interface. The timing of privacy indicators tested were the following: not at all (instead, users were presented with irrelevant indicators in the search engine interface as the control), alongside search engine results, in a frame above the destination website, or on an interstitial webpage after clicking a search result and before viewing the destination website. Vendors collaborated with this study, setting the prices for the user study items based on a premium survey completed prior to the study. Participants who viewed the privacy indicators in the search engine interface were the most likely to pay a premium for high privacy when purchasing privacy-sensitive items.

The laboratory experiment tested the following hypotheses:

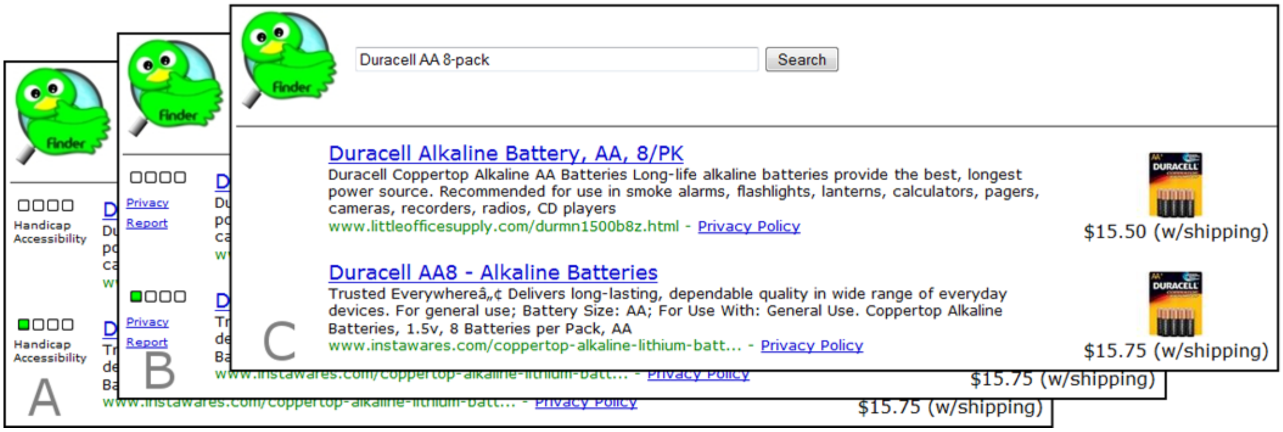
Hypothesis 1: Participants will pay for increased privacy when they see privacy indicators.

Hypothesis 2: Participants who see privacy indicators will pay more for the privacy-sensitive item than the item that does not raise additional privacy concerns.

Hypothesis 3: Participants will be more likely to pay for increased privacy when they see privacy indicators alongside search results before visiting a website than when they see privacy indicators after clicking on search result links.

Hypothesis 4: Participants will be more likely to pay for increased privacy when they see privacy indicators before they see the content of a website than when they see privacy indicators alongside the content of a website.

Hypothesis 5: Participants who see privacy indicators after clicking on search result links will visit more websites than those who see privacy indicators alongside search results.



Duracell AA 8-pack

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.littleofficesupply.com/durmn1500b8z.html - Privacy Policy
$15.50 (w/shipping)

Duracell AA8 - Alkaline Batteries
Trusted Everywhereâ„¢ Delivers long-lasting, dependable quality in wide range of everyday devices. For general use; Battery Size: AA; For Use With: General Use. Coppertop Alkaline Batteries, 1.5v, 8 Batteries per Pack, AA
www.instawares.com/coppertop-alkaline-lithium-batt... - Privacy Policy
$15.75 (w/shipping)

Figure 9.1: Screenshot of the search results for the four study conditions: (A) participants in the *handicap* condition saw the handicap accessibility indicators; (B) participants in the *privacy* condition saw the privacy indicators; and (C) participants in the *frame* and *interstitial* conditions did not have annotated search results.

9.1 Study Design

We conducted a laboratory experiment during the summer of 2008 using participants from the Pittsburgh area. We recruited 89 participants using Craigslist and flyers on bus stops, telephone poles, and community bulletin boards. We used a screening survey to gather basic demographic data and to assess privacy concerns related to using the Internet and online shopping. Because the privacy indicators we tested were designed for use by individuals who have privacy concerns when shopping online, we used the same screening survey and screening methodology used in our previous study to screen out those who perceived little or no privacy risk when shopping online [113]. Based on this requirement, we screened out 16.39% (50 of 305) responses.

We selected the same purchase items from the Privacy Information Purchasing Study (Section 7): the “Pocket Rocket Jr.,” as the privacy-sensitive item and an 8-pack of Duracell

Hit #	Indicator	Price
1	☐☐☐☐	$15.50
2	🟩☐☐☐	$15.75
3	🟩🟩☐☐	$16.00
4	🟩🟩🟩🟩	$16.25
5		$16.75+

Table 9.1: The prices and privacy ratings for both sets of search results, the batteries and the sex toy. Participants who wanted the highest level of privacy had to pay an additional $0.75 for each product.

AA batteries as the item unlikely to raise additional privacy concerns. We tightly controlled the price of each item by collaborating with four office supply vendors and four sex toy vendors who had varying privacy policies.[1] We asked the vendors to set specific prices based on their privacy policies and the results of our privacy premium survey.[2] Privacy Finder returned static results pages when specific search strings (or variants thereof) were submitted: “Pocket Rocket Jr. Red” and “Duracell AA 8-pack.” Each of these two pages of search results contained five hits with varying prices and privacy ratings, as seen in Table 9.1. In both sets of search results we also included a fifth search result that did not have a privacy rating. This website had the highest price of the five and was included because we were curious if any participants would pay more than the $0.75 privacy premium to buy from a website with an unknown privacy policy, and whether they would understand that the lack of any indicator corresponds to an unknown privacy policy.[3]

---

[1] We contacted over twenty vendors for each product until four vendors for each product agreed to participate. For the vendors who lowered their prices, we compensated them for the difference. We only contacted vendors who participants were likely unfamiliar with; a full list of the vendors appears in the Acknowledgements.

[2] We used a privacy premium of $0.75 based on the results of the survey. Due to vendor constraints we had to set the base price at $15.50 rather than the $15.00 we used in the premium survey.

[3] No subject purchased either product from this website, and we therefore do not mention it in the analysis.

We randomly assigned participants to one of three experimental conditions or the control condition, balancing the gender of participants in each condition:

- *Handicap Accessibility (control)*: Participants were shown annotated search results (Figure 9.1A). However, we labeled the privacy indicators as "handicap accessibility" so that the indicators were not associated with privacy. The links to the privacy reports (i.e. the machine-generated privacy policy summaries) were removed.[4] We used this condition to examine whether participants in the other conditions were genuinely thinking about privacy or whether they were choosing websites simply based on the presence of irrelevant green indicators.
- *Privacy (experimental)*: Participants were shown annotated search results with privacy indicators (Figure 9.1B).
- *Frame (experimental)*: Participants were shown search results that were not annotated (Figure 9.1C). Once a participant visited a website from the search results, a frame appeared at the top of the website that displayed the privacy indicator and a link to the privacy report (Figure 9.2). We created this condition to simulate the Privacy Bird experience: users who wanted to comparison shop based on privacy indicators would have to visit a website in order to see its privacy rating. We hypothesized that users would find this tedious and therefore make poor privacy choices, especially when purchasing the batteries since they would likely be less motivated to protect their privacy.
- *Interstitial (experimental)*: Participants were shown search results that were not an-

---

[4] Privacy reports are not discussed anywhere else in this paper since too few participants clicked them for us to draw any conclusions.

notated (Figure 9.1C). Once a participant visited a website from the search results, they saw an interstitial—a full screen message—with the privacy indicator (Figure 9.3). We created the interstitial condition to examine whether the content of a website detracted from the privacy indicator. We wanted to control for users being able to view website content alongside the privacy indicator in the *frame* condition. We hypothesized that users would choose higher privacy in this condition because they would be making the decision solely based on the privacy indicator.

	Female	Male	Mean Age
Handicap	12	10	27.6 (σ = 9.32)
Privacy	12	10	31.3 (σ = 13.45)
Frame	12	10	31.9 (σ = 12.90)
Interstitial	12	11	30.1 (σ = 13.35)

Table 9.2: Gender data for participants in each condition.

The demographics of each condition are summaries in Table 9.2. We found no significant differences between the average ages ($\mu = 30.24, \sigma = 12.253$) of the groups. Differences paid for each product by gender were not significant ($t_{87} = 1.73$, $p < 0.087$ for the sex toy; $t_{87} = 0.96$, $p < 0.34$ for the batteries). We therefore believe the groups consisted of comparable populations.

Our flyers solicited participants for a study on the usability of an online search engine so that we would not prime participants to privacy. The flyers informed participants that we would be paying them to shop online and that they would “Keep the Change!" When participants arrived for the experiment, we handed them instruction sheets that labeled the various features of Privacy Finder: the search box, the list of results, the annotated price information, the product pictures, and the privacy indicators. All references to “Pri-

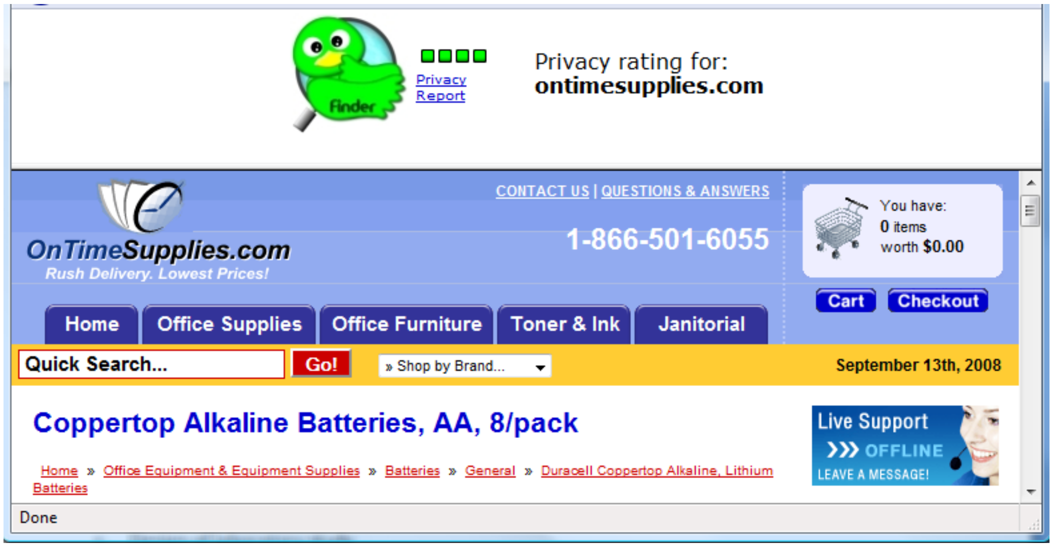


Figure 9.2: Screenshot of a website in the *frame* condition.

vacy Finder” were changed to “Finder” in order to reduce priming effects. Likewise, we scheduled all participants at least 72 hours after taking our privacy concerns screening survey.

We gave participants packets that instructed them to complete several information retrieval tasks in addition to the two purchasing tasks in order to familiarize them with the interface and to conceal the purpose of the study. The tasks included searches for boot prices, prices and average lifetimes of light bulbs, and the prices and available sizes of tote bags. After two information retrieval tasks, participants used Privacy Finder to find websites offering either the sex toy or the batteries and purchased these products. The order in which participants purchased these two items was assigned randomly. The instructions specified the search strings to use to find these products. Unbeknownst to participants, these search strings returned our static search results.

Participants conducted additional information retrieval tasks between the first and sec-

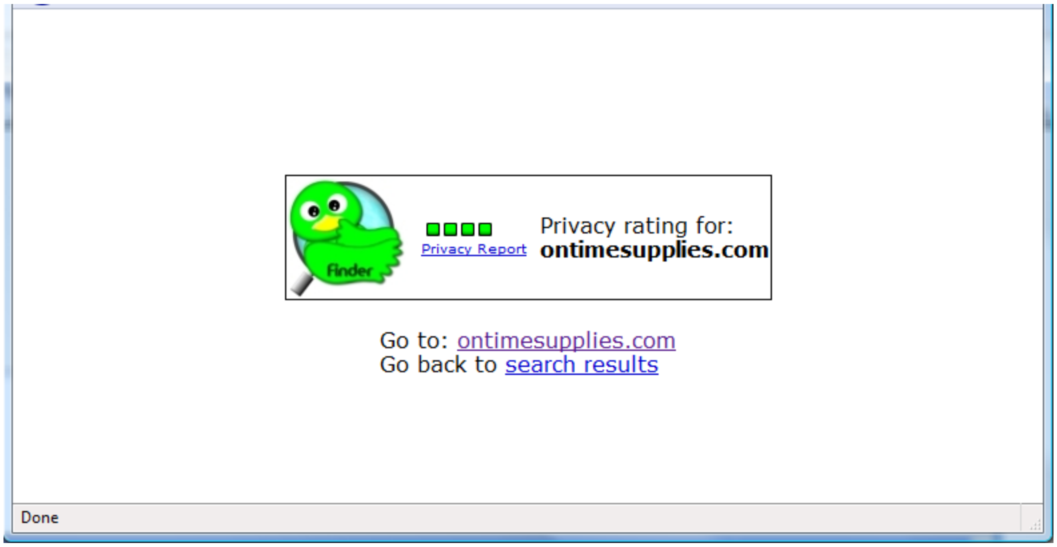


Figure 9.3: Screenshot of a website in the *interstitial* condition.

ond purchases. If they had purchased the batteries first, they purchased the sex toy second, and vice versa. After the second purchase, participants completed an online exit survey that asked questions about their purchases and overall reactions. They were required to use their own credit card and billing information for both purchases so that they would treat the purchases as “real" purchases. However, we allowed them to ship unwanted items to our laboratory. To prevent gaming of the study, we gave participants $10 in cash for completing the laboratory experiment and then another $40 by mail once we had confirmation that their orders had been shipped.[5]

---

[5] We asked participants to mail us invoices or email us tracking numbers for their purchases so that they would not plan to cancel their orders after they left our laboratory (which would make item prices less of a factor since they would not actually pay for them).

9.2 Analysis

Our most significant finding was that the timing of privacy indicator display had a highly significant impact on the behavior of participants who chose to make a purchase on the first website they visited. Those participants paid for increased privacy only when their search results were annotated with privacy indicators; participants who saw the indicators at a later time were significantly more likely to ignore them. Participants who chose to comparison shop by visiting several websites before making a purchase were influenced by the privacy indicators regardless of when they were displayed. Likewise, participants' reliance on the privacy indicators also depended on whether or not they were purchasing the privacy-sensitive item, as well as the strength of the privacy indicator to which they were exposed.

In this section we describe how purchasing behaviors changed when participants were exposed to privacy indicators. Next, we examine how privacy concerns and purchasing behaviors varied based on the type of product being purchased. Finally, we detail how the timing of the privacy indicators resulted in very nuanced behaviors regarding the prices participants paid for the items, how website content had less of a role than we expected, and how timing had an impact on the number of websites participants visited.

9.2.1 General Effects of Privacy Indicators

Hypothesis 1: Participants will pay for increased privacy when they see privacy indicators.

We compared the average price paid by participants in the control (*handicap*) condition

Condition	Battery Premium	Sex Toy Premium
Handicap	$0.15	$0.11
Privacy	$0.34	$0.52
Frame	$0.26	$0.41
Interstitial	$0.39	$0.49

Table 9.3: The average privacy premiums paid for both products across all four study conditions. This is the amount paid above the $15.50 base price for increased privacy.

with the average price paid by participants in the three experimental conditions to determine whether participants would pay more to shop at sites with privacy indicators than they would to shop at sites with irrelevant green indicators. We performed an ANOVA to compare the prices paid for each product between each of the experimental groups and found that when purchasing the sex toy, participants in the three experimental groups paid significantly more than participants in the *handicap* condition ($F_{3,85} = 7.938$, $p < .0005$). However, while participants in the experimental groups also paid more for batteries than those in the *handicap* condition, we did not observe any significant differences in price paid for batteries between the conditions. We concluded that participants were influenced by privacy indicators rather than by irrelevant indicators. Table 9.3 shows the average premium that participants paid for each product across all four conditions.

Our observed data corroborated the exit survey data: participants who did not see privacy indicators were less likely to consider privacy when making their purchases. We provided participants a text box on the exit survey to enter the biggest factor that they considered when making each purchase. In the *handicap* condition, 82% of participants indicated price was the primary factor during the battery purchase, and 86% indicated price for the sex toy purchase. At the same time, 9% said the website rating was the primary factor during the battery purchase, and 14% mentioned it for the sex toy purchase. In the other conditions, participants claimed price had a less important role, and the website rating was more important. In the *privacy* condition, 64% mentioned price for the batteries (36% cited the privacy rating), but only 36% mentioned price for the sex toy (55% cited the privacy rating); in the *frame* condition, 64% mentioned price for the batteries (18% cited the privacy rating), but only 46% mentioned price for the sex toy (36% cited the privacy rating); in the *interstitial* condition, 52% mentioned price for the batteries (35% cited the privacy rating), while 44% mentioned price for the sex toy (48% cited the privacy rating). We price was not the driving factor, privacy ratings played more of a role in participants' purchasing decisions.

We selected vendors that we believed would be unfamiliar to participants. During the exit survey three participants (3.4% of 89) disclosed that they had done business with our vendors in the past (two sex toy vendors and one battery vendor). However, when we asked them if previous experiences with a particular company were factors (using a 7-point Likert scale) for either purchase, we found no correlation between self-reported familiarity and where participants made purchases during the study.

9.2.2 Product-Specific Privacy

Hypothesis 2: Participants who see privacy indicators will pay more for the privacy-sensitive item than the item that does not raise additional privacy concerns.

We performed a pairwise t-test across both purchases to compare the prices paid for the sex toy with the prices paid for the batteries in each condition (Table 9.3), and found that participants paid significantly more—for higher privacy levels—for the sex toy than for the batteries in both the *privacy* ($t_{21} = 2.935$, $p < 0.008$) and *frame* ($t_{21} = 2.346$, $p < 0.029$) conditions.

What we found most interesting was that participants in the *interstitial* condition did not pay significantly more for one product versus the other. Instead, they paid a privacy premium for both products. In this case, the effect of the privacy indicators being displayed as an interstitial diluted the role of product-specific concerns when the participants made their purchases. Thus, they were motivated to find the high privacy websites for both products.

We compared our observed data to the self-reported data that participants provided on our exit survey. In the exit survey we asked participants to rate their privacy concerns for both products on a 7-point Likert scale (six represented “extremely concerned,” while zero represented “not concerned at all”). Participants reported an average concern level of 5.56 for the sex toy ($\sigma = 2.291$) and 3.56 for the batteries ($\sigma = 1.864$). We performed a paired t-test and determined that participants had significantly higher levels of concern when purchasing the sex toy ($t_{88} = 7.884, p < .0005$). Participants used another 7-point Likert scale to specify how concerned they were during each purchase when providing specific types of information: credit card numbers, email addresses, physical addresses, phone numbers, and purchase histories. For each piece of information, participants were significantly more concerned about what would happen to that information when they provided it for the sex toy purchase than for the batteries purchase, as shown in Table 9.4.

Participants who saw privacy indicators were able to address many of their privacy concerns by purchasing the sex toy from websites with better privacy policies. However,

Information	Sex toy	Battery	t_{88} statistic	p value
Credit card	4.92	4.55	2.938	.004
Email address	4.87	3.96	5.002	.0005
Physical address	4.29	3.45	4.738	.0005
Phone number	4.62	3.94	4.008	.0005
Purchase history	3.87	2.92	5.499	.0005

Table 9.4: Participants used a 7-point Likert scale to specify how concerned they were during each purchase when providing various types of personal information.

this was not the case for those in the *handicap* condition, who did not see the privacy indicators.

9.2.3 The Effect of Timing on Prices

Hypothesis 3: Participants will be more likely to pay for increased privacy when they see privacy indicators alongside search results before visiting a website than when they see privacy indicators after clicking on search result links.

Hypothesis 4: Participants will be more likely to pay for increased privacy when they see privacy indicators before they see the content of a website than when they see privacy indicators alongside the content of a website.

The results of our study indicate that the impact of timing was nuanced: Hypothesis 3 was correct for participants who clicked only one search result, but false for participants who visited multiple websites before deciding where to purchase. Table 9.5 shows the average prices paid for each product across the four study conditions, broken down based on whether participants visited more than one website.

Condition	Websites	Batteries	(n)	Sex toy	(n)
Handicap	1	\$0.16	(13)	\$0.10	(16)
	>1	\$0.14	(9)	\$0.17	(6)
Privacy	1	\$0.41	(14)	\$0.46	(13)
	>1	\$0.22	(8)	\$0.61	(9)
Frame	1	\$0.03	(8)	\$0.06	(8)
	>1	\$0.39	(14)	\$0.61	(14)
Interstitial	1	\$0.03	(8)	\$0.19	(8)
	>1	\$0.58	(15)	\$0.65	(15)

Table 9.5: Average privacy premiums paid—above the base price of \$15.50—for each product by participants in the four study conditions. The study conditions are broken down based on whether participants visited multiple websites before making a purchase. The numbers in parentheses reflect the size of the groups.

9.2.4 One-click purchases

We performed an ANOVA to compare the amounts participants paid between the different conditions when they visited only one website before purchasing the batteries ($F_{3,39} = 4.772$, $p < 0.006$). We discovered that participants in the *privacy* condition paid significantly more than those in the *frame* ($p < 0.019$) or *interstitial* ($p < 0.019$) conditions.[6] This indicates that participants used the search result annotations to choose websites with increased privacy levels. However, when the privacy indicators were displayed after participants had selected websites from the search results, the participants ignored those indicators, perhaps because they were unwilling to return to the search results. Instead, they were focused on the purchasing task. For these participants the increase in privacy for the batteries was not worth the hassle of selecting new websites from the search results.

We observed slightly different behaviors when participants purchased the sex toys. Again, we observed significant differences between the study conditions ($F_{3,31} = 4.402$,

---

[6] All post-hoc analysis throughout this paper was done using Tukey's HSD test.

$p < 0.009$), but now the differences were between the *privacy* condition and the *handicap* ($p < 0.012$) and *frame* ($p < 0.027$) conditions. Again, participants in the *privacy* group paid more for privacy when visiting only one website because they saw the privacy indicators before choosing a website to visit. The lack of a significant difference between the *privacy* and *interstitial* conditions is likely a random phenomenon that may disappear with a larger sample size.

9.2.5 Multiple-click purchases

Of the participants who visited multiple websites before purchasing an item, we found that the timing of the privacy indicators did not significantly impact the selection of the website from which they made their purchases. An ANOVA yielded significantly different prices paid for the batteries between the study conditions ($F_{3,42} = 5.424$, $p < 0.003$). Using post-hoc analysis we discovered that participants in the *interstitial* condition paid significantly more than participants in both the *handicap* ($p < 0.004$) and *privacy* ($p < 0.030$) conditions. However, there were no significant differences in battery prices when comparing the *frame* condition with the *handicap* and *privacy* conditions. This can likely be attributed to the role of website content—those who viewed content alongside the privacy indicator relied on the privacy indicator less. It is also likely that because the interstitial interrupted their immediate task and required their attention to dismiss it, the strength of this privacy indicator was greater than that of the other two.

The significantly stronger effect of the *interstitial* condition was only observed during the battery purchase: we observed significant differences between the conditions when examining prices paid by participants who visited multiple websites when purchasing the sex toy ($F_{3,40} = 8.860$, $p < 0.0005$), but this was because everyone exposed to privacy indicators—regardless of timing and placement—paid significantly more than those in the *handicap* condition ($p < 0.001$ for *handicap* vs. *privacy*, and $p < 0.0005$ for both *frame* and *interstitial* vs. *handicap*). This is interesting because it means that those who saw privacy indicators after choosing websites from the search results still ended up purchasing the sex toy from the higher privacy websites—it just took them longer to find them.

9.2.6 The Effect of Timing on Website Visits

Hypothesis 5: Participants who see privacy indicators after clicking on search result links will visit more websites than those who see privacy indicators alongside search results.

We further explored the role of timing by examining the number of search results visited by participants in the *frame* and *interstitial* conditions. Recall that these participants only saw privacy indicators after selecting search results. Table 9.6 shows the number of websites participants in all conditions visited on average before making a purchase. We performed an ANOVA and found significant differences between the conditions for both the battery ($F_{3,85} = 4.475$, $p < 0.006$) and the sex toy ($F_{3,85} = 8.394$, $p < 0.0005$) purchases.

Because we were primarily interested in how long it took participants to find the websites with the highest privacy levels, we performed another ANOVA, though this time only examining participants who purchased from the websites with four green boxes. When purchasing the batteries, participants in the *privacy* condition clicked significantly fewer

Condition		Batteries	Sex Toy
Handicap	(22)	1.86 ($\sigma = 1.17$)	1.41 ($\sigma = 0.91$)
Privacy	(22)	1.86 ($\sigma = 1.36$)	1.73 ($\sigma = 1.12$)
Frame	(22)	3.05 ($\sigma = 1.79$)	3.09 ($\sigma = 1.77$)
Interstitial	(23)	3.09 ($\sigma = 1.78$)	3.04 ($\sigma = 1.69$)
Interstitial*	(23)	2.09 ($\sigma = 1.38$)	1.74 ($\sigma = 1.10$)

Table 9.6: The total number of search results visited (out of a maximum of five) before participants purchased each product. The last row shows the number of sites visited by members of the *interstitial* condition when they chose to proceed to the website in light of the privacy indicator.

search results to find the website with the four green boxes ($F_{3,22} = 23.126$, $p < 0.0005$). Participants in the *interstitial* and *frame* conditions clicked 203% more search results on average than those in the *privacy* condition to purchase from this same website and obtain the same level of privacy ($p < 0.0005$ for both comparisons). Thus it took participants in the *interstitial* and *frame* conditions significantly longer to find the same high-privacy website that those in the *privacy* condition were able to locate with a single click.

Recall that in the *interstitial* condition, participants must acknowledge the privacy indicator before viewing the destination website. If instead of examining the number of search results clicked, we examine the number of websites viewed by those in the *interstitial* condition, we no longer see a significant difference between the *interstitial* condition and the *privacy* and *handicap* conditions. That is, when participants encountered the interstitial privacy indicator on a website with a low privacy level, they were more likely to return to the search results without viewing that website.

This distinction was also apparent when we examined the number of search results clicked prior to purchasing the sex toy from the website with the highest privacy level ($F_{3,33} = 21.039$, $p < 0.0005$): participants in the *interstitial* and *frame* conditions clicked an average of 168% more websites ($p < 0.0005$ for both comparisons) than those in the *privacy* condition. Again, participants in these three conditions did not differ on the level of privacy they achieved, it merely took them longer to achieve that same level of privacy when the indicators were displayed after search results were selected. Therefore, displaying privacy indicators alongside search results creates more efficient shopping experiences for most users, while also helping users who click fewer search results to achieve greater levels of privacy.

9.3 Discussion

With this research, we showed that the timing of privacy information display impacts purchasing decisions: participants who decided to visit only one website to make their purchases paid significantly more money for a higher level of privacy when privacy indicators were presented alongside their search results; similar participants who did not see privacy indicators until after they had already selected a website were unwilling to spend time finding websites with higher privacy levels and instead made purchases from cheaper websites. Likewise, participants who did comparison shopping were just as willing to use interstitial and frame privacy indicators to find websites with higher privacy levels, even though this meant visiting significantly more search results.

These results have several public policy implications. We see that a significant proportion of users, when not presented with salient privacy information alongside search results were likely to simply not bother with looking for privacy information. Those that did comparison shop had to spend more time and effort to find those site that offered better privacy. Privacy information needs to be made more prominent in order for people to take those cues into account to guide their behavior. Any standards or regulations proposed to help people to protect their privacy must take into account the amount of effort that must be made for that information to be effective. It may require mandating a fewer number of “clicks" to obtain access to that information.

Finally, we observed that privacy decisions depended on privacy concerns surrounding the items being purchased: participants had greater privacy concerns when making the sex toy purchases and therefore went out of their way to use the privacy indicators to find websites that offered higher levels of privacy, even if this meant paying a premium. Likewise, many participants were not willing to pay a privacy premium for the batteries because the product did not trigger the same level of privacy concern as the sex toy.

9.3.1 Limitations & Future Work

While we demonstrated that the timing of a privacy indicator’s appearance has an impact on whether users visit websites with better privacy policies, there are still many unanswered questions. We did not compare the effect of privacy indicators with other relevant indicators such as customer ratings, nor did we explore the extent to which participants might view privacy indicators as a proxy for other indicators of trustworthiness unrelated to privacy. Two additional areas that we plan to focus on in future studies are how consumers make decisions about privacy premiums and how website content competes with indicators for a user’s attention.

9.3.2 Privacy Premiums

We observed that participants were willing to pay premiums to receive higher levels of privacy. In this particular study we used a privacy premium of $0.75. However, we do not know if participants view privacy premiums as a percentage of a purchase price or as a flat rate. That is, would participants have paid this same premium on an item that cost half as much? Would participants pay a $1.50 privacy premium on an item that cost twice as much?

9.3.3 Website Content

Fogg et al.'s work on website credibility indicates that the "look and feel" of a website is the main factor when users make trust decisions [49]. However, we were surprised to discover that this was not always the case: many times participants placed more weight on the privacy indicators than the websites. That being said, it is unclear how exactly participants assessed the quality of the websites they visited. Future studies might examine how participants assess the look and feel of websites while also examining their reactions to privacy indicators.

9.4 Privacy Concerns and Purchasing Factors Over Time

In both the Privacy Information Purchasing Study (Section 7), October 2006, and the Privacy Information Timing Study, July 2008, we asked people interested in participating in our online shopping studies to complete a screening survey. In this survey we asked participates to rate their levels of concern related to the information practices of website and the factors that affect their decision when selecting a website from which to make a purchase.

The website information practices include the following:

- A website shares your financial information with other companies (Financial Information).
- A website does not allow you to be removed from marketing/mailing lists (No Removal).
- A website does not allow you to find out what information it stores about you (No Knowledge of Stored Info).
- A website shares personally identifying information with other companies (Shared Identifying Info).
- A web site shares your health information with other companies (Health Information).
- A website contacts you about other services or products via telephone (Telephone).
- A website uses your financial information to determine website content or ads (Finance Info for Ads).
- A website uses your financial information to determine website content or ads (Privacy Policy).
- A website uses personally identifying information to determine your habits, interests, or other characteristics (Profiling).
- A website contacts you about other services or products via email or postal mail (Mail).

- A web site uses your health information to determine website content or ads (Health Info for Ads).
- A website shares information that does not personally identify you with other companies (Share Non-Identifying Info).
- A website uses information that does not personally identify you to determine your habits, interests, or other characteristics (Non-Identifying Profiling)

For the website information sharing practices, participants were asked to rate their level of concern on a 7-point Likert scale ranging from not concerned at all to extremely concerned. The practices and the average score for each study are detailed in Table 9.7. We see that, over time, the level of concern that participants have regarding website practices has not changed, save for becoming less concerned about websites using information that does not personally identify you to determine your habits, interests, or other characteristics.

To quantifying the factors that influence a consumer's decision in the selection of a website from which to make a purchase, we asked participants to rate how much each factor affects their choice on a 7-point Likert scale ranging from not at all to a great deal. The factors and the results of their comparisons to the value of the website's privacy policy with a paired t-test are presented in Table 9.8 for the 2006 values and in Table 9.9 for the 2008 values. We see that between the two studies, the same factors (customer reviews, the design of the website, and how quickly the website loads) continue to be rated as influential as a website's privacy policy.

To determine whether any factors had changed in level of influence between the two studies, we compared the means of each factor in a two-sample t-test. We see that sev-

Information Practice	Privacy Information 2006	Timing 2008	p value
Financial Information	6.47	6.54	0.41
No Removal	6.43	6.38	0.60
No Knowledge of Stored Info	6.13	6.19	0.58
Shared Identifying Info	6.18	6.16	0.88
Health Information	5.91	5.96	0.73
Telephone	5.96	5.94	0.84
Finance Info for Ads	5.83	5.86	0.78
Privacy Policy	5.25	5.05	0.23
Profiling	5.16	5.03	0.34
Mail	4.68	4.67	0.90
Health Info for Ads	4.69	4.58	0.50
Share Non-Identifying Info	4.20	4.1	0.55
Non-Identifying Profiling	4.05	3.70	**0.03**

Table 9.7: This table contains the mean responses for responses to made in study recruitment surveys to determine how concerned users are about website privacy practices. Participants used a 7-point Likert scale (ranging from not concerned at all to extremely concerned) to specify how concerned they were about each scenario. The responses between studies was compared using a two-sample t-test.

eral factors decreased in importance, including the design of a website (M_2006= 4.88, M_2008 = 4.51, t(586) = 2.94, p = 0.003), the webpage load speed (M_2006= 4.81, M_2008 = 4.50, t(586) = 2.17, p = 0.03), the popularity of the site (M_2006= 4.60, M_2008 = 4.21, t(586) = 2.68, p = 0.008), a site's compatibility with mobile phone web browsers (M_2006= 1.61, M_2008 = 1.34, t(586) = 2.89, p = 0.004), and its accessibility for site-impaired users (M_2006= 1.51, M_2008 = 1.30, t(586) = 2.34, p = 0.02).

The consistency with levels of concern related to website information practices suggests that the research we conduct to evaluate and address privacy concerns continues to be relevant and of importance. We also see that the factors that affect users' decisions of whether or not to make a purchase from a particular website have also remained constant. Price continues to be the driving factor.

Factor	Mean	t_{282} statistic	p value
Price	6.53	14.3	$<$0.0001
Return Policy	5.55	6.51	$<$0.0001
Shipping Speed	5.42	4.23	$<$0.0001
Customer Service	5.35	3.52	0.0005
Privacy Policy	4.97	-	-
Customer Reviews	4.95	-0.17	**0.87**
Website Design	4.88	-0.80	**0.41**
Webpage Load Speed	4.81	-1.43	**0.15**
Popularity	4.60	-2.73	0.007
Software Compatibility	4.48	-4.09	$<$0.0001
Physical Location	3.19	-15.08	$<$0.0001
Cell Phone Compatibility	1.61	-28.22	$<$0.0001
Handicap Accessibility	1.51	-29.12	$<$0.0001

Table 9.8: Survey results for people the influence of factors considered when selecting a website from which to make a purchase in the Privacy Information Purchasing Study (2006). Mean values are based on a Likert scale from 1 to 7, ranging from not at all to a great deal.

Factor	Mean	t_{304} statistic	p value
Price	6.50	16.26	$<$0.0001
Return Policy	5.31	6.74	$<$0.0001
Shipping Speed	5.22	4.22	$<$0.0001
Customer Service	5.15	4.01	$<$0.0001
Customer Reviews	4.83	0.08	**0.94**
Privacy Policy	4.72	-	-
Website Design	4.51	-1.70	**0.10**
Webpage Load Speed	4.50	-1.70	**0.09**
Software Compatibility	4.30	-3.31	0.001
Popularity	4.21	-3.80	0.0002
Physical Location	2.93	-14.02	$<$0.0001
Cell Phone Compatibility	1.34	-29.57	$<$0.0001
Handicap Accessibility	1.30	-30.55	$<$0.0001

Table 9.9: Survey results for people the influence of factors considered when selecting a website from which to make a purchase in the Privacy Information Timing Study (2008). Mean values are based on a Likert scale from 1 to 7, ranging from not at all to a great deal.

Chapter 10

Privacy Finder Usage Study

> This chapter is largely a reproduction of a paper co-authored with Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti. This research was funded in part by U.S. Army Research Office contract no. DAAD19-02-1-0389 (Perpetually Available and Secure Information Systems) to Carnegie Mellon University's CyLab and by Microsoft Research.

One of the motivations behind the development of Privacy Finder was the notion of making privacy information more prominent. When privacy information is made more accessible or evaluable, it may be more likely that people will consider the level of privacy protections afforded by a specific site when selecting a website from lists of search results. We designed our field study of Privacy Finder to test whether users do, in fact, take privacy information into account. Specifically, we tested the following hypotheses:

Hypothesis 1: By displaying privacy information alongside search results, users will be more likely to visit websites that offer higher levels of privacy protection, as denoted by our privacy indicators.

Hypothesis 2: By displaying privacy information in the search engine, users will be more likely to visit websites further down the list of search results when those sites have privacy indicators, as compared to visitation rates when no privacy indicators are present. Sites with privacy indicators will have a higher probability of being visited than sites in the same position without privacy indicators.

10.1 Participant Recruitment

From December 2007 to October 2008, we recruited participants to test a privacy-enhanced search engine. We posted announcements about the study on various volunteer solicitation websites, including Craigslist and online sweepstakes sites. We used a raffle as an incentive for people to use our search engine regularly. For each day that participants conducted searches using Privacy Finder, they were issued a raffle ticket. We conducted weekly raffles of $20 Amazon.com gift certificates, and a $200 Amazon.com grand prize raffle.

To participate in the study, participants first registered their email addresses and completed a pre-study survey that contained questions about their attitudes toward online privacy. Subsequently, when participants logged in to Privacy Finder using their email addresses, we placed a cookie on their computers. The cookie was used to distinguish the study participants from other Privacy Finder users and to create entries in our prize drawing database. All searches were anonymized, and we used the email addresses solely to contact participants in the event that they won a prize drawing. When users were logged in (i.e. we detected the cookie), we recorded their queries, the times and dates of the queries, the search engine selected, the privacy level of the search engine, the search results that were returned, the privacy ratings for those search results, and any results visited.

10.2 Data Analysis

We analyzed our pre-study survey results to gain information about the population of users who participated in our study and to understand their levels of privacy concern. Then, we analyzed our Privacy Finder search data by comparing the browsing behavior of users whose queries produced search results that contained privacy indicators—websites with P3P—with the behavior of users whose queries produced a set of search results without privacy indicators. By using statistical tests to compare visitation-rates between these different types of queries, we investigated whether privacy indicators impacted browsing behavior.

10.2.1 Pre-study Survey

During the participant recruitment process, we asked potential subjects to complete a 10-question online survey. We collected survey responses from 740 people.[1] The average age of our participants was 34.7 years, and 57.7% of the respondents were female. Our sample was also relatively highly educated, with 88.2% of respondents having a college

---

[1] Only 62% of those who completed the survey chose to participate in the search result analysis portion of the study.

education. Based on a 7-point Likert scale from “Never” (1) to “Always” (7), we found that, on average, participants “sometimes” noticed whether or not a website has a privacy policy (μ = 3.89, 95% CI = 3.76 - 4.03), and that they do not often read website privacy policies (μ = 2.82, 95% CI = 2.70 - 2.94).

In addition to collecting basic demographic information, we queried our respondents about their privacy concerns. We used a four-item risk belief scale developed in previous studies to calculate a risk score for each participant [113]. Participants’ responses to the four 7-point Likert scale questions were averaged (the lower the score a respondent receives, the less concerned they are about their privacy). The risk belief scale consists of the the following questions:

- I feel safe giving my personal information to online stores. (Strongly disagree to strongly agree (*reversed*))
- Providing online stores with personal information involves too many unexpected problems. (Strongly disagree to strongly agree)
- I generally trust online companies with handling my personal information and my purchase history. (Strongly disagree to strongly agree (*reversed*))
- How concerned are you about threats to your personal privacy online in American today? (Not concerned at all to extremely concerned)

We plotted a histogram of participants’ risk scores, as shown in Figure 10.1, where the bin size is 0.25. This histogram and the superimposed normal distribution curve (μ = 3.25, σ = 1.11) indicate that the risk scores for our sample are well represented by a normal

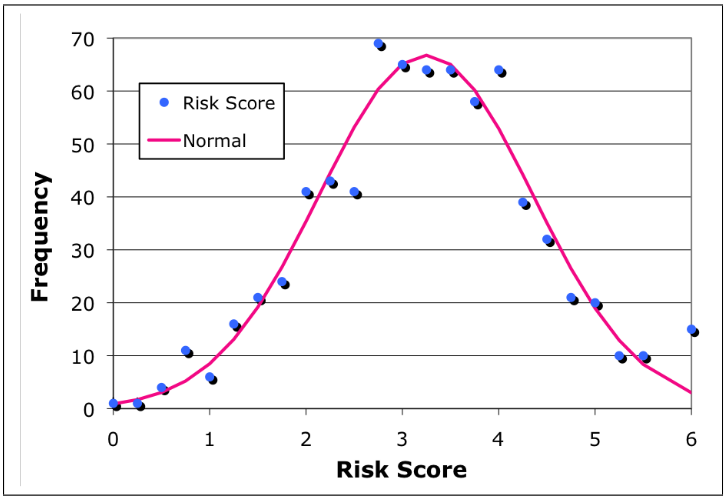


Figure 10.1: The histogram for the risk scores for our participants as compared to the normal distribution, plotting the risk score and the number of people who had that same risk score. We see that the risk scores have a good fit to the normal distribution, bin size 0.25.

distribution.[2] This distribution indicates that a majority of our participants had a medium level of privacy concern, with a slightly higher proportion of higher concern respondents than low concern respondents.

The results of our pre-study survey mimics those found in the Westin surveys. Alan Westin conducted a series of privacy concern surveys that gathered longitudinal data about the level of privacy concern and online privacy concern among Americans. In 1996, he created a “Privacy Concern Index" that divided respondents into three categories: the privacy fundamentalist (high privacy concern), the privacy pragmatist (medium privacy concern), and the privacy unconcerned (low privacy concern) [119]. In this 1996 survey and in subsequent Westin surveys, we see that the majority of respondents are classified as privacy pragmatists, with a slightly higher population of privacy fundamentalists than the privacy

---

[2] Using Pearson’s chi-squared test, we see that we cannot reject the null hypothesis that the risk scores for our participants are consistent with the normal distribution, χ^2 = 0.36.

unconcerned [73].

Our sample of subjects may suffer, naturally, from self-selection bias, albeit of a particular nature: our subjects were drawn to participating in a study which explicitly focused on privacy protection; yet they were also willing to reveal (albeit anonymously) their search results to the researchers.[3] However, we created a monetary incentive to recruit participants, which also served to counter-weight the potential biasing effect of the privacy incentive. Specifically, we offered a weekly raffle incentive to keep people interested in the search engine and to promote its use. Based on the responses to questions in the pre-study survey (see Figure 10.1) we conclude that, in fact, we did not only attract individuals who were highly concerned about their privacy: rather, we see that the majority of our respondents had medium levels of privacy concern. Thus, even though our sample was self-selected, their privacy concerns are likely representative of the larger population.

10.2.2 Experimental Control

When designing a research study, researchers must always consider how they will design or deploy an experimental control. In this field study, we were asking users to use Privacy Finder as their normal search engine. We would have ideally liked to create a control for Privacy Finder (a search engine that did not annotate search results with privacy indicators) or a method to test other indicators (e.g. a search engine that annotated results with merchant rating indicators). By assigning participants randomly to these additional conditions, we would have been able to directly compare the behavior of users under identical

---

[3] Subjects were told that their searches would be logged, but that we would not individually identify them, other than to inform them in the event they won a prize.

conditions but without privacy indicators, with privacy indicators, and with other indicators. A large search engine operator could easily setup such conditions by simultaneously deploying privacy indicators and another type of indicator each to a small subset of their users, while continuing to provide no indicators to most users. However, this is much more difficult to setup when no existing users are available and new users must be recruited for each experimental condition.

After considering the use of these additional search engine conditions, we determined that it would be too difficult to find enough users to use several different search engines for long periods of time without offering a good reason why. In the commercial search engine market, a small number of search engines have maintained the majority of search engine market share for over half a decade. The majority of searches are conducted on the Google (63.0%), Yahoo! (21.0%), or Microsoft (8.3%) sites, indicating that it is difficult to grab market share from the large search engine players [32]. In the meantime, many search engines have gone out of business [107]. Despite the low switching costs of choosing a new search engine [51], it seems that the most successful search engines provide such good quality results or have added features (e.g. integration with email) that it makes users reluctant to switch to new search engines.

Instead of implementing a control search engine condition, we used a within study control for statistical analysis purposes. We partitioned the search results pages returned to users into two sets: those with at least one privacy indicator and those with no privacy indicators (because none of the results on those pages had P3P). We compared the visitation rates of results in the privacy-indicator set with those in the no-privacy-indicator set as the

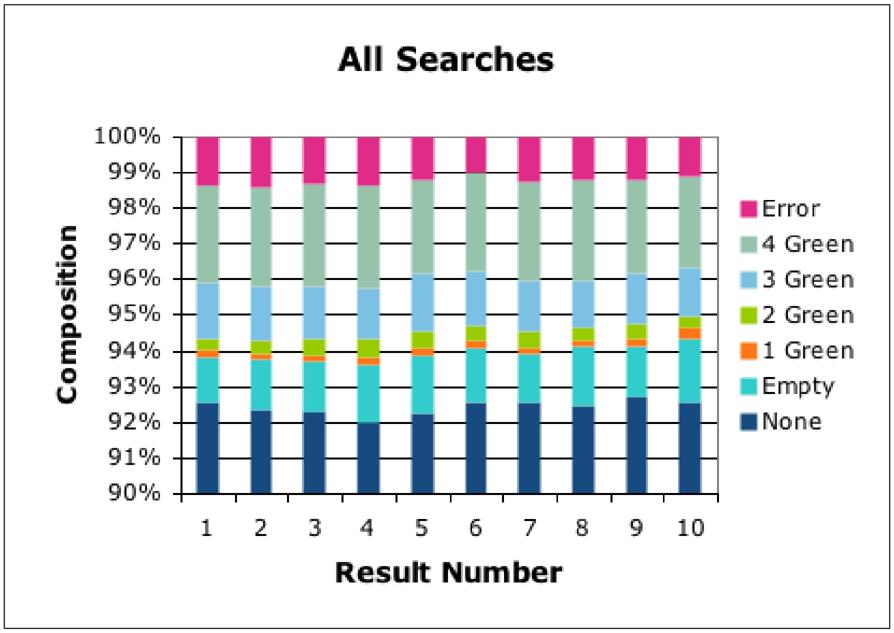


Figure 10.2: Composition of search results based on privacy ratings and position on the search results page.

control.

10.2.3 Privacy Finder Usage Data

Over the course of the study, 460 unique users logged in and allowed us to track their searches. These users conducted 15,116 queries over a ten month period. On average, each participant used Privacy Finder for six days and conducted 33 queries, with a median of four queries.

Privacy Finder allowed users to select which search engine they wished to use (Google, Yahoo!, or Yahoo! Shopping) and to customize the level of the privacy preference setting (low, medium, high, or custom). Google was the default selection for the search engine, and was used for over 80.70% of the searches. Yahoo! was used for 18.34% of the

Privacy Indicator	# of Results	% of results with indicator
No Indicator	134,340	92.43%
0 Green	2,181	1.50%
1 Green	289	0.20%
2 Green	595	0.41%
3 Green	2,125	1.46%
4 Green	4,003	2.75%
Error	1,807	1.24%

Table 10.1: The frequency with which each privacy indicator appeared in the search results.

# of Results with Indicator	# of searches	% of searches
No Indicators	9481	62.72%
1	3,102	20.52%
2	1,348	8.92%
3	544	3.60%
4	244	1.61%
5	175	1.16%
6	73	0.48%
7	42	0.28%
8	31	0.21%
9	21	0.14%
10	55	0.36%

Table 10.2: The frequency of results pages annotated with 0-10 privacy indicators. For example, there were 55 pages where all 10 search results were annotated with privacy indicators.

searches (2,633) and Yahoo! Shopping was used for 0.96% of the searches (147). The majority of searches were made at the default privacy setting of *medium* (91%), with 5% of the searches made using the *high* setting, 3% at *custom*, and 1% at *low*.

Privacy Finder computes a privacy rating based on elements of websites' privacy policies and the privacy preferences setting in Privacy Finder. The frequencies with which each privacy indicator appeared in the search results are depicted in Table 10.1. Most searches returned a page with ten search results, although some queries returned fewer results.

The queries conducted in this study returned a combined total of 145,340 search results, of which 6.33% were annotated with privacy indicators and 1.24% were P3P-enabled but no privacy rating could be computed due to errors in their P3P policies.

We examined the frequency of search results with privacy indicators. We found that the majority of queries returned results without any P3P policies, and therefore without any privacy indicators. The frequencies of the number of privacy indicators per set of search results are summarized in Table 10.2. The highest privacy rating (four green boxes) was the privacy indicator that occurred most frequently in our data set. As shown in Figure 10.2, the frequencies of each of the privacy indicators were evenly distributed across all pages of ten search results. (A chi-square test shows that there are no statistically significant differences in the distribution of P3P-rated results by result number, p = 0.47, $\chi^2 = 8.64$.) This indicates that it was not the case that a specific result number was more likely to be annotated with a privacy indicator (i.e., participants are not more likely to visit result 3 simply because there were a higher number of search results with privacy indicators that happened to be in position three). On average, each of the ten search result positions was annotated with a privacy indicator 7.57% of the time.

We categorized the search terms participants used to determine the types of queries conducted (navigational, transactional, or informational). We found that the most frequent searches were navigational in nature. Nine out of the top ten searches were navigational. The top ten searches made up about 1% of the total queries conducted. When users conduct navigational queries, they typically know which website they are looking for. We found that when participants visited search results for the nine navigational queries in our top ten most frequent searches, they visited the first result 79.7% of the time.

In our data analysis, we examined the position of each search result and how frequently search results were visited. A “visit" in the context of this paper refers to the user clicking on a website in a set of search results in order to go to that specific website. Examining our dataset for usage changes between the search engines, we found no statistical differences in browsing patterns between the Google and Yahoo! search engines (when using a chi-square test to examine the proportion of privacy-annotated results visited). Due to the small sample size of the Yahoo! Shopping searches, we eliminated those searches from the remainder of the analysis. We also filtered out searches where none of the search results were visited. Our hypotheses focus on browsing behavior; searches without clicks are irrelevant to answering our research questions.

Our final dataset consisted of 7,046 queries made through the Google and Yahoo! search engines where at least one search result on the search results page was visited. Of these queries, 79.1% were made through Google (5,571) and 20.9% (1,475) through Yahoo!.

10.2.4 Browsing Patterns

Throughout the study, we found it difficult to retain users. We found that people were mostly likely to sign up for the study, conduct multiple searches over the course of the day, and fail to return to the Privacy Finder site on subsequent days (294 out of 460 participants). To determine if the browsing patterns of these users (1,030 queries) skewed our results (due to the novelty of seeing privacy indicators), we compared the proportions of visits to

P3P-rated sites for the *one day* users to the visitation patterns of users who participated in the study over a longer period of time. We found that *one day* users visited 5.22% (46 out of 881) of the search results that had privacy indicators while the rest of the participants in the study visited 8.27% (825 of 9,975) of the search results with privacy indicators, Fisher's exact $p <$ 0.001. This indicates that the privacy indicator-annotated search result visitations were significantly different, but that *one day* users were actually *less* likely to visit sites with privacy indicators. Despite the novelty of privacy indicator annotated search results, these indicators did not significantly sway their search result visitations.

To further determine if continued use of Privacy Finder would alter search behavior over time, we examined the search queries of the 32 participants who used Privacy Finder for two weeks or longer. We specifically examined the searches made over the first seven days of participation and compared them to the searches made over the second set of seven days. We find that for the first seven days of study participation, these participants visited 7.74% (121 of 1,563) of the search results that were annotated with privacy indicators. Over the second week, these participants visited 7.96% (93 of 1,168) of the sites with privacy indicators. These proportions of visitations were not statistically different (Fisher's Exact p = 0.83). It appears that continued use over this 14-day period did not significantly alter browsing behavior; participants continued to visit sites with privacy indicators at about the same rate.

10.2.5 Data Validation

In addition to our analysis of the privacy attitudes of the participants in the study and the within-study control, we also validated the search result visitation rate in our dataset. We were interested in knowing whether or not people were visiting search results at a normal rate or if they were attempting to falsify their visitation patterns (i.e. visiting the last search result in all of their search queries).

To address potential concerns with our data, we validated the use of Privacy Finder to search behavior data from a major search engine. Microsoft provided us with the Spring 2006 search data collected from users of their search engine, Live Search.[4] This data consisted of about 15 million queries sampled over one month. The attributes of this dataset included query strings, timestamps, any URLs visited, and the positions on the results page for each URL visited. This dataset only contained queries where a user visited at least one of the URLs. We will refer to this dataset throughout the paper as the *MS Live* dataset.

We can determine the likelihood that users will visit a certain website based on its position on the results page. Based on the methodology implemented in the study of search results by Agichtein et al. [12], we calculated the relative click frequencies for the *MS Live* and *Privacy Finder* search results. This allows us to evaluate the proportions of visitations relative to the first search result. This provided us with a standardized method with which to evaluate search result visitations across the two datasets.

We calculated the relative visitation frequencies in two parts. First, the actual frequency

---

[4] http://www.live.com

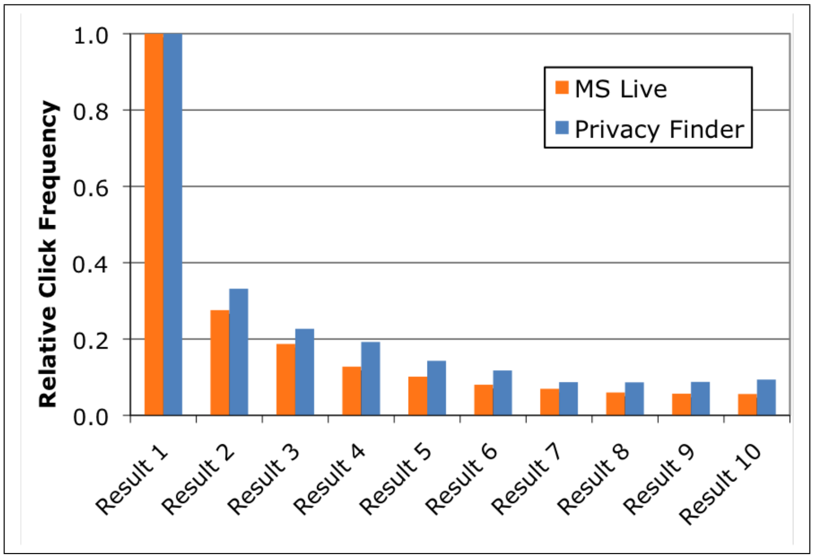


Figure 10.3: Relative click frequency rates for the *Privacy Finder* and *MS Live* datasets based on position on the search results page.

of visiting a search result was calculated for each result position. Second, these frequencies were normalized by comparing them to the first result so that the relative frequency of a visit at the top position was 1.0. We calculated the relative click frequency for the two datasets, and compared the *MS Live* click frequency to the click frequency for the *Privacy Finder* dataset. Figure 10.3 shows that the relative click frequencies for the *Privacy Finder* and *MS Live* datasets were very similar.

The search patterns from our study participants seem to mimic those from a real world search engine. There was a 50% overlap in the top ten search terms in these two data sets. The top five search terms common to the two data sets were “Google," “Yahoo," “Amazon.com," “eBay" and “MySpace." This is reassuring, in that it appears that our users were not focused on the privacy indicators, but on conducting real search queries.

10.3 Results

After examining these general browsing patterns, we proceeded to test our first hypothesis:

Hypothesis 1: By displaying privacy information alongside search results, users will be more likely to visit websites that have high levels of privacy, as denoted by our privacy indicators.

To test *Hypothesis 1*, we calculated the visitation rates to search results annotated with each type of privacy indicator. We calculated the probability that a user will visit a result based on its privacy rating: the chance of someone visiting a site if it has no privacy rating, 0-4 green boxes, or the P3P error icon. On average, regardless of the position on the search results page, a site without a privacy rating was visited 14.24% of the time. When a site had a high privacy rating—four green boxes—it was visited 17.39% of the time.

We compared the proportion of visits to websites with each level of privacy rating to the proportion of visits to those sites that were not annotated with any privacy indicators (14.24%). Table 10.3 shows the results of the visitation comparisons between each privacy indicator as well as the statistical significance for those proportions based on Fisher’s exact

Privacy Indicator	% Results Visited	Fisher's Exact p
0 Green	13.66% (144)	0.63
1 Green	8.60% (8)	0.14
2 Green	13.21% (42)	0.68
3 Green	14.73% (137)	0.67
4 Green	17.39% (367)	$<$ **0.001**
Error	15.46% (143)	0.30

Table 10.3: Comparison of visitation rates between search results without privacy indicators (14.24%) to visits to search results annotated with privacy indicators. Significantly more users visited search results annotated with the highest privacy rating (Fisher's exact $p < 0.001$).

test. To account for multiple tests, we applied the Bonferroni correction by setting $\alpha = 0.008$.

We found that having low or medium privacy ratings (0-3 green boxes) had no detrimental effect on visitation rates: our statistical tests indicated that there was no observable difference between the visitation rates for results annotated with low or medium privacy ratings and the visitation rates to the sites without privacy ratings. Instead, we found that having a high privacy rating—four green boxes—significantly increased the number of visits to those sites.

To evaluate the overall impact on visitation rates to sites with privacy indicators, in general, we grouped all the search results annotated with privacy indicators. We found that sites with privacy indicators attracted a greater proportion of visits (15.49%, or 841 of 5,429 including websites with P3P errors) compared to sites without P3P (14.24%, or 9,145 of 64,221). We performed a one-tailed Fisher's exact test and found that this result was statistically significant ($p < 0.007$). We conclude that that privacy indicators have an impact on which website a user decides to visit.

To determine whether having a higher privacy rating induces people to visit search results lower on the page despite the presence of other less highly rated search results with privacy indicators, we examined the visitation patterns of sets of search results with multiple privacy indicators in a single search query. To determine if these lower-postioned high privacy websites had any impact on browsing patterns, we compared the visitation rates to sets of results with one privacy indicator to the visitation rates of sites with multiple indicators. We found that a total of 5,302 searches had exactly one privacy indicator in their set of search results. Of those searches, users visited sites with privacy indicators 416 times. This indicates that when people are presented with search results with exactly one privacy indicator, they visited that result 7.85% of the time. Comparatively, there were 311 searches that had multiple privacy indicators on a page where a site with a higher privacy rater was in a lower position on the search engine page (e.g. search result 3 had an indicator with two green boxes but search result 6 had an indicator with four green boxes). Of these cases, users visited the lower (higher-rated) result for 35 of those searches, for a proportion of 11.25%. We conclude that our participants were influenced by better privacy indicators, visiting sites with better ratings a higher proportion of the time when they were available (Fisher's Exact p = 0.04).

We find that *Hypothesis 1* is supported: users presented with privacy information were more likely to visit websites that had a high privacy rating.

Hypothesis 2: By displaying privacy information in the search engine, users will be more likely to visit websites further down the list of search results when those sites have privacy indicators, as compared to visitation rates when no privacy indicators are present. Sites with privacy indicators will have a higher probability of being visited than sites in the same position without privacy indicators.

To test *Hypothesis 2* and to examine the impact of position on the search results page and website visitations, we compared two subsets of our *Privacy Finder* dataset:

No Indicator: The *No Indicator* data acts as the control and includes all the queries whose sets of search results did not contain any privacy indicators. When users see search results that fall under this category, they would see the results without any additional indicators or privacy-related information.

One Indicator: The *One Indicator* data consists of the searches where there was exactly one search result with a privacy indicator on the search results page. This dataset controls for the effect of having a privacy indicator at a specific position on the search results page. Otherwise, the presence of multiple privacy indicators on a single page may be a confounding factor, making it more difficult to examine the impact of the indicators on the probability that a user will visit a certain result based on its position.[5]

We compared the proportions of visitations for each result position for the two datasets. For each result position, a Fisher's exact test was used to compare the proportions of visitations in the *No Indicator* dataset to the *One Indicator* dataset. We used one-tailed tests due to our hypothesis of having higher proportions of visits to sites with privacy indicators. The results of these tests are depicted in Figure 10.4 and Table 10.4. Using Fisher's Exact tests, we found that privacy indicators did have an impact on visitations, significantly increasing the visitation rates to results further down on the search results page.

---

[5] Searches that contained P3P errors were filtered out of this dataset.

We explored the role of privacy indicators on visitation rates further by grouping all of the ranked search results together. We excluded the first search result on each page because many of these were navigational, and therefore users were likely to visit them regardless of whether or not they were annotated with privacy indicators. We performed a chi-square test and found that users were significantly more likely to visit search results beyond the first result when the additional results were annotated with privacy indicators, (8.67% (4,076) (No indicator) vs 12.42% (138) (One indicator), $p < 0.0001$, $\chi^2 = 19.13$). Thus, we found that *Hypothesis 2* is supported by our data: users are more likely to visit search results which are lower on the search results page if those results are annotated with privacy indicators.

10.4 Discussion and Limitations

Based on this research, we find that when privacy indicators are annotated to search results, they do have a significant impact on which websites users choose to visit, especially when a website is annotated with a high-privacy indicator. This indicates that websites, in general, may be able to leverage the quality of their privacy protections to drive more traffic to specific sites.

While field study data supported our two hypotheses, certain limitations in the experimental design should be kept in mind. While we asked users to use Privacy Finder as their normal search engine, it is sometimes hard to convince users to switch from an existing search engine, especially as search engines become more tailored to each individual user (e.g. Google's web history). Additionally, due to our use of a daily raffle ticket incentive,

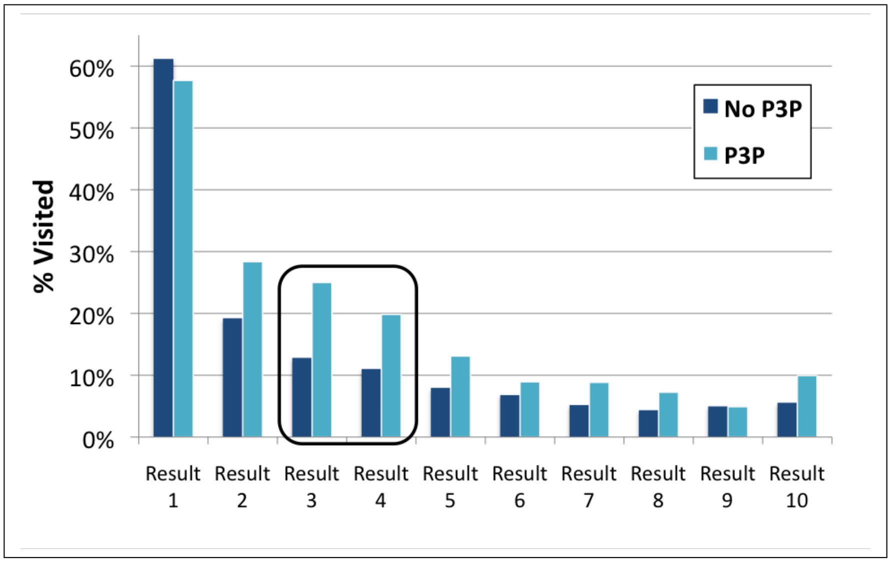


Figure 10.4: Visitation rates for the *No Indicator* and *One Indicator* search results based on the position on the search results page. The circle around Results 3 and 4 indicate that these specific search results were visited at a significantly higher rate when websites in those positions had privacy indicators.

some users may have participated with a minimal amount of effort, performing one query, and then simply closing the browser. For example, we had ten cases where people who participated in the study for longer than one day conducted small numbers of searches for the days they participated (e.g. a user who conducts 6 searches over 5 days). However, since we eliminated sets of search queries where none of the results were visited, this may have cut back on confounding effects where participants were not actually interested in finding information. Additionally, we did not have a set of perfect control data for this study. Instead, we used the search result visitation patterns gleaned from the use of a large commercial search engine to validate the search visitation patterns of our data, and a within-study control of search result sets returned without privacy indicators. A preferrable situation would be to form a research partnership with a large search engine company. With this partnership, we would be able to work with the large search engine company to

	No Indicator	One Indicator	Fisher's Exact p
Result 1	61.16% (3,225)	57.69% (45)	0.30
Result 2	19.21% (1,015)	28.36% (19)	0.05
Result 3	12.81% (674)	25.00% (22)	**0.002**
Result 4	11.01% (575)	19.84% (25)	**0.003**
Result 5	7.96% (416)	13.11% (16)	0.04
Result 6	6.79% (355)	8.94% (11)	0.22
Result 7	5.18% (271)	8.85% (10)	0.07
Result 8	4.34% (226)	7.25% (10)	0.08
Result 9	4.96% (257)	4.91% (8)	0.58
Result 10	5.55% (287)	9.94% (17)	0.02

Table 10.4: Visitation rates for sets of search results when none of the search results had a privacy indicator and when exactly one result had a privacy indicator. Fisher's exact test was used to compare the proportions of visitations using the Bonferroni correction to account for multiple testing ($\alpha = 0.005$).

integrate Privacy Finder into their search engine, and deploy a larger scale Privacy Finder field study to a subset of their users for a specific amount of time.

In addition to privacy indicators, defaults have a strong impact on user interface settings. Our data analysis focused on searches made in the Google and Yahoo! search engines. While the Yahoo! Shopping search engine option was available for our participants, we did not collect enough data to specifically examine differences in general information seeking searches versus shopping based searches. The majority of searches (91%) were also conducted at the default privacy preference level (medium), suggesting that the privacy settings may have lacked real meaning to users.

Examining the impact of privacy information, we found that people are drawn to the high-privacy indicators. In our previous laboratory studies, we found that it was not the indicator (green boxes) itself that was the draw, but what those indicators symbolized [113, 45], in this case, privacy. Further work is needed to validate the impact of random indicators versus meaningful ones in the field to determine if people are attracted to indicators, regardless of their meaning. Additionally, sites with P3P policies are relatively rare in the search results, and seeing the P3P indicators may be somewhat of a novelty. While we did not see a “novelty" effect in the search result visitations for the users who only used Privacy Finder for one day, the browsing patterns for larger samples of users may be different. This leaves an open question of the impact of P3P indicators once adoption rates have increased. Likewise, our dataset was too small to significantly examine the impact of multiple P3P results on a single page. This would be an interesting question to examine once P3P adoption rates increase.

Another avenue of research is that of the impact of privacy signaling. Privacy indicators may also be viewed as a proxy for reliable websites. Further research should be conducted into the extent that people take privacy indicators into account compared to other factors such as the design of the website or the brand name of the website.

10.5 Conclusions

People use Internet search engines to satisfy the majority of their informational needs. However, even though people are more concerned about their online privacy, they do not take the time to thoroughly examine the privacy policy of every website they encounter. The P3P standard was created to make this privacy information more accessible. Often, it is this lack of access to privacy policy information, or information asymmetry [6], that causes people to not act according to their privacy preferences. Thus, making privacy policy information available in the search engine can be a significant boon to users.

The results of this field study support our previous findings that people will seek out or visit sites with visible privacy ratings. Accessible privacy information does have an impact on search result browsing behavior. We find that the Privacy Finder search engine interface can act as an asset to both users and to websites that post P3P information. Users can choose to visit sites that better match their privacy practices. Websites can increase their visitation rates if they have P3P policies that search engines interpret and use as the basis for privacy indicators. The results of this study suggest that the adoption of P3P and the increased transparency for privacy policies will not have a detrimental effect on search result visitations, even if a website's specific policy may not be as good of a match to a user's privacy settings. Specifically, it can drive more clicks if the site is rated with a high privacy rating.

Part IV

Conclusions

Chapter 11

Conclusions

This thesis focuses on the impact of salient privacy information on privacy concerns and behavior. Through the use of online surveys, we collected and evaluated people's stated attitudes and concerns related to their online and location information based privacy. We conducted laboratory studies and field studies to examine how users actually behaved when using interfaces that provide salient privacy information, or how they react to feedback and expressive privacy settings in location-sharing systems that restrict the disclosure of location information. Many people are concerned about their privacy, but they often have difficulty addressing their concerns. I found that making privacy information more salient by providing people with awareness, notification and control can be an effective way of allowing people to consider this information in the decisions that they make.

11.1 Contributions

The original contributions of this thesis are the following:

- *Dimensions of salient privacy information:* Privacy information can be made more salient through indicators that provide users with *awareness* of the level of privacy offered by the site, through feedback as *notification* in a mobile-location system that allows people to check to see who has viewed their location information, and through *control* or rules that allow people to define and restrict who has access to their information in the first place.
- *Location privacy risk/benefit analysis:* My analysis of the perceived risks associated with the use of location-sharing technologies allows technology developers to better understand how to address the concerns associated with these technologies. I also examine the perceived benefits so that promoters of these technologies can better make a case for the use and adoption of location-sharing applications.
- *Evaluations of feedback in social mobile systems:* I evaluate the impact of providing feedback in a location-sharing system. My findings suggest that feedback can increase the comfort associated with the use of a location-sharing technology when the application itself is in the context of an open system, or a system where users can be requested by strangers. In a follow up study, my results suggest that feedback did not have an impact in a more closed system, where people could only be located by people with whom they already had a connection (e.g. Facebook friends), and where users were provided with a more expressive ruleset.

- *An experimental design to test the valuation of privacy in a real-world setting:* In this research, I developed an experimental protocol to evaluate user behavior regarding the valuation of privacy under real-world settings. Participants in our privacy information studies used our interface to select online merchants from which to make purchases using their own credit cards.
- *Evidence of the willingness-to-pay for privacy premiums:* My user studies have shown that people presented with prominent privacy information are willing to pay a premium to purchase from sites that offer better privacy policies. I found that people are willing to pay a premium when purchasing both privacy-sensitive and non-privacy sensitive items.
- *Evaluation of the timing of privacy information:* I found that the timing of when prominent privacy information is presented has an impact on whether or not people factor that information into their decision-making. Privacy information has the greatest impact when that information is presented in a search engine interface.
- *Evaluation of prominent privacy information on search result browsing patterns:* My evaluation of a field study of Privacy Finder search engine user suggests that high privacy indicators act as a draw for users and resulted in higher visitation rates as compared to sites without privacy indicators. I also note that search results lower on the search results page benefit from higher visitation rates when those results are appended with privacy indicators.

11.2 Recommendations

In this research and in other research [17], we see that the same types of privacy concerns continue to persist, despite changes in technology. Similarly, the same dimensions of privacy concern continue to exist across different types of technology domains. While this research focused specifically on mobile location-sharing technologies and Internet search and website privacy policies, the implications of this research impact other areas where the users have similar privacy concerns (such as in social networking sites or the adoption of cloud computing technologies). We provide recommendations related to the use and adoption of salient privacy information in three domains: public policy, business, and technology development.

11.2.1 Recommendations for Public Policy

The recommendations apply for multiple types of policy makers, ranging from those in the federal or state government, to those who define industry standards, to those within each organization.

Privacy salience is essential for effectiveness: Mandating that policies exist or that information be made available is not the same as ensuring that information is visible or understandable. In the United States, financial institutions (as mandated by the Gramm-Leach-Bliley Act was enacted in 1999) and Internet merchants who do business with consumers residing in California (as mandated by the State of California's Online Privacy Protection Act of 2003) must provide privacy notices to their consumers. In general, we see that people tend to ignore and misunderstand these privacy policies [117]. When this privacy information is made more salient, this research has shown that users can better incorporate privacy policy information into their decision-making.

When policymakers deal with standards or regulations to provide information regarding information practices, they should consider how that information can have an impact and how they can require that the information be make prominent and usable.

Mandate user testing and evaluation: To enforce policies mandating salient privacy information, include provisions in regulations to ensure that user testing occurs for the evaluation of mandated policies. One good example is the Federal Trade Commission's (FTC) project to develop alternative forms of financial privacy notices for consumers through consumer testing [47].

Consider controls for privacy: When developing regulations (or overseeing the development of regulations) related to consumer privacy, ensure that provisions exist that provide people with control. Depending on the domain, that control can be in the form of controlling the disclosure or sharing of personal information. In the domain of consumer privacy, control may be presented as the ability to opt in or opt out of organization's mailing lists. Other forms of control include the ability to create rules governing the release of personal information, such as one's location or profile information.

Directly address privacy concerns: When crafting guidelines to address users' privacy concerns, ensure that those guidelines address those concerns. To help mobile and wireless providers protect user privacy, CTIA, the International Association for the Wireless

Telecommunications Industry,[1] issued Best Practices and Guidelines for LBS providers. These guidelines highlight *user notice* regarding the provider's use, disclosure, and protection of location information and *consent* regarding the disclosure of information to third parties [1]. Unfortunately, these guidelines do not address users' most prevalent concerns, that of being stalked or revealing the location of their home to others they wish to avoid.

To encourage adoption of a new technology and to minimize users' privacy concerns, policy makers should seek to understand those privacy concerns. Any guidelines developed should directly address those concerns. In the case for location-sharing applications, in addition to the use of location information by third parties, privacy policies should also address how users can control access to location information and notice regarding location requests.

11.2.2 Recommendations for Businesses

Many businesses have a web presence and allow customers to request information or to make purchases online. These organizations can leverage privacy as good business.

Good privacy can be profitable: Adopting P3P and a privacy policy that protects consumer information can be profitable. This research shows that users will pay a premium to purchase from websites that offer better privacy policies if that privacy information is made prominent.

Good privacy can increase visitation rates: A privacy-protective privacy policy can act as a draw, increasing visitation rates when that privacy information is presented in a search

---

[1] The CTIA Wireless Association. `http://www.ctia.org/`

engine interface. In the Privacy Finder Usage study, we found that having privacy indicators had a positive impact on search result browsing patterns.

11.2.3 Recommendations for Technology Development

Developers who are creating applications to leverage and share users' information should be aware of their information practices and users' privacy concerns regarding the use of these applications.

Consider the context of your technology while you are designing its privacy features: Determine the goals of your application and the context in which it will be used. Consider how the technology may benefit from providing users with salient privacy information to reduce their privacy concerns. Making privacy more salient may increase users' comfort with using your system and increase adoption.

Provide users with the means to define access controls: Having control over the disclosure of one's own personal information may reduce privacy concerns. Users of our location-sharing systems were able to use and define expressive rules to determine with whom, when, and where their location information would be disclosed. This research suggests that being provided with a diverse palette of privacy control options had an impact on reducing users concerns with using location-sharing systems.

11.3 Future Work

Many opportunities exist in the exploration and development of usable privacy policies. While privacy indicators had an impact on consumer decision-making, more work must be done to help users to understand the content and choices offered to them in traditional privacy policies. Additionally, the creation of design standards would significantly aid users by providing them with the means to compare across privacy policies, thus making privacy policies more useful.

Along those lines, other opportunities are available for researchers to evaluate the mental models related to the use of location-sharing technologies. At this point in time, users are struggling with understanding the usefulness of the social aspects of location-sharing technologies. Until a clear use case is elicited, developers will struggle with convincing consumers to adopt the use their technologies. Similarly, users are struggling with how to protect their privacy and security in using cloud computing based technologies. The existing recommendations regarding one's privacy in the cloud ask users to carefully consider each services' privacy policies. As we know, a better way must be developed for users to obtain and understand this privacy information.

Part V

Appendices

A.1 Location Privacy Surveys

A.1.1 Location Privacy Concerns Study

Appendix. Location-Sharing Applications

As of 8/26/2009

Open Systems: Users can be requested by people with whom they do not have a connection (i.e. Strangers)

Closed Systems: Users must be "Friends" or connected to one another

***** Application also has time and location-based access restrictions

Application	Creation Date	URL	System	Accessible Privacy	Privacy Policy	Black-list	Explicit Request	Friends	Gran-ularity	Group	In-visible	Network	Time Expire	None	N/A	Un-known
Aka-Aki	03/01/07	http://www.aka-aki.com/	Open	No	Yes			X			X					
Belysio	08/22/08	http://www.belysio.com/	Open	No	Yes			X			X	X				
Bliin	10/17/06	http://www.bliin.com/	Open	No	No			X			X					
Bluemapia	06/17/08	http://www.bluemapia.com/	Open	No	No						X					
Blummi!	10/18/08	http://www.blummi.com/	Open	Unknown	No				X							
Brightkite	04/01/07	http://www.brightkite.com/	Open	Yes	Yes			X	X	X	X	X				
Buddy Beacon	11/10/06	http://where.com/buddybeacon/	Open	No	Yes	X										
BuddyCloud	04/01/08	http://www.buddycloud.com/cms/	Open	No	No				X							
BuddyMob	12/01/08	http://www.buddymob.com/	Open	No	No									-		
Buddyway	08/11/08	http://www.buddyway.com/	Open	No	No									-		
Buzzd	02/06/08	http://buzzd.com/	Open	No	Yes			X			X					
Carticipate	03/08/08	http://www.carticipate.com/	Open	No	Yes									-		
Centrl	03/16/07	http://centrl.com/	Open	No	Yes			X				X				
CitySense	06/09/08	http://www.citysense.com/	N/A	NA	Yes										-	
ComeTogethr	10/01/08	http://www.cometogethr.com/	Open	Yes	Yes			X		X	X					
Dopplr	07/01/07	http://www.dopplr.com/	Closed	No	No			X								
EagleTweet	04/04/09	http://eagletweet.com/	Open	No	No											
FindbyClick	12/21/06	http://www.findbyclick.com	N/A	NA	No										-	
FindMe	03/18/08	http://electricpocket.com/findme/	Open	No	No						X					
FireEagle	08/12/08	http://fireeagle.yahoo.net/	API	Yes	Yes				X		X	X				
Flaik	11/26/07	http://www.flaik.com/	Open	Unknown	No											-
Footprint History	02/01/09	http://www.footprinthistory.com/	Closed	No	Yes			X								
FourSquare	03/13/09	http://playfoursquare.com/	Closed	No	Yes			X								
Foyage	12/01/08	http://i.foyage.com	Open	No	No						X					
Friends on Fire	03/13/09	http://apps.facebook.com/on-fire/	Closed	Yes	Yes			X	X							
GeoMe	10/01/08	http://www.geo-me.com	Closed	No	Yes			X								
GeoSpot	03/12/08	http://www.geospot.com/gs/Home	N/A	NA	Yes										-	
GeoUpdater	12/10/08	http://linuxinside.org/geoupdater/	Closed	Yes	Yes			X	X			X				
Google Latitude	02/04/09	http://www.google.com/latitude	Closed	Yes	Yes	X		X								

Application	Creation Date	URL	System	Accessible Privacy	Privacy Policy	Blacklist	Explicit Request	Friends	Granularity	Group	Invisible	Network	Time Expire	None	N/A	Unknown
Groovr	12/29/06	http://www.Groovr.com	Closed	Yes	Yes			X		X						
Gympse	05/22/09	http://www.glympse.com/	Closed	Yes	Yes			X					X			
GyPSii	03/06/08	http://www.GyPSii.com/	Open	No	Yes			X			X					
HeyWay	06/17/09	http://niftybrick.com/heyway.html	Closed	No	No		X	X		X		X				
HiMyTribe	08/07/09	http://www.himytribe.com/	Closed	No	No			X		X						
ICloseby	01/30/08	http://www.icloseby.com	Open	No	No	X										
iPling	06/29/07	http://www.iPling.com	Open	No	Yes				X							
Ipoki	12/18/07	http://www.ipoki.com/	Open	Yes	Yes			X			X					
IRL	04/19/09	http://corp.irlconnect.com	Open	No	No									-		
LightPole	01/01/07	http://www.lightpole.net	N/A	NA	Yes										-	
Limbo	08/01/07	http://www.limbo.com	Open	No	Yes	X				X						
Locaccino*	03/01/09	http://www.locaccino.org	Closed	Yes	Yes			X		X		X				
Locatik	05/22/08	http://www.locatik.com	Open	No	Yes									-		
Locatrix	04/08/09	http://www.locatrix.com	Closed	No	Yes	X		X	X		X					
Locle	10/01/08	http://www.locle.com	Closed	No	No	X		X								
Loki	04/09/07	http://www.loki.com	API	No	Yes		X									
Loopt	11/16/06	http://www.loopt.com	Closed	Yes	Yes	X		X				X				
Map My Tracks	12/23/07	http://www.mapmytracks.com	Open	No	Yes									-		
MapMe	07/01/08	http://www.mapme.com	Open	No	Yes			X			X	X				
Match2Blue	12/21/08	http://www.match2blue.com/cms/	Open	No	Yes									-		
Meet Now Live	04/01/08	http://www.meetnowlive.com	Open	No	Yes									-		
MeetMoi	11/25/08	http://www.meetmoi.com	Open	No	Yes				X							
Microsoft Vine	04/28/09	http://www.vine.net/default.aspx/	Closed	Yes	Yes			X		X						
Mizoon	10/02/08	http://www.mizoon.com/	Open	No	No									-		
Mobilaris	11/01/03	http://www.mobilaris.com	Open	No	No						X					
Mobiluck	09/01/07	http://www.mobiluck.com	Open	Yes	Yes	X		X			X					
Mologogo	10/01/07	http://www.mologogo.com	Open	No	Yes						X					
Moximiti	09/26/08	http://www.moximity.com	Closed	No	Yes			X								
MyGeoDiary	09/17/08	http://www.mygeodiary.com	Open	No	Yes						X					
MyGeolog	12/10/08	http://www.mygeolog.com/	Open	No	No						X	X				
Myrimis	09/04/07	http://www.Myrimis.com	Closed	No	Yes			X								
Now Here	03/22/08	http://www.nowhere.de/	Closed	No	No			X								
Nulaz	04/10/08	http://www.nulaz.net/	Open	No	Yes			X			X					
Plazes	08/16/04	http://www.Plazes.com	Open	No	Yes			X				X				
Pocket Life	12/16/08	http://www.pocketlife.com	Closed	No	Yes			X		X	X					
Quiro	09/01/06	http://www.myqiro.de	Closed	No	Yes			X			X					

Application	Creation Date	URL	System	Accessible Privacy	Privacy Policy	Black-list	Explicit Request	Friends	Gran-ularity	Group	In-visible	Network	Time Expire	None	N/A	Un-known
Rummble	12/13/07	http://www.Rummble.com	Open	Yes (Web), No (Phone)	Yes			X			X					
Shizzow	03/05/09	http://www.shizzow.com	Open	Yes	Yes	X					X					
Skobbler	09/28/08	http://beta.skobbler.de/	Open	No	Yes					X						
Skout	01/16/09	http://www.us.skout.com	Open	No	Yes	X					X					
Sniff	04/01/08	https://www.sniffu.com/us/	Closed	No	Yes	X		X			X					
Snikkr	05/21/09	http://www2.snikkr.net/	Open	No	No						X		X			
Sociallight	10/19/05	http://socialight.com/	Open	No	Yes			X								
Sparrow	02/12/09	http://clickontyler.com/sparrow/	Open	No	No									-		
Spot Adventures	05/21/09	http://www.spotadventures.com	Open	No	Yes						X					
SpotJots	01/29/08	http://www.spotjots.com/	Open	No	No									-		
The Grid	12/30/07	http://www.thegrid.co.za/	Closed	No	Yes			X								
TownKing	07/04/07	http://www.townqueens.com/	Open	No	No									-		
Trackut	10/08/08	http://www.trackut.com	Closed	No	Yes			X								
Trapster	04/01/08	http://www.trapster.com	N/A	NA	Yes										-	
Tripit	06/27/07	http://www.tripit.com/	Closed	No	Yes			X								
Troovy	06/10/07	http://troovy.com/bc/vancouver/	Open	No	No									-		
Twibble	03/17/08	http://www.twibble.de/	Open	No	No									-		
Twinkle	04/01/08	http://tapulous.com/twinkle/	Open	No	Yes									-		
Twittelator	07/11/08	http://www.stone.com/Twittelator/	Open	No	No	X										
WeNear	07/01/08	http://www.wenear.com/	Closed	No	No	X		X			X					
Whereis Everyone	07/03/08	http://everyone.whereis.com/	Closed	No	Yes	X		X	X		X					
WhereYou GonnaBe	04/18/08	http://www.whereyougonnabe.com	Closed	No	No			X								
Whrrl	10/23/07	http://whrrl.com/	Open	No	Yes					X						
Zhiing	10/18/08	http://zhiing.com/	Closed	No	Yes			X								

* Application also has time and location-based access restrictions

surveygizmo

Survey: Location-Sharing Survey

Status: Launched (survey active)

1. Welcome!

Copy page • Delete page •

Thank you for your interest in this mobile technologies survey!

This survey helps us understand how people feel about sharing their information online!

You will need about **15 minutes** to complete this survey.

Participation!

There will be a raffle for a $75 Amazon.com gift cerficate for those who complete the survey.

1. What is your email address? (We need this so we can send you your Amazon.com gift certificate if you win!) *

☐

2. What is your age? *

☐

3. What is your gender? *

○ Female

○ Male

4. Have you heard about technologies that allow you to share your location with other people? *

○ Yes

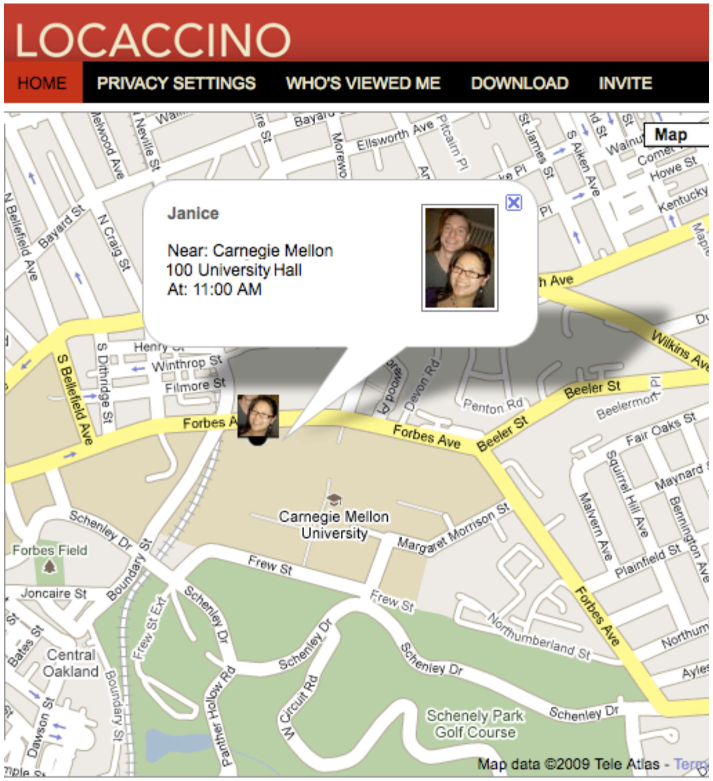
○ No

2. Location-sharing Technologies

Copy page • Delete page •

Several companies have developed technologies that allow you to share your location information. Based on the location of your mobile phone, others may be able to view your information online.

The figure below depicts this type of technology. You can share your information with others. By going to a website, or using a web-enabled mobile application, they will be able to see your location on a map.



Janice

Near: Carnegie Mellon
100 University Hall
At: 11:00 AM

5. Please list some benefits associated with using this type of technology. *

6. Please list some risks or dangers associated with using this type of technology. *

3. Sharing your location

Copy page • Delete page •

Imagine you, your friends, family, and coworkers all use a location-sharing technology. Please answer the following:

7.
How useful would it be for you to be able to share your location with others?
*

1: Not useful	2	3	4	5	6	7: Extremely useful
○	○	○	○	○	○	○

8.
How concerned are you about allowing others to view your location?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

9.
How concerned are you, about controlling who has access to your location?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

10.
Is the risk of making your location available worth the benefits of making your location available?
*

1: The risk far outweighs the benefit	2	3	4	5	6	7: The benefit far outweighs the risk
○	○	○	○	○	○	○

4. Likelihood of Situations

Copy page • Delete page •

11. For each of the following statements, please indicate how likely each of these scenarios would be if you were to use location-sharing technologies.
*

	1 - Very unlikely	2	3	4	5	6	7 - Very Likely
Keeping track of the location of children in your family	○	○	○	○	○	○	○
Having people intrude on your private space	○	○	○	○	○	○	○
Finding information based on your location	○	○	○	○	○	○	○
Coordinating family activities	○	○	○	○	○	○	○
Having your boss spy on you	○	○	○	○	○	○	○
Using people's locations to coordinate a meeting	○	○	○	○	○	○	○
Being found when you want to be alone	○	○	○	○	○	○	○
Being bothered by ads that use your location	○	○	○	○	○	○	○
Finding a coworker who is running late for a meeting	○	○	○	○	○	○	○
Revealing the location of your home to people you do not want to give your address to	○	○	○	○	○	○	○
Having the government track you	○	○	○	○	○	○	○
Revealing activities you are participating in	○	○	○	○	○	○	○
Being found by someone you don't want to see	○	○	○	○	○	○	○
Finding new people with similar interests	○	○	○	○	○	○	○
Being stalked	○	○	○	○	○	○	○
Being judged based on your location	○	○	○	○	○	○	○
Keeping track of where	○	○	○	○	○	○	○

you've been	○	○	○	○	○	○	○
Checking people's locations to make sure they are ok	○	○	○	○	○	○	○
Finding nearby friends for social activities	○	○	○	○	○	○	○
Coordinating ride sharing or carpooling	○	○	○	○	○	○	○
Recruiting people to participate in activities	○	○	○	○	○	○	○
Discovering that a friend from out of town is visiting	○	○	○	○	○	○	○
Finding people in an emergency	○	○	○	○	○	○	○
Keeping track of elderly relatives	○	○	○	○	○	○	○
Having fun with locations (e.g. games, pranks)	○	○	○	○	○	○	○

5. Situations

Copy page • Delete page •

12. For each of the following statements, please indicate how harmful you perceive each situation.
*

	1 - Not harmful at all	2	3	4 - Moderately harmful	5	6	7 - Extremely harmful
Having your boss spy on you	○	○	○	○	○	○	○
Revealing activities you are participating in	○	○	○	○	○	○	○
Revealing the location of your home to people you wouldn't want to give your address to	○	○	○	○	○	○	○
Being found when you want to be alone	○	○	○	○	○	○	○
Being judged based on your location	○	○	○	○	○	○	○
Having the government track you	○	○	○	○	○	○	○
Having people intrude on your private space	○	○	○	○	○	○	○

Being found by someone you don't want to see	○	○	○	○	○	○	○
Being bothered by ads that use your location	○	○	○	○	○	○	○
Being stalked	○	○	○	○	○	○	○

13. For each of the following statements, please indicate the benefit you would obtain from each situation.
*

	1 - No benefits at all	2	3	4 - Moderate benefit	5	6	7 - Great benefits
Using people's locations to coordinate a meeting	○	○	○	○	○	○	○
Keeping track of where you've been	○	○	○	○	○	○	○
Keeping track of children in your family	○	○	○	○	○	○	○
Coordinating ride sharing or carpooling	○	○	○	○	○	○	○
Discovering that a friend from out of town is visiting	○	○	○	○	○	○	○
Keeping track of of elderly relatives	○	○	○	○	○	○	○
Finding nearby friends for social activities	○	○	○	○	○	○	○
Finding information based on your location	○	○	○	○	○	○	○
Having fun with locations (e.g. games, pranks)	○	○	○	○	○	○	○
Recruiting people to participate in activities	○	○	○	○	○	○	○
Finding people in an emergency	○	○	○	○	○	○	○
Coordinating family activities	○	○	○	○	○	○	○
Finding a coworker who is running late for a meeting	○	○	○	○	○	○	○
Checking people's locations to make sure they are ok	○	○	○	○	○	○	○
Finding new people with similar interests	○	○	○	○	○	○	○

6. Location-Sharing Attitudes

Copy page • Delete page •

14.
Now that you know a bit more about the technology, how useful would it be for you to be able to share your location with others?
*

1: Not useful	2	3	4	5	6	7: Extremely useful
○	○	○	○	○	○	○

15.
Now that you know a bit more about the technology, how concerned are you about allowing others to view your location?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

16.
Is the risk of making your location available worth the benefits of making your location available?
*

1: The risk far outweighs the benefit	2	3	4	5	6	7: The benefit far outweighs the risk
○	○	○	○	○	○	○

17. Please rate the likelihood of the following groups of people using location-sharing technologies. (Assume that everyone has the technology (e.g. mobile phone), and that it is free.) *

	1 - Very unlikely	2	3	4	5	6	7 - Very Likely
You	○	○	○	○	○	○	○
Your family	○	○	○	○	○	○	○
Your friends	○	○	○	○	○	○	○
Your company or employer	○	○	○	○	○	○	○

7. Privacy

Copy page • Delete page •

18. Please rate how much you agree or disagree with the following statements. *

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	○	○	○	○	○	○	○
I'm concerned that online companies are collecting too much personal information about me.	○	○	○	○	○	○	○
Online companies should have better procedures to correct errors in personal information.	○	○	○	○	○	○	○
Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	○	○	○	○	○	○	○
Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers.	○	○	○	○	○	○	○
I am concerned about threats to my personal privacy today.	○	○	○	○	○	○	○

8. Demographics

Copy page • Delete page •

19. How many people live in your household (including you)?
*

☐

20. How many children do you have? *

☐

21. If you have children, how old are they?

22. What is your highest level of education? *

○ Some high school
○ High school diploma
○ College degree
○ Graduate degree
○ Professional degree (including trade school)

23. What is your occupation? *

24. Please let us know if you have any feedback or comments!

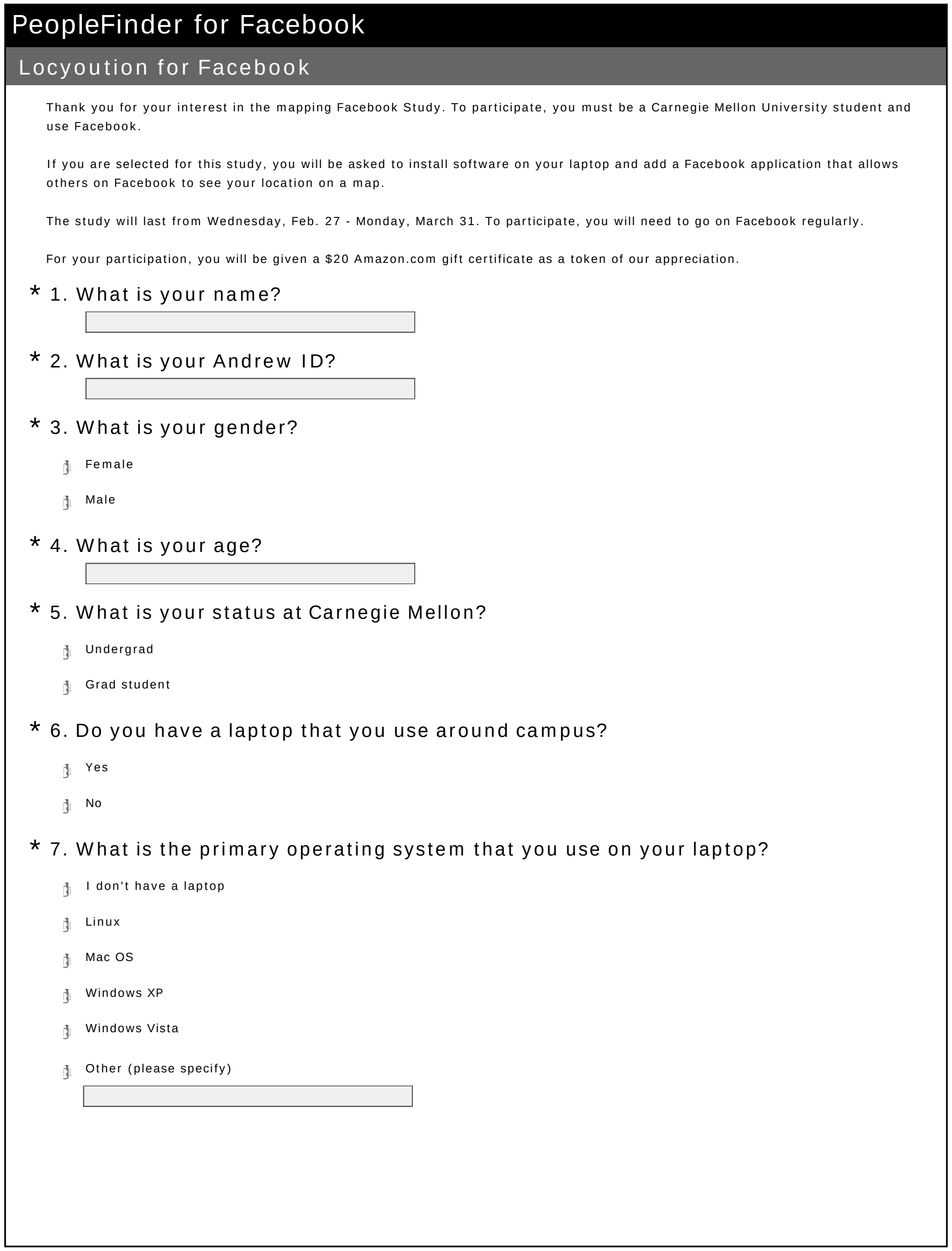
'Thank You'/Redirect Page

Thank you for completing this survey!

You will be notified in 2 weeks whether or not you won the raffle!

A.1.2 Location-Sharing Feedback Study 1 (Locyoution)

Locyoution Screening Survey



PeopleFinder for Facebook

Locyoution for Facebook

Thank you for your interest in the mapping Facebook Study. To participate, you must be a Carnegie Mellon University student and use Facebook.

If you are selected for this study, you will be asked to install software on your laptop and add a Facebook application that allows others on Facebook to see your location on a map.

The study will last from Wednesday, Feb. 27 - Monday, March 31. To participate, you will need to go on Facebook regularly.

For your participation, you will be given a $20 Amazon.com gift certificate as a token of our appreciation.

* 1. What is your name?

* 2. What is your Andrew ID?

* 3. What is your gender?

○ Female

○ Male

* 4. What is your age?

* 5. What is your status at Carnegie Mellon?

○ Undergrad

○ Grad student

* 6. Do you have a laptop that you use around campus?

○ Yes

○ No

* 7. What is the primary operating system that you use on your laptop?

○ I don't have a laptop

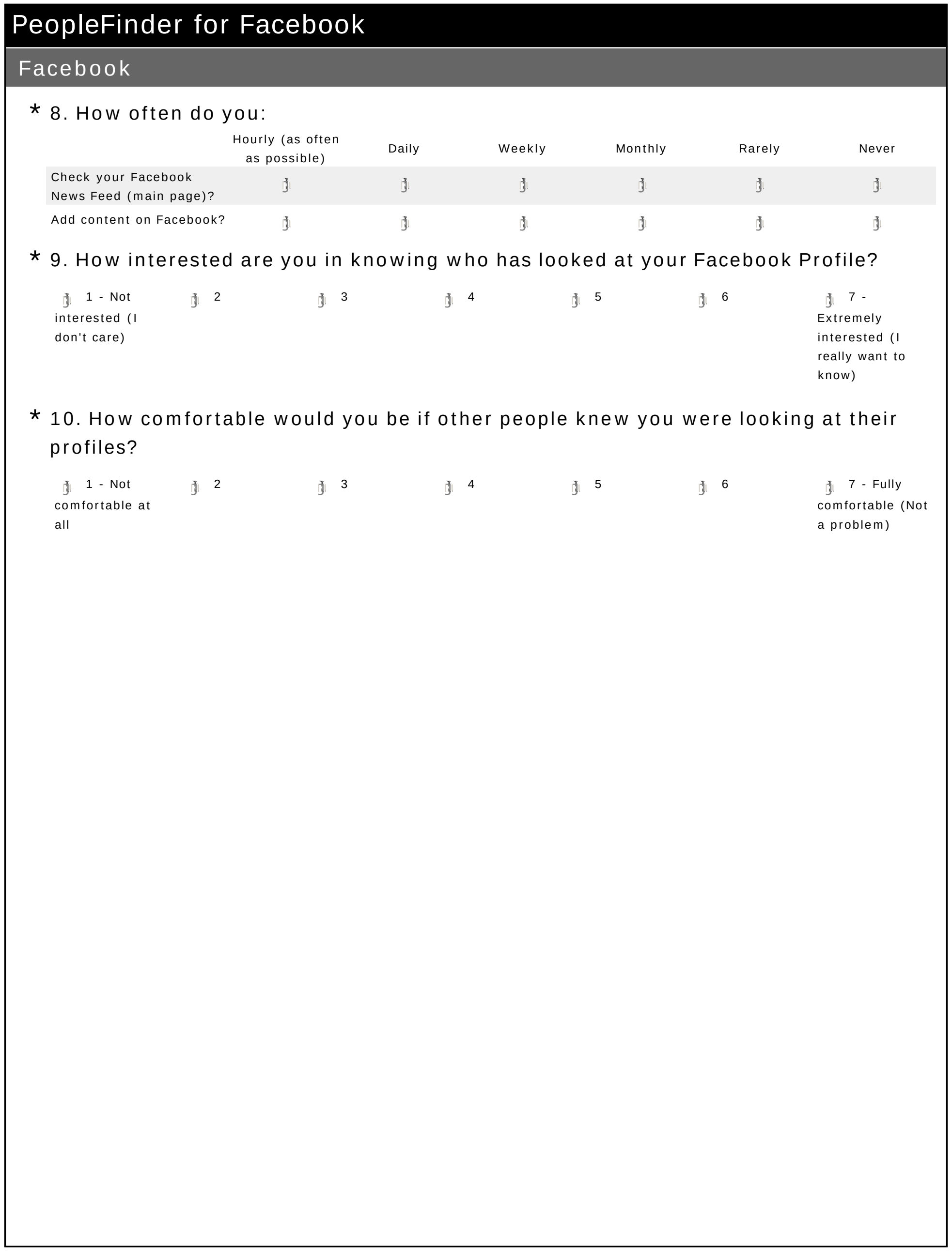
○ Linux

○ Mac OS

○ Windows XP

○ Windows Vista

○ Other (please specify)



PeopleFinder for Facebook

Facebook

* 8. How often do you:

	Hourly (as often as possible)	Daily	Weekly	Monthly	Rarely	Never
Check your Facebook News Feed (main page)?	○	○	○	○	○	○
Add content on Facebook?	○	○	○	○	○	○

* 9. How interested are you in knowing who has looked at your Facebook Profile?

○ 1 - Not interested (I don't care)	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7 - Extremely interested (I really want to know)

* 10. How comfortable would you be if other people knew you were looking at their profiles?

○ 1 - Not comfortable at all	○ 2	○ 3	○ 4	○ 5	○ 6	○ 7 - Fully comfortable (Not a problem)

PeopleFinder for Facebook

Location Sharing

* 11. Imagine that you are using a location-finding application (on your phone or computer) that allows other people to see your location on a Google map on their phones or on a webpage.

Please rate how comfortable you would be if close friends could check your location:

	1 - Not comfortable at all	2	3	4	5	6	7 - Fully comfortable (Not a problem)
Anytime	○	○	○	○	○	○	○
At times you have specified	○	○	○	○	○	○	○
At locations you have specified	○	○	○	○	○	○	○

* 12. Please rate how comfortable you would be if acquaintances could check your location:

	1 - Not comfortable at all	2	3	4	5	6	7 - Fully comfortable (Not a problem)
Anytime	○	○	○	○	○	○	○
At times you have specified	○	○	○	○	○	○	○
At locations you have specified	○	○	○	○	○	○	○

* 13. Please rate how comfortable you would be if strangers could check your location:

	1 - Not comfortable at all	2	3	4	5	6	7 - Fully comfortable (Not a problem)
Anytime	○	○	○	○	○	○	○
At times you have specified	○	○	○	○	○	○	○
At locations you have specified	○	○	○	○	○	○	○

* 14. Please rate how concerned you would be, overall, for your privacy when using a location-finding application.

○ 1 - Not concerned ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Extremely concerned

* 15. How often do you expect the following to happen:

	Never	Seldom (Less than once a week)	Sometimes (Several times a week)	Regularly (More than once a day)	A lot (More than 10 times a day)
Other people check your location	○	○	○	○	○
You check other people's location	○	○	○	○	○

PeopleFinder for Facebook

Technical Affinity

16. Please rate how much you agree or disagree with the following statements.

	1 - Strongly disagree	2	3	4	5	6	7 - Strongly agree
I can solve most technical problems I am confronted with.	○	○	○	○	○	○	○
Technical equipment is often difficult to understand and master.	○	○	○	○	○	○	○
I really enjoy solving technical problems.	○	○	○	○	○	○	○

PeopleFinder for Facebook

Privacy Concerns

* 17. Please rate how much you agree or disagree with the following statements.

	1 - Strongly disagree	2	3	4	5	6	7 - Strongly agree
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	○	○	○	○	○	○	○
I'm concerned that online companies are collecting too much personal information about me.	○	○	○	○	○	○	○
Online companies should have better procedures to correct errors in personal information.	○	○	○	○	○	○	○
Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	○	○	○	○	○	○	○
Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers.	○	○	○	○	○	○	○
I am concerned about threats to my personal privacy today.	○	○	○	○	○	○	○

PeopleFinder for Facebook

Thank You!

Thank you for filling out our survey.

You will be contacted in the next few days if you are selected for this study.

Locyoution Exit Survey (Feedback Condition)

CMU Locyoution - Facebook Study (Group 1)

1. Locyoution for Facebook Exit Survey

Thank you for participating in the Locyoution for Facebook Study.

Upon completion of the exit survey, you will receive a $20 Amazon.com gift certificate.

* 1. What is your Andrew ID? (We need this so we can send you your Amazon.com gift certificate!)

☐

* 2. For the last several weeks, you were using an online location-finding application called Locyoution in Facebook.

Please answer the following questions about your experiences with the technology.

	1 - Very unwelcome	2	3	4	5 - Very welcome
Allowing other people to see where I am is...	○	○	○	○	○

* 3. Are you interested in continuing to use Locyoution for Facebook?

○ Yes

○ No

* 4. Please select whether you agree or disagree with the following statements:

	1 - Strongly disagree	2	3	4	5	6	7 - Strongly agree
I could easily and clearly explain the PeopleFinder/Locyoution technology to people who had never heard of it.	○	○	○	○	○	○	○
It was easy to get everything installed and working for Locyoution.	○	○	○	○	○	○	○
It was easy to view my location in Facebook (once I got everything installed and working).	○	○	○	○	○	○	○
People who influence my behavior (peers, friends, etc.) think I should use Locyoution.	○	○	○	○	○	○	○
If my friends knew about Locyoution, they would want to share their locations on Facebook, too.	○	○	○	○	○	○	○
I liked being able to share my location in Facebook.	○	○	○	○	○	○	○

5. Please provide us with any comments you have about the installation process.

☐

CMU Locyoution - Facebook Study (Group 1)

2. Location Sharing

* 6. Please rate how concerned were you, overall, for your privacy when using this location-finding application.

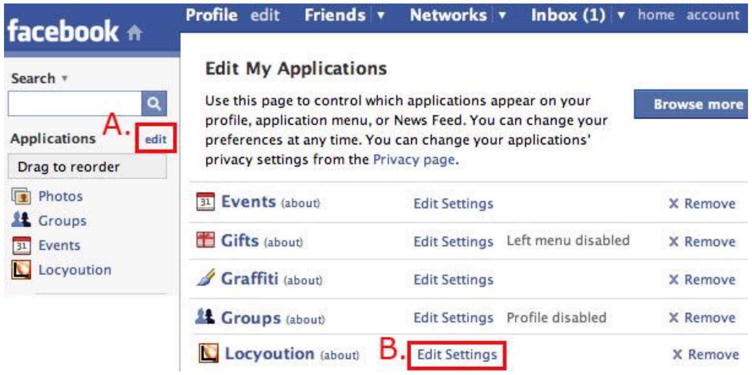
○ 1 - Not concerned ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Extremely concerned

* 7. How comfortable were you with allowing the following people to check your location?

	1 - Not comfortable at all	2	3	4	5	6	7 - Fully comfortable (Not a problem)	N/A
Close friends	○	○	○	○	○	○	○	○
Acquaintances	○	○	○	○	○	○	○	○
Strangers (in your network)	○	○	○	○	○	○	○	○

To answer the next question, you must check your privacy settings for Locyoution for Facebook.

Open Facebook.
A. Click on EDIT on the left bar in Facebook.
B. Click on Edit Settings for Locyoution.



Edit My Applications

Use this page to control which applications appear on your profile, application menu, or News Feed. You can change your preferences at any time. You can change your applications' privacy settings from the Privacy page.

Events (about)	Edit Settings		✕ Remove
Gifts (about)	Edit Settings	Left menu disabled	✕ Remove
Graffiti (about)	Edit Settings		✕ Remove
Groups (about)	Edit Settings	Profile disabled	✕ Remove
Locyoution (about)	Edit Settings		✕ Remove

CMU Locyoution - Facebook Study (Group 1)

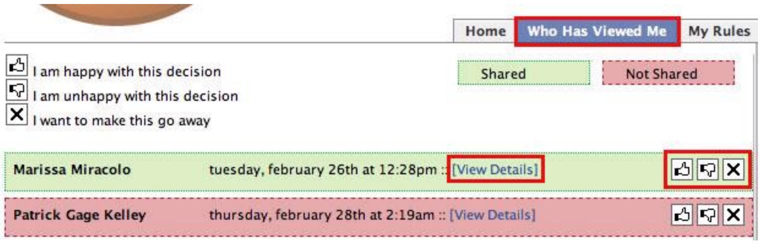
* 8. What privacy setting did you set for Locyoution?

○ All of my networks and all of my friends
○ Some of my networks and all of my friends
○ Only my friends
○ Only me
○ No one
○ I don't know
○ I never got the application working
○ Custom
☐

CMU Locyoution - Facebook Study (Group 1)

3. Who Has Viewed You

Please answer the following questions about the "Who Has Viewed Me" feature of Locyoution for Facebook.



I am happy with this decision
I am unhappy with this decision
I want to make this go away

Marissa Miracolo tuesday, february 26th at 12:28pm :: [View Details]
Patrick Gage Kelley thursday, february 28th at 2:19am :: [View Details]

* 9. Did you notice the "Who Has Viewed Me" tab?

○ Yes
○ No

* 10. Did you ever check to see who had viewed you?

○ Yes
○ No

* 11. If you checked to see who had viewed you, were you happy that this feature was available?

○ Yes
○ No
○ I never checked

* 12. Do you agree or disagree with the following statement:

Using Locyoution, I believe that the technology is strong enough to allow me to control who has access to my location.

○ 1 - Strongly disagree ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Strongly agree

* 13. Would you rather not know who has viewed you?

○ Yes
○ No

CMU Locyoution - Facebook Study (Group 1)

* 14. Does being able to see Who Has Viewed You make you more willing to share your location with others? (Compared to not knowing who is viewing you).

○ Yes

○ No

○ I don't know

* 15. There are tradeoffs when systems allow users to see who has viewed them. Would you prefer a closed system where no one can see requests being made, or a system where all users can see the requests made of them.

○ Closed system (no notifications)

○ System where you can see all requests (notifications)

16. Please provide us with any comments you have about the Who Has Viewed Me feature.

CMU Locyoution - Facebook Study (Group 1)

4. Rules

In order for others to view your location on Facebook, you needed to set up rules to allow that access. Please answer the following question about your rules.

* 17. Please rate how easy was it to create a rule to define when people could see you.

○ 1 - Not easy ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Very easy

* 18. How confident are you that your rules accurately represented your privacy preferences?

○ 1 - Not confident ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Very confident

* 19. How confident are you that people could NOT see your location when you did not what them to (i.e. confident that the rules worked)?

○ 1 - Not confident ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Very confident

* 20. Do you agree or disagree with the following statement.

Rules based on specific time ranges gave me enough control over when people could see me.

○ 1 - Strongly disagree ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 - Strongly agree

* 21. How likely would it be for you to use the following features:

	1 - Very unlikely	2	3	4	5	6	7 - Very likely
Rules based on your location (i.e. allow people to see my location only when I am on campus).	○	○	○	○	○	○	○
Rules based on a specific person, group of people, or friend list.	○	○	○	○	○	○	○
Rules that allowed only people located near you to see your location (i.e. 1 mile).	○	○	○	○	○	○	○
Rules that allow people to see an approximate location (i.e. city or state).	○	○	○	○	○	○	○

22. Please describe any other types of rules or restrictions that you would like to place on when people can see your location with Locyoution.

CMU Locyoution - Facebook Study (Group 1)

5. Technology

* 23. Please select whether you agree or disagree with the following statements:

	1 - Strongly disagree	2	3	4	5	6	7 - Strongly agree
New technology renders everyday life easier or more complicated.	○	○	○	○	○	○	○
Humans are overrun by new technology.	○	○	○	○	○	○	○
New technology represents positive progress for human kind.	○	○	○	○	○	○	○

* 24. Please select whether you agree or disagree with the following statements:

	1 - Strongly disagree	2	3	4	5	6	7 - Strongly agree
I would feel helplessly exposed when using a location-finding application.	○	○	○	○	○	○	○
No matter what I do, I will not be in a position to control the sharing of my location with Locyoution.	○	○	○	○	○	○	○
Nothing can protect me from being located (in general).	○	○	○	○	○	○	○
I perceive that I have no influence over who views my location in Locyoution.	○	○	○	○	○	○	○

25. What changes would you like to see us make to Locyoution to make it more useful to you?

CMU Locyoution - Facebook Study (Group 1)

6. Thank You!

Thanks again for participating in this study. If you would like to continue using Locyoution, feel free to do so. We will continue to collect the same Locyoution usage data that we have been collecting throughout the study, using it for research purposes only.

If you would like to uninstall the Locyoution/PeopleFinder software, simply remove the program. (Windows: PeopleFinder and Skyhook, Mac: PF4Mac)

You will receive a $20 Amazon.com gift certificate via email in the next few days in appreciation of your participation.

A.1.3 Location-Sharing Feedback Study 2 (Locaccino)

Locaccino Screening Survey

surveygizmo

Survey: **LOCACCINO - CMU Study** Status: **Launched**

1. Introduction

Copy page • Delete page •

Thank you for your interest in Locaccino!
Locaccino was created by the Mobile Commerce Lab, a research group at Carnegie Mellon University.
Prior to using Locaccino we would appeciate if you could spend a few minutes to fill out the following survey.
This survey is intended to help us better understand people's attitudes towards using social applications like Locaccino.

Requirements:
* You must be a member of the Carnegie Mellon community
* You must be an active user of Facebook
* You must use a wifi-enabled Laptop

Participation!
You will receive a $20 Amazon.com gift certificate after using Locaccino for a month.

1. What is your andrew ID? *

2. What is your age? *

3. What is your gender? *

○ Female
○ Male

4. What is your affiliation with Carnegie Mellon? *

-- Please Select --

5. Do you have a laptop that you use regularly? *

○ Yes
○ No

6. If so, how frequently do you move your laptop between home and other locations? *

○ Several times per day
○ Almost every day
○ A few times a week
○ About once a week
○ Occasionally or never

○ I don't have a laptop

7. If you have a laptop, how many hours a day do you spend using it?
*

○ Less than 3 hours
○ 3-7 hours
○ 7-12 hours
○ 12-18 hours
○ More than 18 hours
○ I don't have a laptop

8. If you are a student, please list your major(s).

9. Please list the dorm or neighborhood in which you reside (e.g. CMU - Donner Hall or Pittsburgh - Shadyside). *

10. Please rate how much you agree or disagree with the following statements. *

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
I can solve most computer-related technical problems I am confronted with.	○	○	○	○	○	○	○
Computer-related technical equipment is often difficult to understand and master.	○	○	○	○	○	○	○
I really enjoy solving computer-related technical problems.	○	○	○	○	○	○	○

2. Facebook

Copy page • Delete page •

11.
How useful would it be for you to be able to share your location with others?
*

1: Not useful	2	3	4	5	6	7: Extremely useful
○	○	○	○	○	○	○

12.
How concerned are you, about allowing others to view your location?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

13.
How concerned are you, about controlling who has access to your location?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

14.
How often do you browse Facebook?
*

Never	Rarely	Monthly	Weekly	Daily	All the time
○	○	○	○	○	○

15. How interested are you in knowing who has looked at your Facebook Profile? *

1: Not interested (I don't care)	2	3	4	5	6	7: Extremely interested (I really want to know)
○	○	○	○	○	○	○

16. How comfortable would you be if other people knew you were looking at their profiles? *

1: Not comfortable at all	2	3	4	5	6	7: Fully comfortable (not a problem)
○	○	○	○	○	○	○

3. Facebook Settings

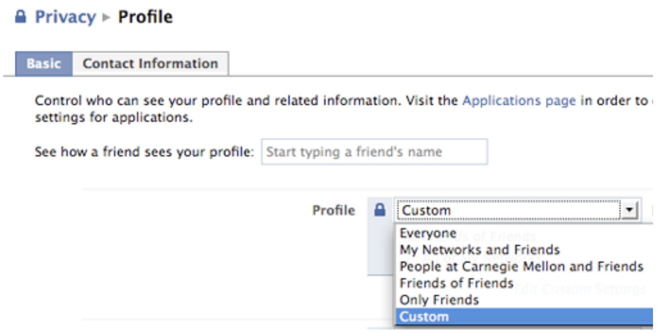
Copy page • Delete page •

We're interesting in knowing what kind of privacy settings you have for Facebook.

On Facebook, who can see your Profile?

The image below shows you where this setting is located.
To check your Facebook Privacy Settings click HERE (opens in a new window).

Facebook Privacy - Profile Settings



Control who can see your profile and related information. Visit the Applications page in order to
settings for applications.

See how a friend sees your profile: Start typing a friend's name

Profile: Custom

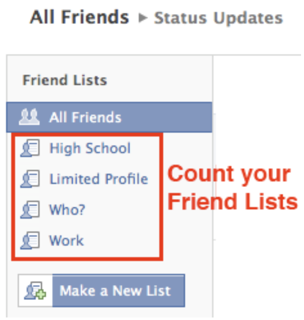
17. Who can see your Profile? Please select all that apply (i.e., if you have selected "Custom"). *

- ☐ Everybody
- ☐ My Networks and Friends
- ☐ People at [Network] and Friends
- ☐ Friends of Friends
- ☐ Only Friends
- ☐ Custom

How many Friends Lists do you have?

The image below indicates where you can find your friend lists.
Click HERE to go to to the Friends page in Facebook (opens in a new window).

Facebook Friends page - Friend Lists



Count your Friend Lists

18. How many Friends Lists do you have? *

19. What are some of the names of your Friend Lists?

4. Location-Sharing

Copy page • Delete page •

Imagine that you are using a location-sharing application (on your phone or computer) that allows other people to see your location on a Google map on their phones or on a webpage.

20. Please rate how comfortable you would be if close friends could check your location: *

	1: Not comfortable at all	2	3	4	5	6	7: Fully comfortable (not a problem)
Anytime	○	○	○	○	○	○	○
Only at times you have specified	○	○	○	○	○	○	○
Only at locations you have specified	○	○	○	○	○	○	○

21. Please rate how comfortable you would be if acquaintances could check your location: *

	1: Not comfortable at all	2	3	4	5	6	7: Fully comfortable (not a problem)
Anytime	○	○	○	○	○	○	○
Only at times you have specified	○	○	○	○	○	○	○
Only at locations you have specified	○	○	○	○	○	○	○

22. Please rate how comfortable you would be if strangers could check your location: *

	1: Not comfortable at all	2	3	4	5	6	7: Fully comfortable (not a problem)
Anytime	○	○	○	○	○	○	○
Only at times you have specified	○	○	○	○	○	○	○
Only at locations you have specified	○	○	○	○	○	○	○

5. Privacy

Copy page • Delete page •

23. Please rate how much you agree or disagree with the following statements. *

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
It is very important to me that I am aware and knowledgeable about how my personal information will be used.	○	○	○	○	○	○	○
I'm concerned that online companies are collecting too much personal information about me.	○	○	○	○	○	○	○
Online companies should have better procedures to correct errors in personal information.	○	○	○	○	○	○	○
Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.	○	○	○	○	○	○	○
Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers.	○	○	○	○	○	○	○
I am concerned about threats to my personal privacy today.	○	○	○	○	○	○	○

6. Thank you

Copy page • Delete page •

Thank you for your interest in this study. Unfortunately, you are not eligible to participate.

7. Untitled Page

Copy page • Delete page •

Locaccino Exit Survey (Feedback Condition)

surveygizmo

Survey: **LOCACCINO - Exit Survey (Feedback)** Status: **Closed**

1. Introduction

Copy page • Delete page •

Thank you for your participation!
Upon completion of this survey, you will be sent a $20 Amazon.com gift certificate via email.

1. What is your andrew ID? *

☐

2. How useful was being able to share your location with others?
*

1: Not useful at all	2	3	4	5	6	7: Extremely useful
○	○	○	○	○	○	○

3. Please list any good things that happened as a result of your use of Locaccino. *

4. Please list any bad things that happened as a result of your use of Locaccino. *

5. Are you interested in continuing to use Locaccino? *

○ Yes
○ No

6. Please select whether you agree or disagree with the following statements: *

	1: Strongly disagree	2	3	4	5	6	7: Strongly agree
I could easily and clearly explain what Locaccino was to people who had never heard of it.	○	○	○	○	○	○	○
It was easy to get everything installed and working for Locaccino.	○	○	○	○	○	○	○
It was easy to view my location in Facebook (once I got everything installed and working).	○	○	○	○	○	○	○
People who influence my behavior (peers, friends, etc.) think I should use Locaccino.	○	○	○	○	○	○	○
If my friends knew about Locaccino, they would want to share their locations on Facebook, too.	○	○	○	○	○	○	○
I liked being able to share my location in Facebook.	○	○	○	○	○	○	○

---

7. Please provide us with any comments you have about the installation process.

2. Location-sharing

Copy page • Delete page •

8.
How concerned were you for your privacy when using Locaccino?
*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

9. How comfortable were you allowing the following people to check your location? *

	1: Not comfortable at all	2	3	4	5	6	7: Very comfortable
Close friends	○	○	○	○	○	○	○
Acquaintances	○	○	○	○	○	○	○
Strangers	○	○	○	○	○	○	○

3. Facebook Settings

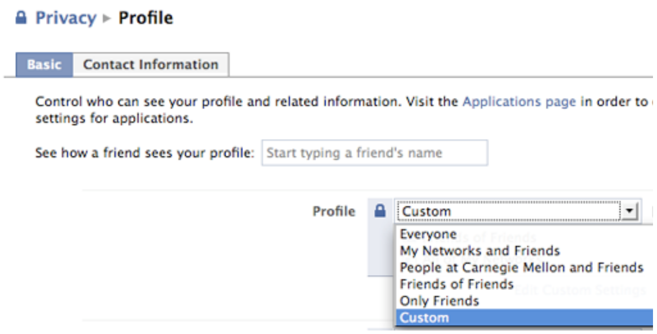
Copy page • Delete page •

We're interesting in knowing what kind of privacy settings you have for Facebook.

On Facebook, who can see your Profile?

The image below shows you where this setting is located.
To check your Facebook Privacy Settings click HERE (opens in a new window).

Facebook Privacy - Profile Settings



Privacy ▸ Profile

Control who can see your profile and related information. Visit the Applications page in order to settings for applications.

See how a friend sees your profile: Start typing a friend's name

Profile: Custom

10. Who can see your Profile? Please select all that apply (i.e., if you have selected "Custom"). *

☐ Everybody
☐ My Networks and Friends
☐ People at [Network] and Friends
☐ Friends of Friends
☐ Only Friends
☐ Custom

4. Privacy Settings

Copy page • Delete page •

In order for others to view your location on Facebook, you needed to set up rules to allow that access. Please answer the following question about your rules.

11.
How concerned are you, about controlling who has access to your location?

---

*

1: Not concerned	2	3	4	5	6	7: Extremely concerned
○	○	○	○	○	○	○

12.
How easy was it to create rules to define when people could see you?
*

1: Not easy	2	3	4	5	6	7: Extremely easy
○	○	○	○	○	○	○

13.
How confident are you that your rules accurately represented your privacy preferences?
*

1: Not confident	2	3	4	5	6	7: Extremely confident
○	○	○	○	○	○	○

14.
How confident are you that your rules worked (i.e. people could only see your location when you wanted them to)?
*

1: Not confident	2	3	4	5	6	7: Extremely confident
○	○	○	○	○	○	○

15. Which type of rules did you use? (Check all that apply.) *

☐ People/Locaccino List
☐ Facebook Network (i.e. Carnegie Mellon)
☐ Time
☐ Location

16. Please rate the usefulness of each type of rules you had available. *

	1: Not useful at all	2	3	4	5	6	7: Extremely useful
People/Locaccino List	○	○	○	○	○	○	○
Facebook Network (i.e. Carnegie Mellon)	○	○	○	○	○	○	○
Time	○	○	○	○	○	○	○
Location	○	○	○	○	○	○	○
A combination of the different types	○	○	○	○	○	○	○

17. Please rate how useful these types of rules would be in controlling access to the following: *

1: Not
7: Extremely

	useful at all	2	3	4	5	6	7: Extremely useful
Your Calendar	○	○	○	○	○	○	○
Photos	○	○	○	○	○	○	○
Profile Information	○	○	○	○	○	○	○
Contact Information	○	○	○	○	○	○	○
Status Updates	○	○	○	○	○	○	○

18. Did you feel any pressure from your friends to modify your rules? *

○ Yes

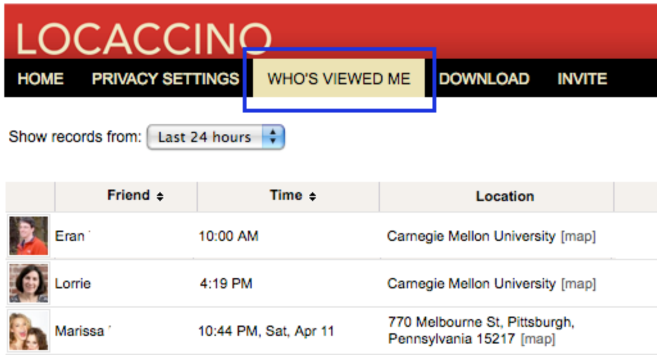
○ No

19. If so, what kind of changes did they want you to make to your rules?

5. Who's Viewed Me

Copy page • Delete page •

Please answer the following questions about the "Who's Viewed Me" feature of Locaccino.



Show records from: Last 24 hours

Friend	Time	Location
Eran	10:00 AM	Carnegie Mellon University [map]
Lorrie	4:19 PM	Carnegie Mellon University [map]
Marissa	10:44 PM, Sat, Apr 11	770 Melbourne St, Pittsburgh, Pennsylvania 15217 [map]

20. Did you notice the "Who's Viewed Me" tab? *

○ Yes

○ No

21. Did you ever check to see who'd checked your location? *

○ Yes

○ No

22. How useful was being able to see who'd checked your location? *

1: Not useful at all	2	3	4	5	6	7: Extremely useful
○	○	○	○	○	○	○

23. Does being able to check "Who's Viewed Me" make you more willing to share your location online (compared with not knowing who is checking your location)? *

○ Yes

○ No

○ I don't know

24.

What was your level of comfort for checking OTHER people's locations after viewing "Who's Viewed Me"? (You know that they know you've checked their location.)

*

1: Not comfortable at all	2	3	4	5	6	7: Very comfortable
○	○	○	○	○	○	○

25.

How likely were you to leave your Locaccino Locator running after being able to check "Who's Viewed Me"?

*

1: Very unlikely	2	3	4: No Impact	5	6	7: Very likely
○	○	○	○	○	○	○

26. Would you prefer a closed system where no one can see who has viewed them, or an open system where all users can see who has viewed them?

*

○ Closed system (no "Who's viewed me")

○ Open system (with "Who's viewed me")

27. Please provide us with any feedback you have about the "Who's Viewed Me" feature.

6. Technology

Copy page • Delete page •

28. Please select whether you agree or disagree with the following statements: *

	1: Strongly disagree	2	3	4	5	6	7: Strongly agreely
New technology renders everyday life easier.	○	○	○	○	○	○	○
Humans are overrun by new technology.	○	○	○	○	○	○	○
New technology represents positive progress for human kind.	○	○	○	○	○	○	○
I would feel helplessly exposed when using a location-finding application.	○	○	○	○	○	○	○
No matter what I do, I will not be able to control the sharing of my location.	○	○	○	○	○	○	○
Nothing can protect me from being located (in general).	○	○	○	○	○	○	○
I perceive that I have no influence over who views my location in Locaccino.	○	○	○	○	○	○	○

29. Please let us know about any improvements you'd like us to make to Locaccino.

7. Thank you!

Copy page • Delete page •

Thanks for completing the survey!

Thanks again for participating in this study. If you would like to continue using Locaccino, feel free to do so. We will continue to collect the same usage data that we have been collecting throughout the study, using it for research purposes only.

If you would like to uninstall the Locaccino software, simply remove the program. (Windows: Add/remove programs, Mac: Delete the Locaccino folder in Applications)

You will receive a $20 Amazon.com gift certificate via email in the next few days in appreciation of your participation.

'Thank You'/Redirect Page

A.2 Online Consumer Privacy Study Materials

A.2.1 Online Privacy Concerns Survey

(Quals Concerns) Online Privacy Survey

1. Concerns

*** 1. Have you made at least one purchase online in the past year?**

○ Yes

○ No

(Quals Concerns) Online Privacy Survey

2.

You have qualified for this survey. 39 questions remain. The winner of the 2 GB iPod nano will be notified via email one week after the close of this survey.

*** 2. Do you have any privacy concerns when you are using the Internet, in general?**

○ Yes

○ No

3. If so, what are they?

*** 4. Do you have any privacy concerns when you are shopping online?**

○ Yes

○ No

5. If so, what are they?

*** 6. Please rate the following statements.**

	Strongly Disagree: 0	1	2	3	4	5	Strongly Agree: 6
I feel safe giving my personal information to online stores.	○	○	○	○	○	○	○
Providing online stores with personal information involves too many unexpected problems.	○	○	○	○	○	○	○

*** 7. How much time do you spend on the Internet per week?**

○ Less than 1 hour

○ 1 to 5 hour

○ 6 to 10 hours

○ 11 to 20 hours

○ 21 to 30 hours

○ More than 31 hours

*** 8. How many online purchases did you make in the last 30 days?**

○ None

○ 1

○ 2 or 3

○ 4 or 5

○ 6 or more

3.

*** 9. What was your last online purchase?**

*** 10. From what online store was your last online purchase made?**

*** 11. Did you look at the privacy policy of that store?**

○ Yes

○ No

*** 12. How much of the privacy policy did you read?**

○ I did not click on it

○ I just clicked the link to make sure they had a privacy policy

○ I skimmed it

○ The first paragraph

○ Half of it

○ The whole thing

*** 13. Please answer the following questions.**

	Never: 0	1	2	3	4	5	Always: 6
Do you generally notice whether or not a website you are visiting has a privacy policy?	○	○	○	○	○	○	○
How often do you read websites' privacy policies?	○	○	○	○	○	○	○

*** 14. When was the last time you checked to see if a website had a privacy policy?**

○ In the last 24 hours

○ In the last week

○ In the last month

○ In the last 6 months

○ In the past year

○ Over a year ago

*** 15. How much of the privacy policy did you read?**

○ I did not click on it

○ I just clicked the link to make sure they had a privacy policy

○ I skimmed it

○ The first paragraph

○ Half of it

○ The whole thing

*** 16. What information do you look for in the privacy policies you read?**

*** 17. How bad is it if an online company you buy from doesn't have a privacy policy?**

	Not bad - 0	1	2	3	4	5	6	7	8	9	Extremely Bad - 10
Privacy Policy	○	○	○	○	○	○	○	○	○	○	○

---

4. Series

You are now about halfway through the survey.

We'd like to ask you about a series of privacy issues that one might encounter when using the Internet. Think back to your last online purchase. Answer these questions considering that purchase and that online store. For each one, please tell us how likely you think it is to occur and how much trouble it would cause you if it happened.

*** 18. If your credit card number were stolen after you made an online purchase...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

*** 19. If you received unwanted emails after you made a purchase...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

*** 20. If you continue to receive email from an online store even after you've asked them to take you off their mailing list...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **21. If an online store sold your name and contact information to other companies after you made an online purchase...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **22. If an online store keeps track of all the items you click on at their website...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **23. If an online store inferred information about your habits or interests after you made a purchase...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **24. If your search engine history was made public...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **25. If your purchase history from multiple online stores was combined with other personal information to produce a detailed profile about you...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **26. If your family members or friends accessed your online purchase records without your permission...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

* **27. If current, perspective, or future employer learned about your online purchase history...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

*** 28. If your purchase history from an online store was made available during a lawsuit you are involved in...**

	Not likely / No trouble at all: 0	1	2	3	4	5	6	7	8	9	Extremely likely / A large amount of trouble: 10
How likely is this?	○	○	○	○	○	○	○	○	○	○	○
How much trouble would it cause you?	○	○	○	○	○	○	○	○	○	○	○

---

5. Public Info

Only 12 more questions to go!

*** 29. How much trouble would it cause you if the following information was publicly available on the Internet?**

	No trouble at all - 0	1	2	3	4	5	6	7	8	9	A large amount of trouble - 10
Age	○	○	○	○	○	○	○	○	○	○	○
Bank account balance	○	○	○	○	○	○	○	○	○	○	○
Business address	○	○	○	○	○	○	○	○	○	○	○
Cell phone number	○	○	○	○	○	○	○	○	○	○	○
Credit card number	○	○	○	○	○	○	○	○	○	○	○
Debt report (bills, loans)	○	○	○	○	○	○	○	○	○	○	○
Employment history	○	○	○	○	○	○	○	○	○	○	○
Favorite snack food	○	○	○	○	○	○	○	○	○	○	○
Favorite television show	○	○	○	○	○	○	○	○	○	○	○
Grocery store purchase history	○	○	○	○	○	○	○	○	○	○	○
Height	○	○	○	○	○	○	○	○	○	○	○
Home address	○	○	○	○	○	○	○	○	○	○	○
Medical information	○	○	○	○	○	○	○	○	○	○	○
Name	○	○	○	○	○	○	○	○	○	○	○
Online purcahse history	○	○	○	○	○	○	○	○	○	○	○
Salary	○	○	○	○	○	○	○	○	○	○	○
Search terms in Google, Yahoo!, etc.	○	○	○	○	○	○	○	○	○	○	○
Social Security Number	○	○	○	○	○	○	○	○	○	○	○
Tax return	○	○	○	○	○	○	○	○	○	○	○
Weight	○	○	○	○	○	○	○	○	○	○	○

6. Westin

* 30. To what extent do you agree or disagree with the following statements?

	Strongly Disagree: 0	1	2	3	4	5	Strongly Agree: 6
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way	○	○	○	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.	○	○	○	○	○	○	○

* 31. Please answer the following question.

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
How concerned are you about threats to your personal privacy online in America today?	○	○	○	○	○	○	○

7. Items

You are on the next to last page of the survey.

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.

* 32. 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?

	Would not purchase	Puchase, very concerned	Purchase, somewhat concerned	Purchase, no concerns
Adult Diapers	○	○	○	○
Book on bankruptcy	○	○	○	○
Book on bomb-making	○	○	○	○
Book on depression	○	○	○	○
Bulletproof jacket	○	○	○	○
Bullets	○	○	○	○
Large bottle of Peroxide	○	○	○	○
Cigarettes	○	○	○	○
Condoms	○	○	○	○
Fertilizer	○	○	○	○
Flowers	○	○	○	○
HIV test	○	○	○	○
Hunting knife	○	○	○	○
Laptop computer	○	○	○	○
Lingerie	○	○	○	○
Office supplies	○	○	○	○
Personal lubricant	○	○	○	○
Pregnancy test	○	○	○	○
Porn DVD	○	○	○	○
Sex toy	○	○	○	○
Sexually Transmitted Disease medication	○	○	○	○
Shoes	○	○	○	○
Textbooks	○	○	○	○

*** 33. What types of concerns would you have with making these purchases?**

*** 34. Please rate the following statements.**

	Strongly Disagree: 0	1	2	3	4	5	Strongly Agree: 6
I generally trust online companies with handling my personal information and my purchase history.	○	○	○	○	○	○	○
In general, I find it risky to shop at an online store.	○	○	○	○	○	○	○

---

8. Demographics

*** 35. What is your age?**

*** 36. What is your gender?**

○ Female

○ Male

*** 37. What is your highest level of education?**

○ Some high school

○ High school diploma

○ College degree

○ Graduate degree

○ Professional degree (including trade school)

38. How would you describe your race and ethnicity?

☐ White

☐ Black

☐ Asian or Pacific Islander

☐ Latino(a)/Hispanic

☐ Native American

☐ Other (please specify)

39. If you have any additional comments about online shopping and privacy, please write them below.

40. What is your email address? This information will only be used to notify you if you have been drawn to win the iPod.

A.2.2 Privacy Information Purchasing Study

Privacy Information Purchasing Study Search Results

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

Non-Privacy Sensitive Item

Duracell AA Batteries – 8 Pack

Session 1		Privacy Information		Session 2	
Price with Shipping	**Difference**	**Privacy Level**	**Privacy Icon**	**Price with Shipping**	**Difference**
$14.60	$0.00	N/A		$14.45	$0.00
$14.96	$0.36	Low	☐☐☐☐	$14.60	$0.15
$15.07	$0.11	Med	🟩🟩☐☐	$14.80	$0.20
$15.14	$0.07	High	🟩🟩🟩🟩	$15.14	$0.34
$15.85	$0.71	N/A		$15.85	$0.71
$15.98	$0.13	N/A	☐☐☐☐	$15.98	$0.13
$14.60	$0.44	Low	🟩🟩🟩🟩	$16.42	$0.44
$14.96	$0.43	High		$16.85	$0.43

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

Privacy-Sensitive Item

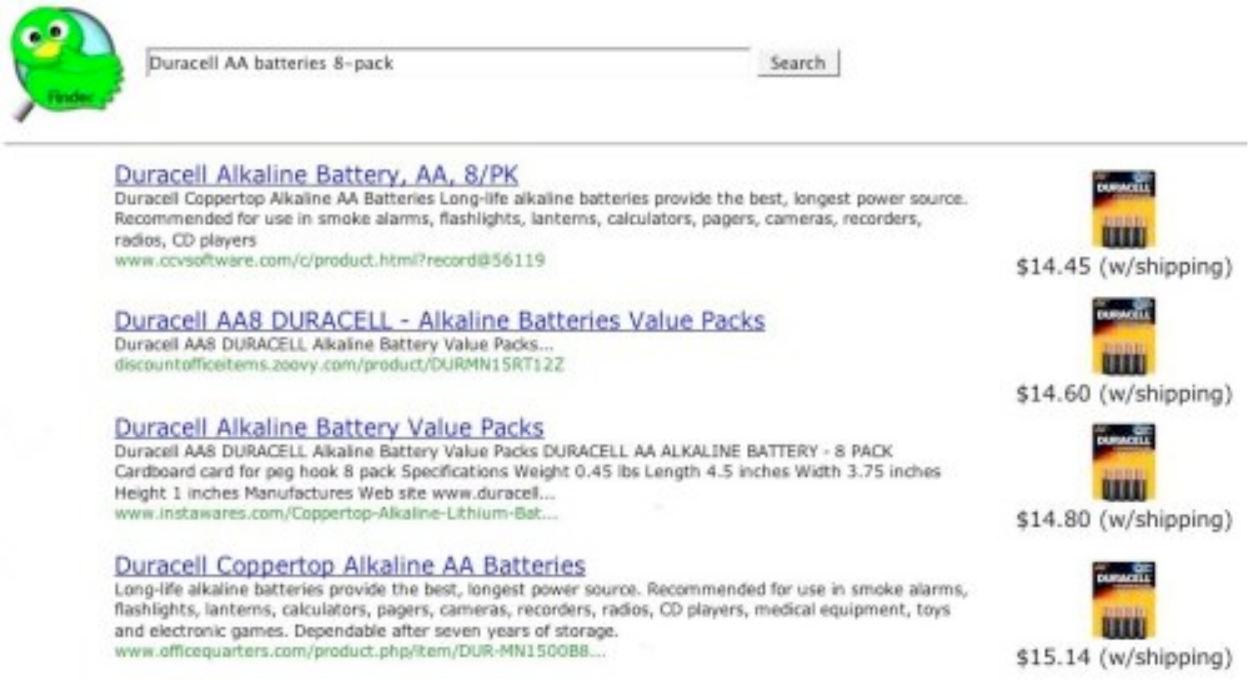
Pocket Rocket Jr.

Session 1		Privacy Information		Session 2	
Price with Shipping	**Difference**	**Privacy Level**	**Privacy Icon**	**Price with Shipping**	**Difference**
$15.08	$0.00	N/A		$15.36	$0.00
$15.74	$0.66	Low	☐☐☐☐	$15.74	$0.38
$15.90	$0.16	Med	🟩🟩☐☐	$15.90	$0.16
$16.54	$0.64	High	🟩🟩🟩🟩	$16.54	$0.64
$16.79	$0.25	N/A		$16.79	$0.25
$16.79	$0.89	N/A		$16.79	$0.89
$17.94	$1.15	Low	☐☐☐☐	$17.94	$1.15
$18.95	$2.16	High	🟩🟩🟩🟩	$18.95	$2.16

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

Search Results Interfaces

Condition 1: No Information



Duracell AA batteries 8-pack

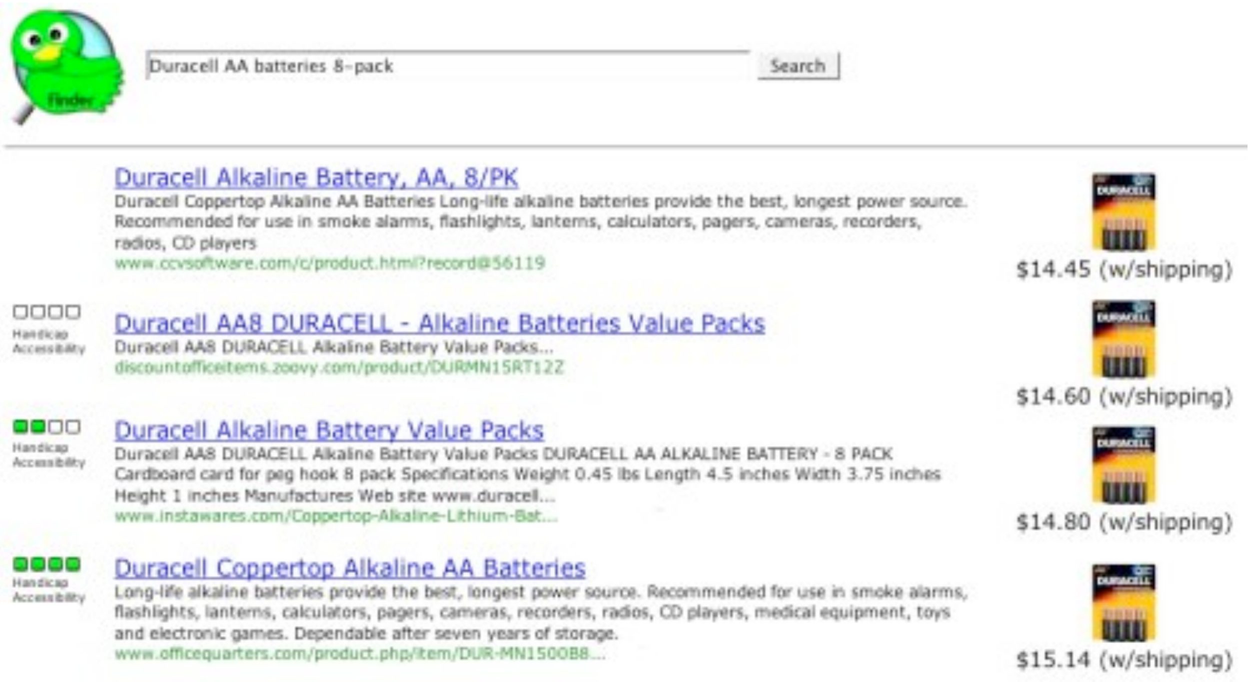
[Duracell Alkaline Battery, AA, 8/PK]
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.html?record@56119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

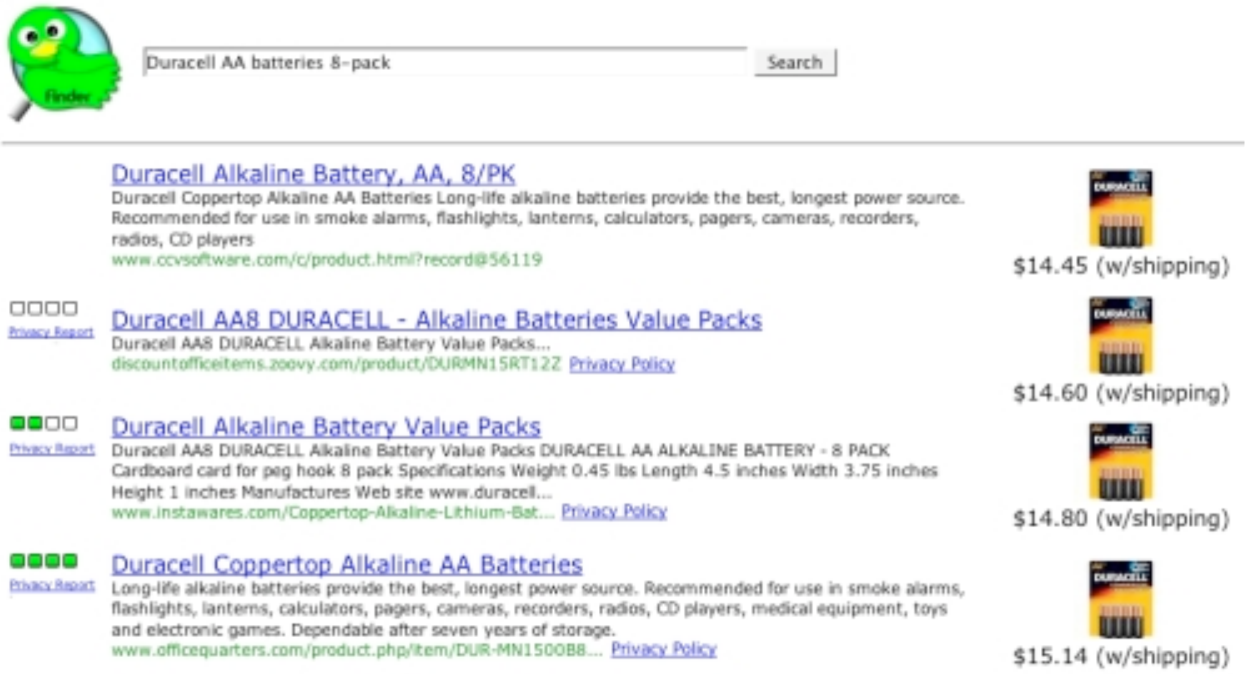
[Duracell Alkaline Battery, AA, 8/PK]
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.html?record@56119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



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)

☐☐☐☐ Privacy Report
Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovy.com/product/DURMN15RT12Z Privacy Policy
$14.60 (w/shipping)

🟩🟩☐☐ Privacy Report
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... Privacy Policy
$14.80 (w/shipping)

🟩🟩🟩🟩 Privacy Report
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... Privacy Policy
$15.14 (w/shipping)

Privacy Information Purchasing Study Screening Survey

Quals - Online Shopping Screening Survey

1. Intro

Thank you for your interest! This Carnegie Mellon University research study on online searching and shopping will give you $45 to shop online for products we specify for you to purchase with your own credit card. You are welcome to keep the change ($10 or more) as well as the products purchased.

You will receive the initial $10 payment on the day of the study and the additional $35 payment after the products you purchased have been shipped.

*** 1. Are you still interested in participating in this study?**

○ Yes

○ No

Quals - Online Shopping Screening Survey

2. Contact Information

*** 2. What is your name?**

*** 3. What is your email address?**

*** 4. What is your phone number?**

*** 5. Gender:**

○ Female

○ Male

*** 6. What is your age?**

7. What is your occupation?

3. Questions

You are about halfway done with the survey.

Please answer the following questions:

8. Indicate your level of experience with the following online procedures:

	No Experience	Minimal Experience	Some Experience	Very Experienced
Using Online Search Engines	○	○	○	○
Shopping Online	○	○	○	○
Using Instant Messenger Systems	○	○	○	○
Checking Email	○	○	○	○
Banking Online	○	○	○	○

*** 9. Have you puchased something online in the past year?**

- ○ Yes
- ○ No

10. Which web browser do you use most frequently (please select ONE)?

- ○ Internet Explorer
- ○ Netscape
- ○ Firefox
- ○ Safari
- ○ Opera
- ○ Don't Know
- ○ Other (please specify)

11. Do you have an online store/vendor that you often visit or purchase from?

- ○ Yes
- ○ No

12. If yes, what store(s) or vendor(s)?

*** 13. When you are selecting a website to purchase an item from, how much do the following factors effect your choice?**

	Not at all: 0	1	2	3	4	5	A great deal: 6
Accessibility for sight-impaired users	○	○	○	○	○	○	○
Compatibility of web site with mobile phone web browsers	○	○	○	○	○	○	○
Customer Reviews	○	○	○	○	○	○	○
Customer Service	○	○	○	○	○	○	○
Location of Physical Store	○	○	○	○	○	○	○
Page load speed	○	○	○	○	○	○	○
Popularity	○	○	○	○	○	○	○
Price	○	○	○	○	○	○	○
Privacy Policy	○	○	○	○	○	○	○
Return Policy	○	○	○	○	○	○	○
Software Compatibility	○	○	○	○	○	○	○
Shipping Speed	○	○	○	○	○	○	○
Website Design	○	○	○	○	○	○	○

4. Privacy Concerns

This is the last page of questions for the survey.

* 14. Please rate your level of concern about the following:

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
A web site uses your health information to determine website content or ads	○	○	○	○	○	○	○
A web site shares your health information with other companies	○	○	○	○	○	○	○
A website contacts you about other services or products via telephone	○	○	○	○	○	○	○
A website contacts you about other services or products via email or postal mail	○	○	○	○	○	○	○
A website does not allow you to be removed from marketing/mailing lists	○	○	○	○	○	○	○
A website uses your financial information to determine website content or ads	○	○	○	○	○	○	○
A website shares your financial information with other companies	○	○	○	○	○	○	○
A website does not allow you to find out what information it stores about you	○	○	○	○	○	○	○
A website makes its privacy policy available	○	○	○	○	○	○	○
A website uses personally identifying information to determine your habits, interests, or other characteristics	○	○	○	○	○	○	○
A website shares personally identifying information with other companies	○	○	○	○	○	○	○
A website uses information that does not personally identify you to determine your habits, interests, or other characteristics	○	○	○	○	○	○	○
A website shares information that does not personally identify you with other companies	○	○	○	○	○	○	○

* 15. Please rate the following statements.

	Strongly Disagree: 0	1	2	3	4	5	Strongly Agree: 6
I feel safe giving my personal information to online stores.	○	○	○	○	○	○	○
Providing online stores with personal information involves too many unexpected problems.	○	○	○	○	○	○	○
I generally trust online companies with handling my personal information and my purchase history.	○	○	○	○	○	○	○

* 16. Please answer the following question.

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
How concerned are you about threats to your personal privacy online in America today?	○	○	○	○	○	○	○

You have now completed the survey. You may be contacted in the next two weeks to be scheduled for the user study.

Privacy Information Purchasing Study Exit Survey (Indicator Conditions)

CMU Searching and Shopping Study Exit Survey (2)

1. Online Shopping Habits

* 1. How much time do you spend on the Internet per week?

○ 1 to 5 hours

○ 6 to 10 hours

○ 11 to 20 hours

○ 21 to 30 hours

○ More than 31 hours

* 2. How many online purchases did you make in the last 30 days?

○ None

○ 1

○ 2 or 3

○ 4 or 5

○ 6 or more

* 3. How much time do you typically spend in an online shopping session when making a purchase?

○ Less than 10 minutes

○ 11 to 29 minutes

○ 30 to 59 minutes

○ 1 to 2 hours

○ More than 2 hours

CMU Searching and Shopping Study Exit Survey (2)

2. Search Engine Specific

* 4. Do you currently use any Internet search engines?

○ Yes

○ No

○ If yes, which one(s)?

* 5. Do you currently use any shopping search engines?

○ Yes

○ No

○ If yes, which one(s)?

* 6. How easy was it to find the following information?

	Very Difficult: 0	1	2	3	4	5	Very Easy: 6
The number of Carnegie libraries	○	○	○	○	○	○	○
The color of Ugg boots for women	○	○	○	○	○	○	○
The price of Ugg boots	○	○	○	○	○	○	○
Where to recycle computers in Pittsburgh	○	○	○	○	○	○	○

3. Product Specific Questions

* 7. Before this study, had you ever purchased batteries online?

○ Yes

○ No

* 8. Was this the first time you made a purchase from the website where you purchased the batteries?

○ Yes

○ No

* 9. How much did the following factors influence your decision to purchase the batteries from that website?

	No Influence at all: 0	1	2	3	4	5	Strongly Influence: 6
The base price of the product	○	○	○	○	○	○	○
The total price of the product (including shipping and taxes)	○	○	○	○	○	○	○
The website design or appearance	○	○	○	○	○	○	○
Prior experience with the website	○	○	○	○	○	○	○
Prior experience with the company (not online)	○	○	○	○	○	○	○
The privacy policy	○	○	○	○	○	○	○
The return policy	○	○	○	○	○	○	○
Other factors (please describe below)	○	○	○	○	○	○	○

10. If there were any other factors, please describe them.

* 11. Which factor had the most influence on your decision?

* 12. Before this study, had you ever purchased sex toys online?

○ Yes

○ No

---

* 13. Was this the first time you made a purchase from the website where you purchased the Pocket Rocket Jr.?

○ Yes

○ No

* 14. How much did the following factors influence your decision to purchase the Pocket Rocket Jr. from that website?

	No Influence at all: 0	1	2	3	4	5	Strongly Influence: 6
The base price of the product	○	○	○	○	○	○	○
The total price of the product (including shipping and taxes)	○	○	○	○	○	○	○
The website design or appearance	○	○	○	○	○	○	○
Prior experience with the website	○	○	○	○	○	○	○
Prior experience with the company (not online)	○	○	○	○	○	○	○
The privacy policy	○	○	○	○	○	○	○
The return policy	○	○	○	○	○	○	○
Other factors (please describe below)	○	○	○	○	○	○	○

15. If there were any other factors, please describe them.

* 16. Which factor had the most influence on your decision?

4. Privacy Preferences

* 17. Please answering the following questions.

	Never: 0	1	2	3	4	5	Always: 6
Do you generally notice whether or not a website you are visiting has a privacy policy?	○	○	○	○	○	○	○
How often do you read websites' privacy policies?	○	○	○	○	○	○	○

* 18. How many privacy policies did you read in the purchasing tasks?

○ None of them

○ 1

○ 2 or 3

○ 4 or more

* 19. How much of the privacy policy did you read?
(Check all that apply)

☐ None

☐ I just clicked the link to make sure there was a privacy policy

☐ I skimmed it

☐ The first paragraph

☐ Half of it

☐ The whole thing

20. For the policies you read, why did you read them?

21. For the policies you didn't read, why didn't you read them?

* 22. Did you notice the green boxes next to some of the URLs?

○ Yes

○ No

* 23. What did you think the presence of green boxes meant?

* 24. What did you think the absence of green boxes meant?

* 25. Did the green boxes influence your decision to visit or not visit a web site?

☐ Yes

☐ No

☐ Why or why not?

* 26. Did the green boxes influence your decision to purchase from a particular web site?

☐ Yes

☐ No

☐ Why or why not?

5. Product Privacy Questions

* 27. What was your level of concern for your privacy when you were purchasing the products in this study?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
AA Batteries	○	○	○	○	○	○	○
Sex Toy	○	○	○	○	○	○	○

* 28. When purchasing the batteries, how concerned were you about what the company would do with the following information?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
Credit Card Number	○	○	○	○	○	○	○
Email Address	○	○	○	○	○	○	○
Physical Address	○	○	○	○	○	○	○
Phone Number	○	○	○	○	○	○	○
Purchase History	○	○	○	○	○	○	○

* 29. What specific privacy concerns, if any, did you have when purchasing the batteries?

* 30. When purchasing the sex toy, how concerned were you about what the company would do with the following information?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
Credit Card Number	○	○	○	○	○	○	○
Email Address	○	○	○	○	○	○	○
Physical Address	○	○	○	○	○	○	○
Phone Number	○	○	○	○	○	○	○
Purchase History	○	○	○	○	○	○	○

* 31. What specific privacy concerns, if any, did you have when purchasing the sex toy?

* 32. Did you have more concerns with purchasing one product or the other product?

○ More concerns when purchasing the AA batteries

○ More concerns when purchasing the Pocket Rocket Jr.

○ Equal privacy concerns when purchasing both products

○ No privacy concerns purchasing either product

* 33. To what extent do you agree or disagree with the following statements?

	Strongly Disagree:0	1	2	3	4	5	Strongly Agree: 6
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way	○	○	○	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today	○	○	○	○	○	○	○

* 34. Have you ever found fraudulent transactions on your account statement?

○ Yes

○ No

* 35. Have you ever had your social security number stolen?

○ Yes

○ No

* 36. Have you ever been notified that your personal information has been stolen or compromised?

○ Yes

○ No

CMU Searching and Shopping Study Exit Survey (2)

6. Demographics

* 37. What is your age?

* 38. What is your gender?

- ○ Female
- ○ Male

* 39. What is your highest level of education?

- ○ Some high school
- ○ High school diploma
- ○ College degree
- ○ Graduate Degree
- ○ Professional degree (including trade school)
- ○ Other (please specify)

40. How would you describe your race and ethnicity?

- ☐ White
- ☐ Black
- ☐ Asian or Pacific Islander
- ☐ Latino(a)/Hispanic
- ☐ Native American
- ☐ Other (please specify)

41. What is your country of origin?

CMU Searching and Shopping Study Exit Survey (2)

7. Privacy Report (Batteries)

Ask the survey administrator for information about your purchases. Please read that information and answer the following questions.

* 42. If you had read this privacy report, would reading it have changed your decision about which site you picked to purchase the batteries?

- ○ Yes
- ○ No

* 43. Do you feel that this website adequately protects your privacy?

- ○ Yes
- ○ No

CMU Searching and Shopping Study Exit Survey (2)

8. Privacy Report (Vibrator)

Ask the survey administrator for information about your purchases. Please read that information and answer the following questions.

* 44. If you had read this privacy report, would reading it have changed your decision about which site you picked to purchase the vibrator?

○ Yes

○ No

* 45. Do you feel that this website adequately protects your privacy?

○ Yes

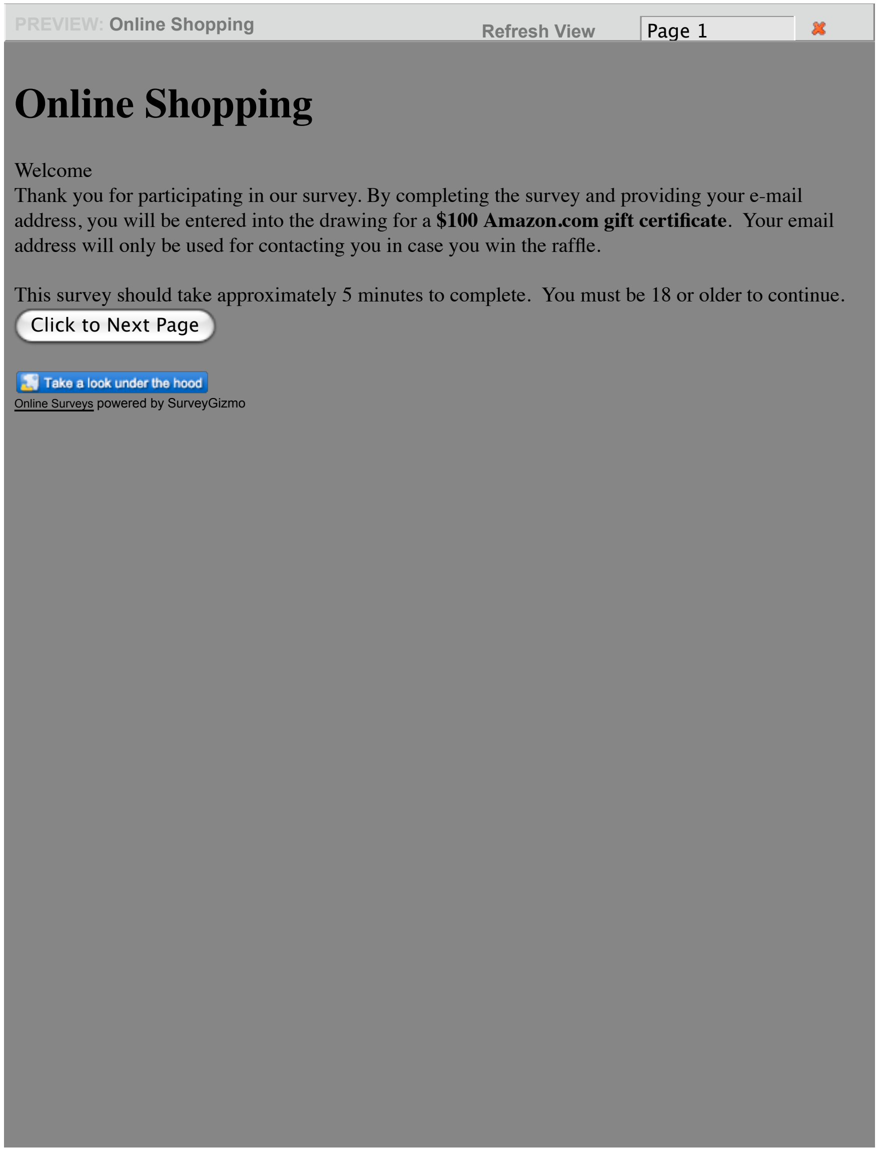
○ No

46. If you have any additional comments about online shopping and privacy, please write them below.

☐

Thank you for completing this questionnaire! Please raise your hand to notify the study administrator and receive your $10 payment. We will send the remainder of your payment ($35) to you after we confirm that the products you ordered have shipped. The study administrator will provide you with instructions for notifying us that your orders have shipped.

A.2.3 Privacy Premium Survey

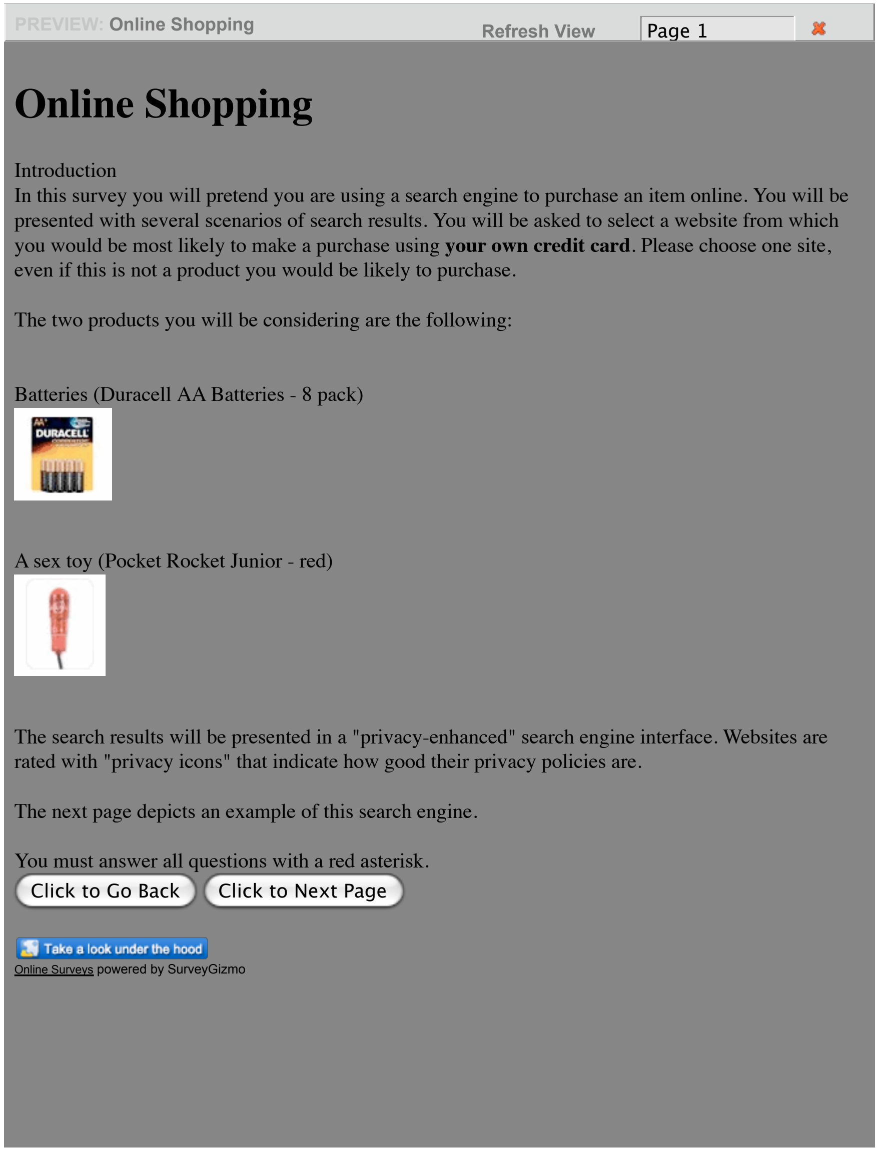

PREVIEW: Online Shopping
Refresh View
Page 1
Click to Next Page
Take a look under the hood
Online Surveys powered by SurveyGizmo

Online Shopping

Welcome

Thank you for participating in our survey. By completing the survey and providing your e-mail address, you will be entered into the drawing for a **$100 Amazon.com gift certificate**. Your email address will only be used for contacting you in case you win the raffle.

This survey should take approximately 5 minutes to complete. You must be 18 or older to continue.



Online Shopping

Introduction

In this survey you will pretend you are using a search engine to purchase an item online. You will be presented with several scenarios of search results. You will be asked to select a website from which you would be most likely to make a purchase using **your own credit card**. Please choose one site, even if this is not a product you would be likely to purchase.

The two products you will be considering are the following:

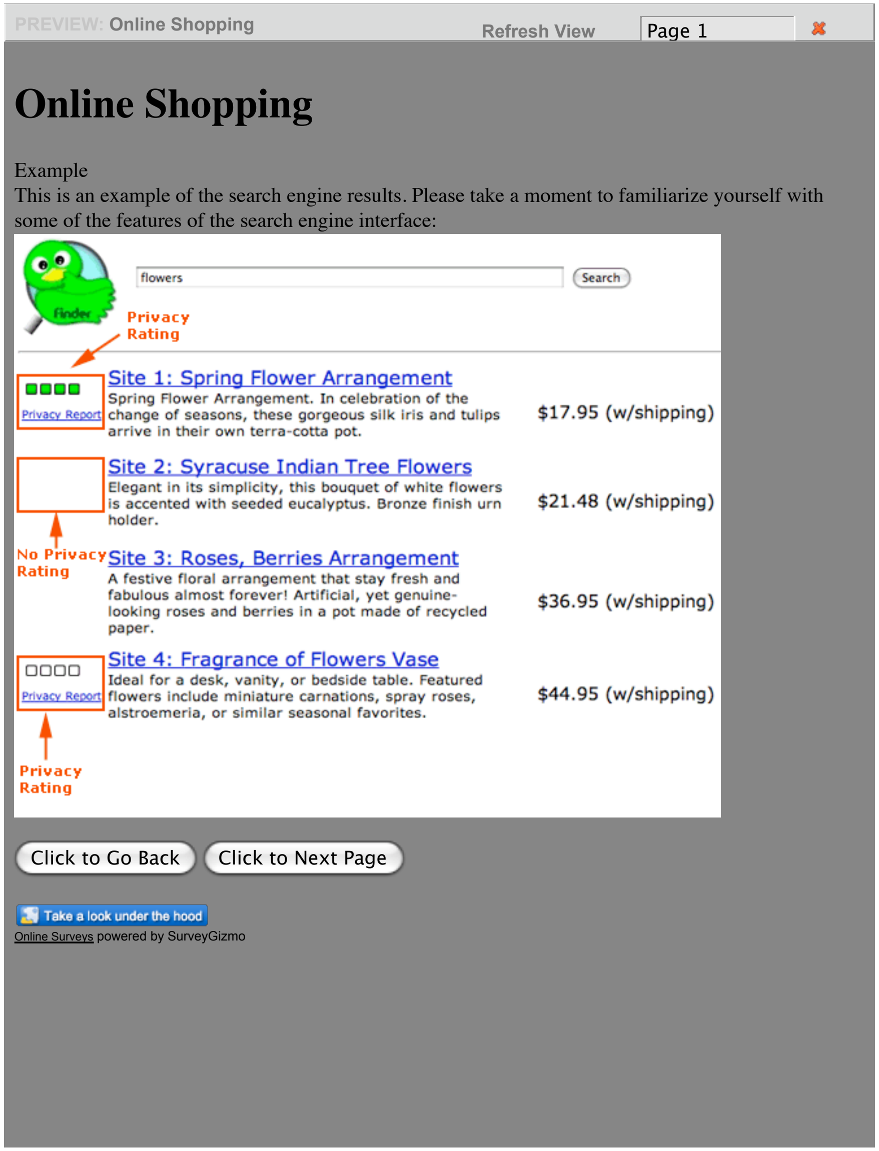
Batteries (Duracell AA Batteries - 8 pack)

A sex toy (Pocket Rocket Junior - red)

The search results will be presented in a "privacy-enhanced" search engine interface. Websites are rated with "privacy icons" that indicate how good their privacy policies are.

The next page depicts an example of this search engine.

You must answer all questions with a red asterisk.



Online Shopping

Example
This is an example of the search engine results. Please take a moment to familiarize yourself with some of the features of the search engine interface:

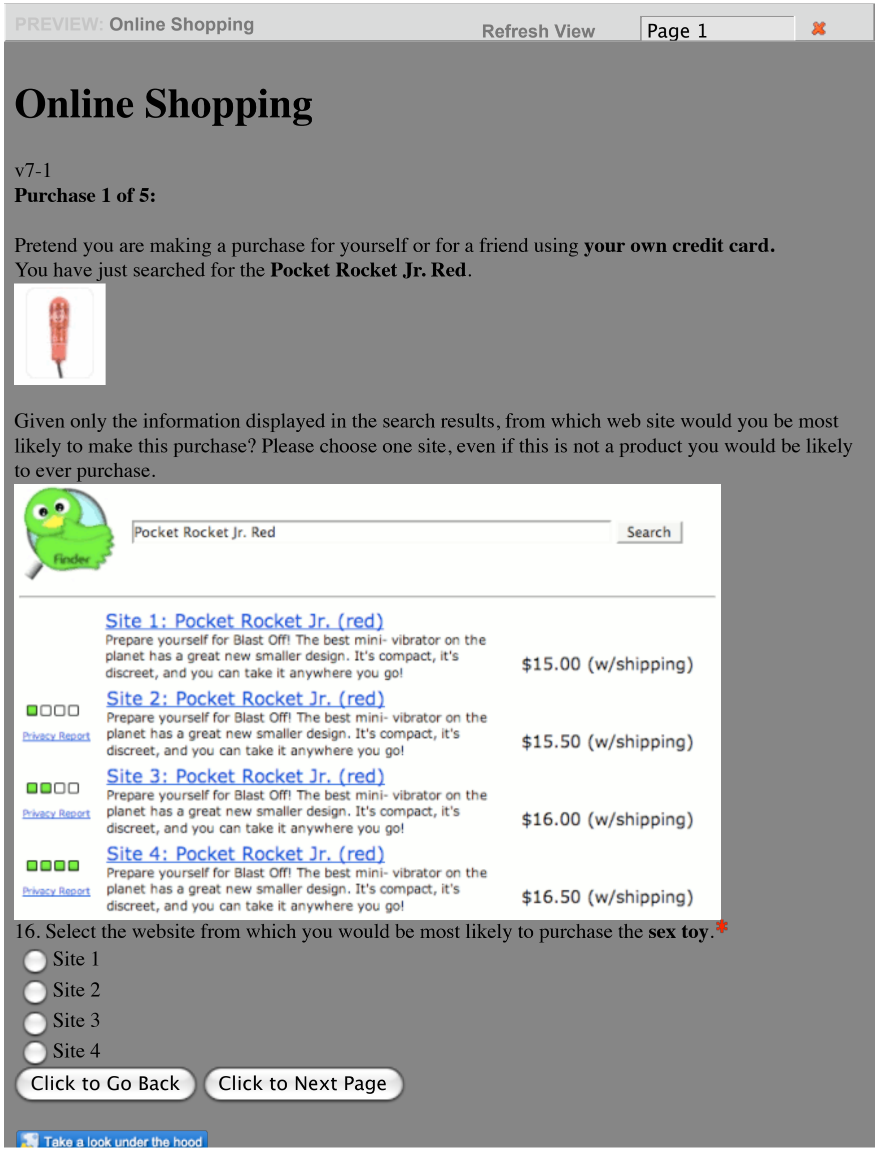
🟩🟩🟩🟩 Privacy Report
Site 1: Spring Flower Arrangement
Spring Flower Arrangement. In celebration of the change of seasons, these gorgeous silk iris and tulips arrive in their own terra-cotta pot.
$17.95 (w/shipping)

Site 2: Syracuse Indian Tree Flowers
Elegant in its simplicity, this bouquet of white flowers is accented with seeded eucalyptus. Bronze finish urn holder.
$21.48 (w/shipping)

Site 3: Roses, Berries Arrangement
A festive floral arrangement that stay fresh and fabulous almost forever! Artificial, yet genuine-looking roses and berries in a pot made of recycled paper.
$36.95 (w/shipping)

☐☐☐☐ Privacy Report
Site 4: Fragrance of Flowers Vase
Ideal for a desk, vanity, or bedside table. Featured flowers include miniature carnations, spray roses, alstroemeria, or similar seasonal favorites.
$44.95 (w/shipping)

Online Surveys powered by SurveyGizmo



Online Shopping

v7-1
Purchase 1 of 5:

Pretend you are making a purchase for yourself or for a friend using **your own credit card.**
You have just searched for the **Pocket Rocket Jr. Red**.

Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.

Site 1: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.00 (w/shipping)

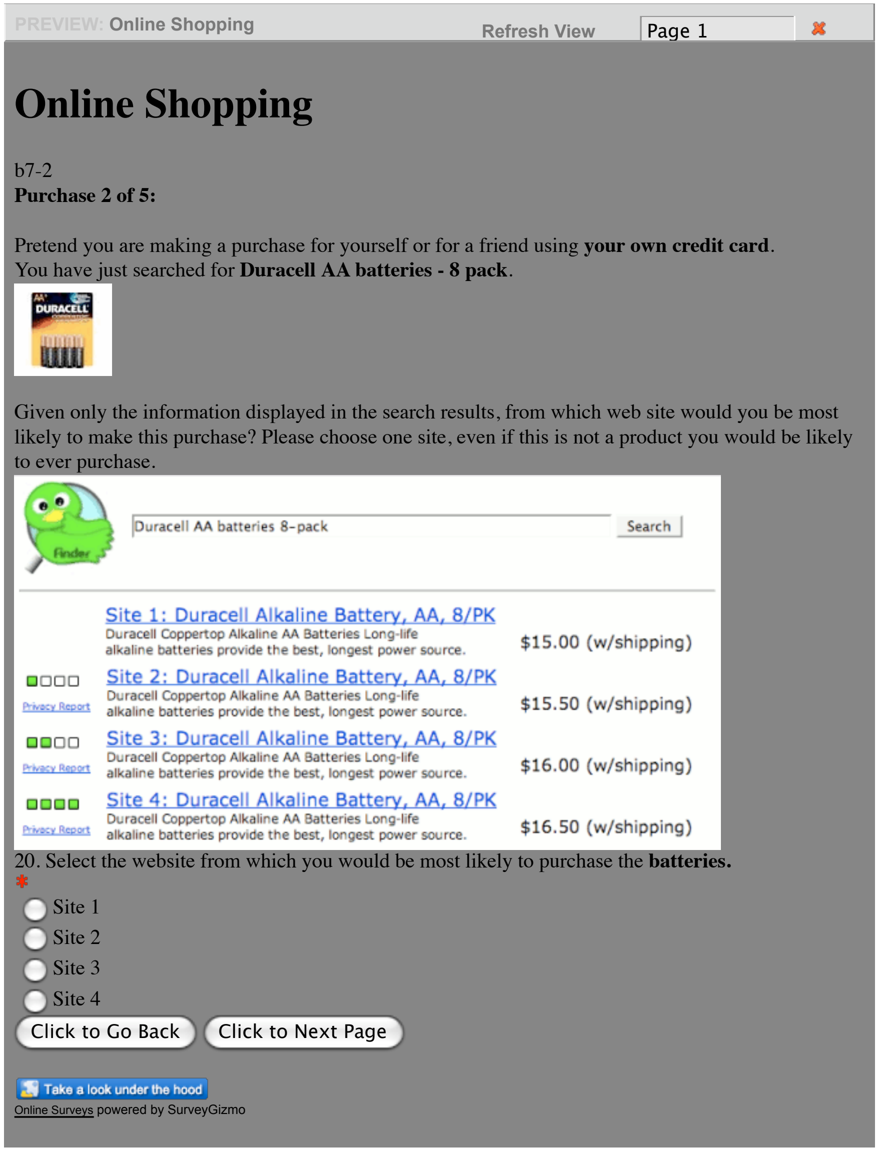
🟩☐☐☐ Privacy Report
Site 2: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.50 (w/shipping)

🟩🟩☐☐ Privacy Report
Site 3: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$16.00 (w/shipping)

🟩🟩🟩🟩 Privacy Report
Site 4: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$16.50 (w/shipping)

16. Select the website from which you would be most likely to purchase the **sex toy**.*

○ Site 1
○ Site 2
○ Site 3
○ Site 4



Online Shopping

b7-2

Purchase 2 of 5:

Pretend you are making a purchase for yourself or for a friend using **your own credit card**. You have just searched for **Duracell AA batteries - 8 pack**.

Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.

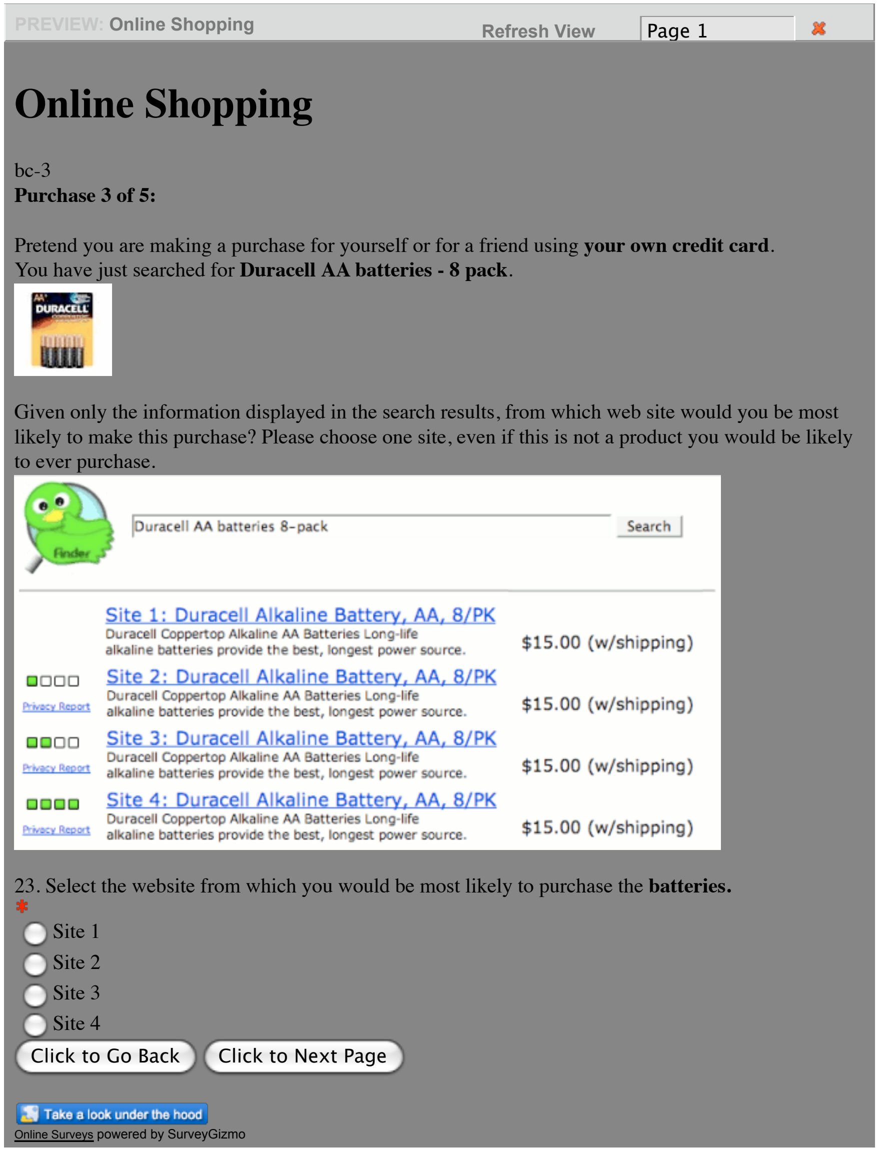
Duracell AA batteries 8-pack

	Site 1: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.00 (w/shipping)
🟩☐☐☐ Privacy Report	Site 2: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.50 (w/shipping)
🟩🟩☐☐ Privacy Report	Site 3: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$16.00 (w/shipping)
🟩🟩🟩🟩 Privacy Report	Site 4: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$16.50 (w/shipping)

20. Select the website from which you would be most likely to purchase the **batteries.**
*

○ Site 1
○ Site 2
○ Site 3
○ Site 4

Online Surveys powered by SurveyGizmo



Online Shopping

bc-3

Purchase 3 of 5:

Pretend you are making a purchase for yourself or for a friend using **your own credit card**. You have just searched for **Duracell AA batteries - 8 pack**.

Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.

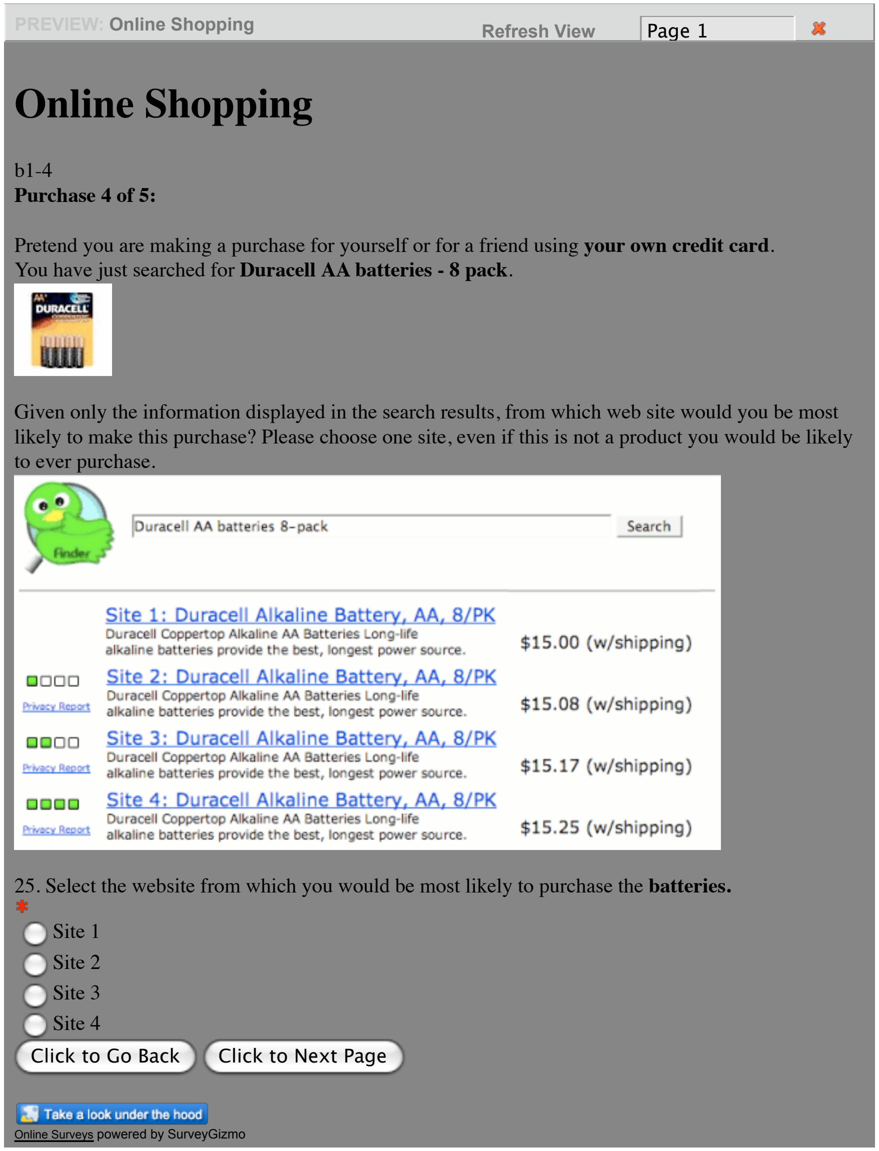
Duracell AA batteries 8-pack

	Site 1: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.00 (w/shipping)
🟩☐☐☐ Privacy Report	Site 2: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.00 (w/shipping)
🟩🟩☐☐ Privacy Report	Site 3: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.00 (w/shipping)
🟩🟩🟩🟩 Privacy Report	Site 4: Duracell Alkaline Battery, AA, 8/PK Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.	$15.00 (w/shipping)

23. Select the website from which you would be most likely to purchase the **batteries.**
*

○ Site 1
○ Site 2
○ Site 3
○ Site 4

Online Surveys powered by SurveyGizmo



Online Shopping

b1-4
Purchase 4 of 5:

Pretend you are making a purchase for yourself or for a friend using **your own credit card**.
You have just searched for **Duracell AA batteries - 8 pack**.

Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.

Site 1: Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.
$15.00 (w/shipping)

🟩⬜⬜⬜ Privacy Report
Site 2: Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.
$15.08 (w/shipping)

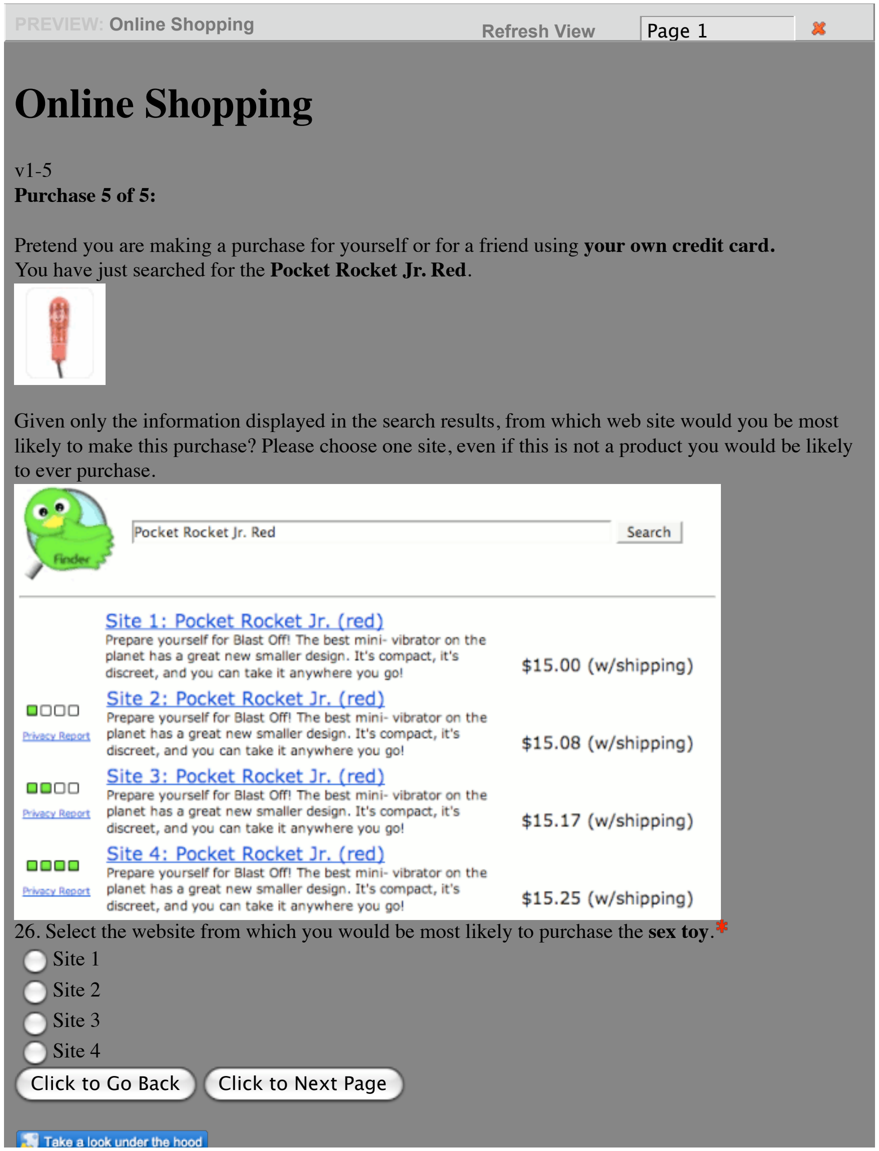
🟩🟩⬜⬜ Privacy Report
Site 3: Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.
$15.17 (w/shipping)

🟩🟩🟩🟩 Privacy Report
Site 4: Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.
$15.25 (w/shipping)

25. Select the website from which you would be most likely to purchase the **batteries.**
*

○ Site 1
○ Site 2
○ Site 3
○ Site 4

Online Surveys powered by SurveyGizmo



Online Shopping

v1-5
Purchase 5 of 5:

Pretend you are making a purchase for yourself or for a friend using **your own credit card.**
You have just searched for the **Pocket Rocket Jr. Red**.

Given only the information displayed in the search results, from which web site would you be most likely to make this purchase? Please choose one site, even if this is not a product you would be likely to ever purchase.

Site 1: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.00 (w/shipping)

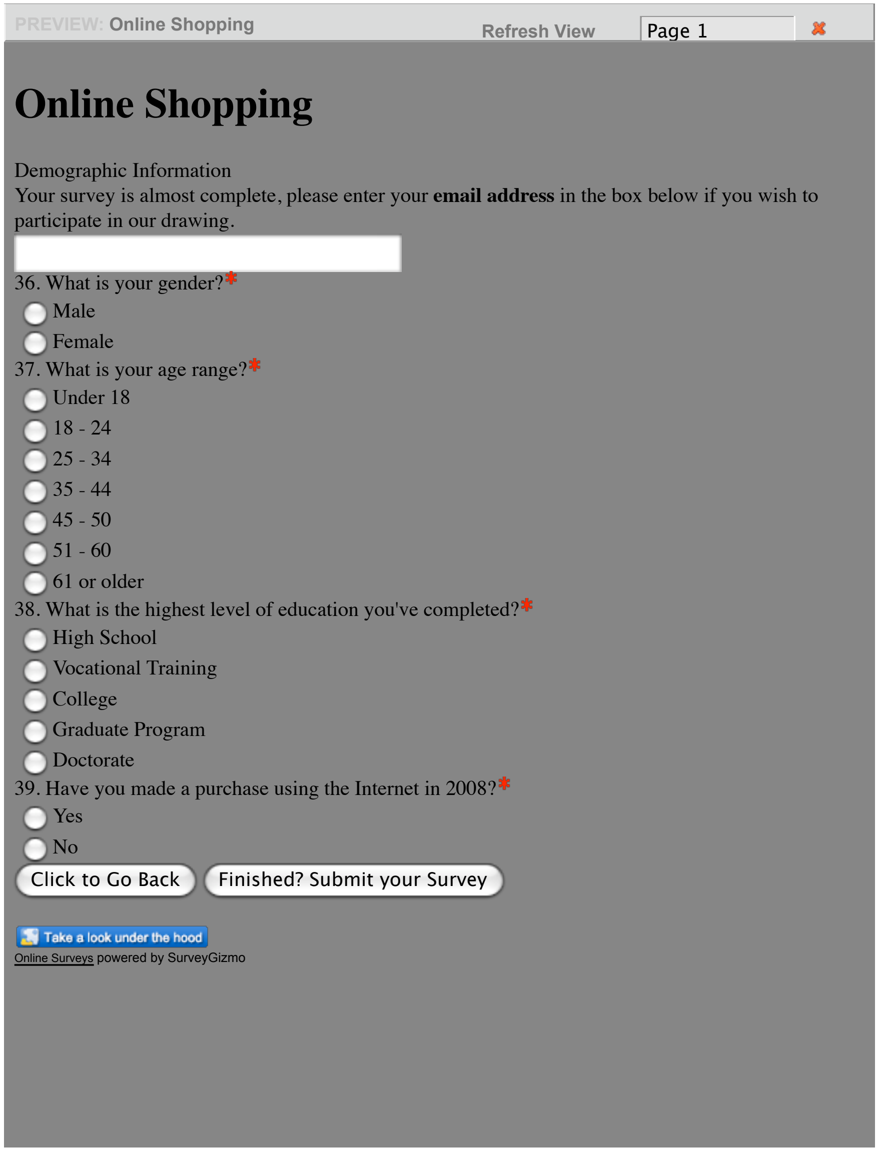
🟩⬜⬜⬜ Privacy Report
Site 2: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.08 (w/shipping)

🟩🟩⬜⬜ Privacy Report
Site 3: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.17 (w/shipping)

🟩🟩🟩🟩 Privacy Report
Site 4: Pocket Rocket Jr. (red)
Prepare yourself for Blast Off! The best mini- vibrator on the planet has a great new smaller design. It's compact, it's discreet, and you can take it anywhere you go!
$15.25 (w/shipping)

26. Select the website from which you would be most likely to purchase the **sex toy**.*

○ Site 1
○ Site 2
○ Site 3
○ Site 4



Online Shopping

Demographic Information
Your survey is almost complete, please enter your **email address** in the box below if you wish to participate in our drawing.

36. What is your gender?*
- ○ Male
- ○ Female

37. What is your age range?*
- ○ Under 18
- ○ 18 - 24
- ○ 25 - 34
- ○ 35 - 44
- ○ 45 - 50
- ○ 51 - 60
- ○ 61 or older

38. What is the highest level of education you've completed?*
- ○ High School
- ○ Vocational Training
- ○ College
- ○ Graduate Program
- ○ Doctorate

39. Have you made a purchase using the Internet in 2008?*
- ○ Yes
- ○ No

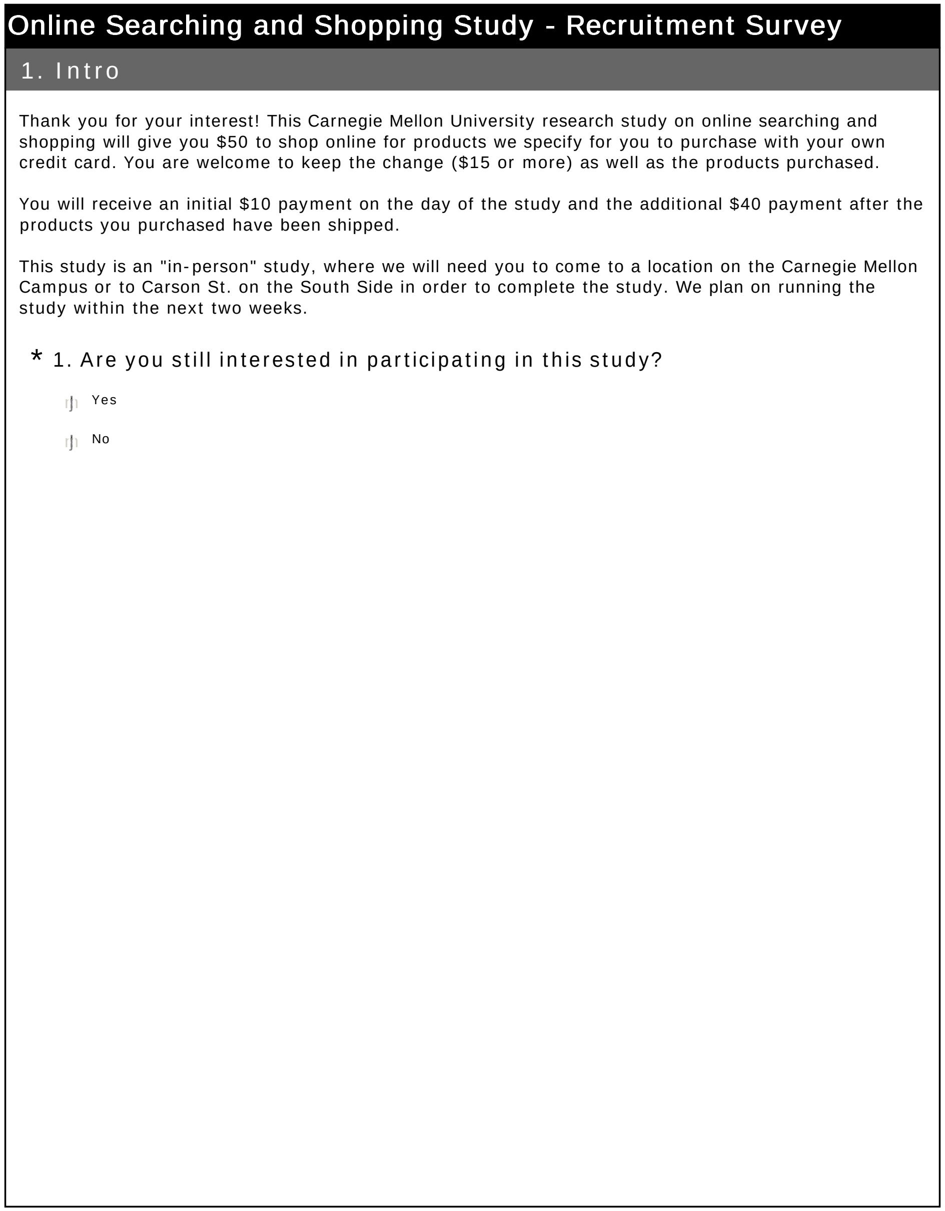
Click to Go Back
Finished? Submit your Survey
Take a look under the hood
Online Surveys powered by SurveyGizmo

A.2.4 Privacy Information Timing Purchasing Study

Privacy Information Timing Purchasing Study

URL	Price	Shipping	Total Price	New Price	New Total	Privacy Level	Privacy Icon
DirtyBunny	$10.00	$9.55	$19.55	$6.18	$15.50	Empty	☐☐☐☐
SheVibe	$8.99	$7.53	$16.52	$7.97	$15.50	1 Box	🟩☐☐☐
Nite Time Toys	$8.99	$4.79	$13.78	$10.71	$15.50	2 Box	🟩🟩☐☐
Eden Fantasy	$9.99	$5.00	$14.99	$10.50	$15.50	High	🟩🟩🟩🟩
Little Office Supply	$7.84	$7.67	$15.51	$7.83	$15.50	Empty	☐☐☐☐
InstaWares	$8.70	$6.95	$15.65	$8.80	$15.75	1 Box	🟩☐☐☐
OfficeQuarters	$7.93	$6.51	$14.44	$9.49	$16.00	2 Box	🟩🟩☐☐
On Time Supplies	$8.35	$7.95	$16.30	$8.30	$16.25	High	🟩🟩🟩🟩

Privacy Information Timing Study Screening Survey



Online Searching and Shopping Study - Recruitment Survey

1. Intro

Thank you for your interest! This Carnegie Mellon University research study on online searching and shopping will give you $50 to shop online for products we specify for you to purchase with your own credit card. You are welcome to keep the change ($15 or more) as well as the products purchased.

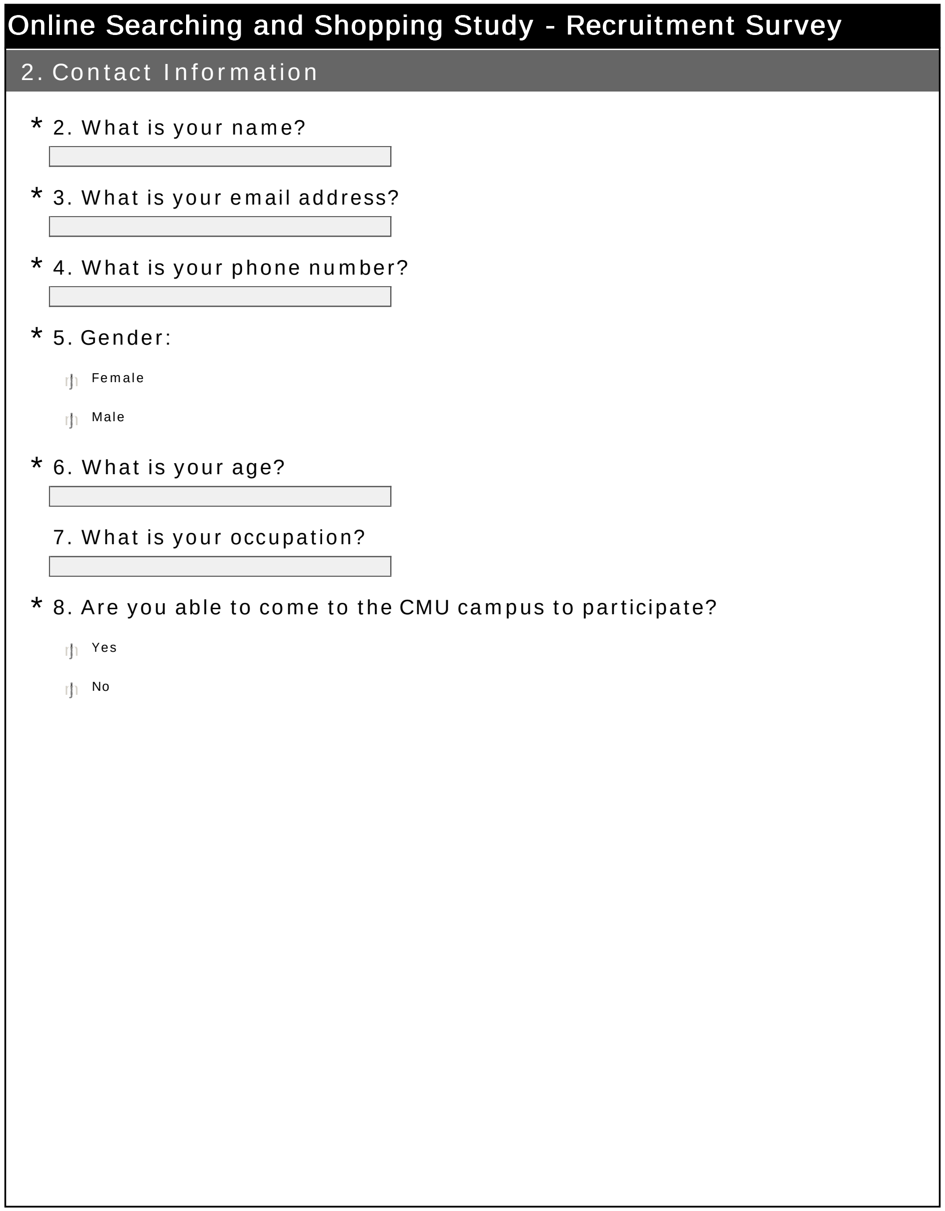
You will receive an initial $10 payment on the day of the study and the additional $40 payment after the products you purchased have been shipped.

This study is an "in-person" study, where we will need you to come to a location on the Carnegie Mellon Campus or to Carson St. on the South Side in order to complete the study. We plan on running the study within the next two weeks.

* 1. Are you still interested in participating in this study?

○ Yes

○ No



Online Searching and Shopping Study - Recruitment Survey

2. Contact Information

* 2. What is your name?

* 3. What is your email address?

* 4. What is your phone number?

* 5. Gender:

○ Female

○ Male

* 6. What is your age?

7. What is your occupation?

* 8. Are you able to come to the CMU campus to participate?

○ Yes

○ No

3. Questions

You are about halfway done with the survey.

Please answer the following questions:

9. Indicate your level of experience with the following online procedures:

	No Experience	Yearly	Monthly	Weekly	Daily
Using Online Search Engines	○	○	○	○	○
Shopping Online	○	○	○	○	○
Using Instant Messenger Systems	○	○	○	○	○
Checking Email	○	○	○	○	○
Banking Online	○	○	○	○	○

* 10. Have you purchased something online this year?

○ Yes

○ No

* 11. Do you have an online store/vendor that you often visit or purchase from?

○ Yes

○ No

12. If yes, what store(s) or vendor(s)?

* 13. When you are selecting a website to purchase an item from, how much do the following factors affect your choice?

	Not at all: 1	2	3	4	5	6	A great deal: 7
Accessibility for sight-impaired users	○	○	○	○	○	○	○
Compatibility of web site with mobile phone web browsers	○	○	○	○	○	○	○
Customer Reviews	○	○	○	○	○	○	○
Customer Service	○	○	○	○	○	○	○
Location of Physical Store	○	○	○	○	○	○	○
Page load speed	○	○	○	○	○	○	○
Popularity	○	○	○	○	○	○	○
Price	○	○	○	○	○	○	○
Privacy Policy	○	○	○	○	○	○	○
Return Policy	○	○	○	○	○	○	○
Software Compatibility	○	○	○	○	○	○	○
Shipping Speed	○	○	○	○	○	○	○
Website Design	○	○	○	○	○	○	○

4. Websites and Webshops

This is the last page of questions for the survey.

* 14. Please rate your level of concern about the following:

	Not concerned at all: 1	2	3	4	5	6	Extremely concerned: 7
A web site uses your health information to determine website content or ads	○	○	○	○	○	○	○
A web site shares your health information with other companies	○	○	○	○	○	○	○
A website contacts you about other services or products via telephone	○	○	○	○	○	○	○
A website contacts you about other services or products via email or postal mail	○	○	○	○	○	○	○
A website does not allow you to be removed from marketing/mailing lists	○	○	○	○	○	○	○
A website uses your financial information to determine website content or ads	○	○	○	○	○	○	○
A website shares your financial information with other companies	○	○	○	○	○	○	○
A website does not allow you to find out what information it stores about you	○	○	○	○	○	○	○
A website makes its privacy policy available	○	○	○	○	○	○	○
A website uses personally identifying information to determine your habits, interests, or other characteristics	○	○	○	○	○	○	○
A website shares personally identifying information with other companies	○	○	○	○	○	○	○
A website uses information that does not personally identify you to determine your habits, interests, or other characteristics	○	○	○	○	○	○	○
A website shares information that does not personally identify you with other companies	○	○	○	○	○	○	○

* 15. Please rate the following statements.

	Strongly Disagree: 1	2	3	4	5	6	Strongly Agree: 7
I feel safe giving my personal information to online stores.	○	○	○	○	○	○	○
Providing online stores with personal information involves too many unexpected problems.	○	○	○	○	○	○	○
I generally trust online companies with handling my personal information and my purchase history.	○	○	○	○	○	○	○

* 16. Please answer the following question.

	Not concerned at all: 1	2	3	4	5	6	Extremely concerned: 7
How concerned are you about threats to your personal privacy online in America today?	○	○	○	○	○	○	○

You have now completed the survey. You will be contacted shortly to be scheduled for this study.

Privacy Information Timing Study Exit Survey (Privacy Information Condition)

1. Online Shopping Habits

* 1. How much time do you spend on the Internet per week?

- ○ 1 to 5 hours
- ○ 6 to 10 hours
- ○ 11 to 20 hours
- ○ 21 to 30 hours
- ○ More than 31 hours

* 2. How many online purchases did you make in the last 30 days?

- ○ None
- ○ 1
- ○ 2 or 3
- ○ 4 or 5
- ○ 6 or more

* 3. How much time do you typically spend in an online shopping session when making a purchase?

- ○ Less than 10 minutes
- ○ 11 to 29 minutes
- ○ 30 to 59 minutes
- ○ 1 to 2 hours
- ○ More than 2 hours

2. Search Engine Specific

* 4. Do you currently use any Internet search engines?

- ○ Yes
- ○ No
- ○ If yes, which one(s)?

* 5. Do you currently use any shopping search engines?

- ○ Yes
- ○ No
- ○ If yes, which one(s)?

* 6. How easy was it to find the following information?

	Very Difficult: 0	1	2	3	4	5	Very Easy: 6
The sizes of reusable bags	○	○	○	○	○	○	○
The color of Ugg boots for women	○	○	○	○	○	○	○
The price of Ugg boots	○	○	○	○	○	○	○
The lifespan of CFLs	○	○	○	○	○	○	○
The CFL replacement for the 100 Watt bulb	○	○	○	○	○	○	○

3. Product Specific Questions

* 7. Before this study, had you ever purchased batteries online?

○ Yes

○ No

* 8. Was this the first time you made a purchase from the website where you purchased the batteries?

○ Yes

○ No

* 9. How much did the following factors influence your decision to purchase the batteries from that website?

	No Influence at all: 0	1	2	3	4	5	Strongly Influence: 6
The base price of the product	○	○	○	○	○	○	○
The total price of the product (including shipping and taxes)	○	○	○	○	○	○	○
The website design or appearance	○	○	○	○	○	○	○
Prior experience with the website	○	○	○	○	○	○	○
Prior experience with the company (not online)	○	○	○	○	○	○	○
The privacy policy	○	○	○	○	○	○	○
The return policy	○	○	○	○	○	○	○
Other factors (please describe below)	○	○	○	○	○	○	○

10. If there were any other factors, please describe them.

* 11. Which factor had the most influence on your decision?

* 12. Before this study, had you ever purchased sex toys online?

○ Yes

○ No

* 13. Was this the first time you made a purchase from the website where you purchased the Pocket Rocket Jr.?

○ Yes

○ No

* 14. How much did the following factors influence your decision to purchase the Pocket Rocket Jr. from that website?

	No Influence at all: 0	1	2	3	4	5	Strongly Influence: 6
The base price of the product	○	○	○	○	○	○	○
The total price of the product (including shipping and taxes)	○	○	○	○	○	○	○
The website design or appearance	○	○	○	○	○	○	○
Prior experience with the website	○	○	○	○	○	○	○
Prior experience with the company (not online)	○	○	○	○	○	○	○
The privacy policy	○	○	○	○	○	○	○
The return policy	○	○	○	○	○	○	○
Other factors (please describe below)	○	○	○	○	○	○	○

15. If there were any other factors, please describe them.

* 16. Which factor had the most influence on your decision?

4. Privacy Preferences

* 17. Please answering the following questions.

	Never: 0	1	2	3	4	5	Always: 6
Do you generally notice whether or not a website you are visiting has a privacy policy?	○	○	○	○	○	○	○
How often do you read websites' privacy policies?	○	○	○	○	○	○	○

* 18. How many privacy policies did you read in the purchasing tasks?

○ None of them

○ 1

○ 2 or 3

○ 4 or more

* 19. How much of the privacy policy did you read?
(Check all that apply)

☐ None

☐ I just clicked the link to make sure there was a privacy policy

☐ I skimmed it

☐ The first paragraph

☐ Half of it

☐ The whole thing

20. For the policies you read, why did you read them?

21. For the policies you didn't read, why didn't you read them?

* 22. Did you notice the green boxes next to some of the URLs?

○ Yes

○ No

---

* 23. What did you think the presence of green boxes meant?

* 24. Did the green boxes influence your decision to VISIT a particular web site?

☐ Yes

☐ No

☐ Why or why not?

* 25. Did the green boxes influence your decision to NOT visit a particular web site?

☐ Yes

☐ No

☐ Why or why not?

* 26. Did the green boxes influence your decision to purchase from a particular web site?

☐ Yes

☐ No

☐ Why or why not?

* 27. Did you read any of the Privacy Reports provided under the green boxes?

○ Yes

○ No

28. If "Yes," what information interested you? (Skip if you answered “No” to the last question.)

- ☐ The location of the website's full privacy policy
- ☐ Conditions under which websites may share your personal information
- ☐ Links to opt-out of additional communications
- ☐ A list of information that is collected about you
- ☐ How your information will be used
- ☐ How you can access your information
- ☐ Company contact information
- ☐ How to resolve privacy-related disputes with the website
- ☐ Other (please specify)

* 29. What kinds of things would you expect to find in the privacy policy of a website with four green boxes?

* 30. Would you consider a website with four green boxes to be adequately protecting your privacy?

- ○ Yes
- ○ No
- ○ I don't know

* 31. What kinds of things would you expect to find in the privacy policy of a website with two green boxes?

* 32. Would you consider a website with two green boxes to be adequately protecting your privacy?

- ○ Yes
- ○ No
- ○ I don't know

---

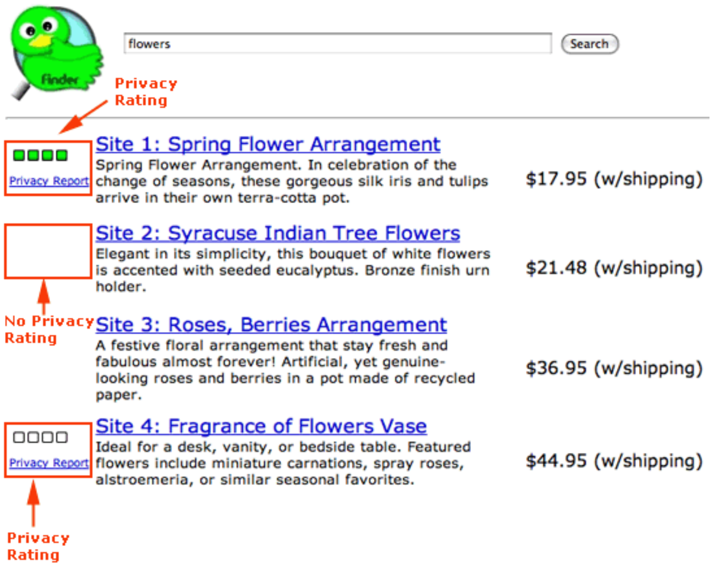
* 33. What kinds of things would you expect to find in the privacy policy of a website with boxes where none of the boxes are green?

* 34. Would you consider a website with four empty boxes to be adequately protecting your privacy?

- ○ Yes
- ○ No
- ○ I don't know

5. Privacy Indicators

Please examine the image below.



Site 1: Spring Flower Arrangement
Spring Flower Arrangement. In celebration of the change of seasons, these gorgeous silk iris and tulips arrive in their own terra-cotta pot.
$17.95 (w/shipping)

Site 2: Syracuse Indian Tree Flowers
Elegant in its simplicity, this bouquet of white flowers is accented with seeded eucalyptus. Bronze finish urn holder.
$21.48 (w/shipping)

Site 3: Roses, Berries Arrangement
A festive floral arrangement that stay fresh and fabulous almost forever! Artificial, yet genuine-looking roses and berries in a pot made of recycled paper.
$36.95 (w/shipping)

Site 4: Fragrance of Flowers Vase
Ideal for a desk, vanity, or bedside table. Featured flowers include miniature carnations, spray roses, alstroemeria, or similar seasonal favorites.
$44.95 (w/shipping)

* 35. What do you think it means when a site has no privacy rating?

* 36. What do you think of the privacy policy of a site with four green boxes compared to a site without any boxes?

The privacy policy of a site with four green boxes is:

○ Better than the one without any boxes

○ The same as the one without any boxes

○ Worse than the one without any boxes

○ I don't know

---

* 37. What do you think of the privacy policy of a site with four empty boxes compared to a site without any boxes?

The privacy policy of a site with four empty boxes is:

○ Better than the one without any boxes

○ The same as the one without any boxes

○ Worse than the one without any boxes

○ I don't know

6. Product Privacy Questions

* 38. What was your level of concern for your privacy when you were purchasing the products in this study?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
AA Batteries	○	○	○	○	○	○	○
Sex Toy	○	○	○	○	○	○	○

* 39. When purchasing the batteries, how concerned were you about what the company would do with the following information?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
Credit Card Number	○	○	○	○	○	○	○
Email Address	○	○	○	○	○	○	○
Physical Address	○	○	○	○	○	○	○
Phone Number	○	○	○	○	○	○	○
Purchase History	○	○	○	○	○	○	○

* 40. What specific privacy concerns, if any, did you have when purchasing the batteries?

* 41. When purchasing the sex toy, how concerned were you about what the company would do with the following information?

	Not concerned at all: 0	1	2	3	4	5	Extremely concerned: 6
Credit Card Number	○	○	○	○	○	○	○
Email Address	○	○	○	○	○	○	○
Physical Address	○	○	○	○	○	○	○
Phone Number	○	○	○	○	○	○	○
Purchase History	○	○	○	○	○	○	○

* 42. What specific privacy concerns, if any, did you have when purchasing the sex toy?

---

* 43. Did you have more concerns with purchasing one product or the other product?

○ More concerns when purchasing the AA batteries
○ More concerns when purchasing the Pocket Rocket Jr.
○ Equal privacy concerns when purchasing both products
○ No privacy concerns purchasing either product

* 44. To what extent do you agree or disagree with the following statements?

	Strongly Disagree:0	1	2	3	4	5	Strongly Agree: 6
Consumers have lost all control over how personal information is collected and used by companies	○	○	○	○	○	○	○
Most businesses handle the personal information they collect about consumers in a proper and confidential way	○	○	○	○	○	○	○
Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today	○	○	○	○	○	○	○

* 45. Have you ever found fraudulent transactions on your account statement?

○ Yes
○ No

* 46. Have you ever had your social security number stolen?

○ Yes
○ No

* 47. Have you ever been notified that your personal information has been stolen or compromised?

○ Yes
○ No

7. Demographics

* 48. What is your age?

* 49. What is your gender?

○ Female

○ Male

* 50. What is your highest level of education?

○ Some high school

○ High school diploma

○ College degree

○ Graduate Degree

○ Professional degree (including trade school)

○ Other (please specify)

51. How would you describe your race and ethnicity?

○ White

○ Black

○ Asian or Pacific Islander

○ Latino(a)/Hispanic

○ Native American

○ Other (please specify)

52. What is your country of origin?

Thank you for completing this questionnaire! Please raise your hand to notify the study administrator and receive your $10 payment. We will send the remainder of your payment ($40) to you after we confirm that the products you ordered have shipped. The study administrator will provide you with instructions for notifying us that your orders have shipped.

Bibliography

[1] Best practices and guidelines for location-based services. *CTIA Wireless Association* (April 2 2008). `http://www.ctia.org/business_resources/wic/index.cfm/AID/11300`.

[2] Wireless quick facts. *CTIA Wireless Association* (2008). `http://www.ctia.org/media/industry_info/index.cfm/AID/10323`.

[3] Bridgewater telephone co. v. city of monticello, 2009. `http://www.lawlibrary.state.mn.us/archive/ctappub/0906/opa081928-0602.pdf`.

[4] ACKERMAN, M. S., CRANOR, L. F., AND REAGLE, J. Privacy in e-commerce: examining user scenarios and privacy preferences. In *EC '99: Proceedings of the 1st ACM conference on Electronic commerce* (New York, NY, USA, 1999), ACM, pp. 1–8.

[5] ACQUISTI, A. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the ACM Electronic Commerce Conference (EC 04)* (New York, NY, 2004), ACM Press, pp. 21–29. http://www.heinz.cmu.edu/ acquisti/papers/privacy-gratification.pdf.

[6] ACQUISTI, A. Privacy in electronic commerce and the economics of immediate gratification. In *ACM Electronic Commerce Conference (EC '04)* (New York, NY, 2004), ACM Press, pp. 21–29.

[7] ACQUISTI, A., AND GROSS, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Privacy Enhancing Technologies Workshop (PET '06)* (2006).

[8] ACQUISTI, A., AND GROSSKLAGS, J. Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior. In *Proceedings of The 2nd Annual Workshop on Economics and Information Security (WEIS '03)* (2003).

[9] ACQUISTI, A., AND GROSSKLAGS, J. Privacy and rationality in individual decision making. *IEEE Security & Privacy* (January/February 2005), 24–30. http://www.dtc.umn.edu/weis2004/acquisti.pdf.

[10] ACQUISTI, A., AND GROSSKLAGS, J. Uncertainty, ambiguity, and privacy. In *Workshop on the Economics of Information Security (WEIS '05)* (2005).

[11] ACQUISTI, A., AND VARIAN, H. Conditioning prices on purchase history. *Marketing Science 24*, 3 (2005), 1–15.

[12] AGICHTEIN, E., AND ZHENG, Z. Identifying "Best Bet" web search results by mining past user behavior. In *Proc. of the ACM International Conference on Knowledge Discovery and Data Mining, (KDD)* (2006).

[13] AKERLOF, G. The market for lemons: quality uncertainty and the market mechanism. *Quarterly Journal of Economcis 84*, 3 (1970), 488–500.

[14] ALTMEYER, C. Smartphones, social networks to boost mobile advertising. *Reuters* (June 29 2009). http://www.reuters.com/article/technologyNews/idUSTRE55S2FY20090629.

[15] ANTHONY, D., KOTZ, D., AND HENDERSON, T. Privacy in location-aware computing environments. *IEEE Pervasive Computing 6*, 4 (2007), 64–72.

[16] ANTON, A., EARP, J., HE, Q., STUFFLEBEAM, W., BOLCHINI, D., AND JENSEN, C. Financial privacy policies and the need for standardization. *IEEE Security & Privacy 2*, 2 (Mar-Apr 2004), 36–45.

[17] ANTON, A., EARP, J. B., AND YOUNG, J. D. How internet users' privacy concerns have evolved since 2002. *In submission* (2009).

[18] BARKHUUS, L. Privacy in location-based services, concern vs. coolness. In *Workshop on Location System Privacy and Control at MobileHCI '04* (Glasgow, Scotland, 2004).

[19] BARKHUUS, L., BROWN, B., BELL, M., HALL, M., SHERWOOD, S., AND CHALMERS, M. From awareness to repartee: Sharing location within social groups. In *CHI '08* (April 2008), pp. 497–506.

[20] BARKHUUS, L., AND DEY, A. Location-based services for mobile telephony: a study of users' privacy concerns. In *INTERACT'03* (2003), pp. 702–712.

[21] BELLOTTI, V., AND SELLEN, A. Design for privacy in ubiquitous computing environments. In *ECSCW '93* (1993).

[22] BITCHER, D. Burger king, subaru trial location-based mobile advertising. *Mobile Marketer* (May 19 2009). http://www.mobilemarketer.com/cms/news/advertising/3276.html.

[23] BLAIS, A.-R., AND WEBER, E. A domain-specific risk-taking (dospert) scale for aduct populations. *Judgement and Decision Making 1* (2006), 44–37.

[24] BROWN, B., TAYLOR, A., IZADI, S., SELLEN, A., KAYE, J., AND EARDLEY, R. Location family values: A field trial of the whereabouts clock. In *Ubiquitous Computing (Ubicomp '07)* (2007), Springer-Verlag, pp. 354–371.

[25] BROWN, M., AND MUCHIRA, R. Investigating the relationship between internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research 5*, 1 (2004), 62–70.

[26] BRUNER, J. S. On perceptual readiness. *Psychological Review 64* (1957), 123–152.

[27] BRUNK, B. D. Understanding the privacy space. *First Monday 7*, 10 (2002). http://firstmonday.org/issues/issue7_10/brunk/index.html.

[28] BUSINESS, P. . A. New survey reports an increase in id theft and decrease in consumer confidence, May 2005. http://www.pandab.org/deloitteidsurveypr.html.

[29] CAMP, L. J. Design for trust. In *Trust, Reputation and Security: Theories and Practice*, R. Falcone, Ed. Springer-Verlag, 2003.

[30] CBS NEWS. Poll: Privacy Rights Under Attack, October 2, 2005; Accessed: July 12, 2009. `http://www.cbsnews.com/stories/2005/09/30/opinion/polls/main894733.shtml`.

[31] CHELLAPA, R., AND SIN, R. Personalization versus privacy: An empirical examination of the online consumers' dilemma. *Information Technology and Management 6*, 2-3 (2005), 181–202.

[32] COMSCORE. INC. comScore Releases January 2009 U.S. Search Engine Rankings, February 18 2009. http://www.comscore.com/press/release.asp?press=2729.

[33] CONSOLVO, S., SMITH, I., MATTHEWS, T., LAMARCA, A., TABERT, J., AND POWLEDGE, P. Location disclosure to social relations: Why, when, & what people want to share. In *CHI '05* (2005).

[34] CONSUMER REPORTS NATIONAL RESEARCH CENTER. Consumer Reports Poll: Americans extremely concerned about Internet Privacy, September 25 2008. http://www.consumersunion.org/pub/core_telecom_and_utilities/006189.html.

[35] CORNWELL, J., FETTE, I., HSIEH, G., PRABAKER, M., RAO, J., TANG, K., VANIEA, K., BAUER, L., CRANOR, L., HONG, J., MCLAREN, B., REITER, M., AND SADEH, N. User-controllable security and privacy for pervasive computing. In *IEEE Workshop on Mobile Computing Systems and Applications (HotMobile '07)* (2007).

[36] CORVIDA. What's plaguing your mobile social network? *ReadWriteWeb* (May 15 2008). `http://www.readwriteweb.com/archives/whats_plaguing_your_mobile_soc.php`.

[37] CRANOR, L. F. *Web Privacy with P3P*. O'Reilly and Associates, Sebastopol, CA, 2002.

[38] CRANOR, L. F., BYERS, S., KORMANN, D., AND MCDANIEL, P. 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), pp. 314–328.

[39] CRANOR, L. F., GUDURU, P., AND ARJULA, M. User Interface for Privacy Agents. *ACM Transactions on Computer-Human Interaction 13*, 2 (June, 2006), 135–178. http://portal.acm.org/citation.cfm?doid=1165734.1165735.

[40] CULNAN, M. J., AND ARMSTRONG, P. K. Information privacy concerns, procedural fairness, and impersonal trust. *Organizational Science 10*, 1 (1999), 104–115.

[41] CULNAN, M. J., AND MILNE, G. R. The Culnan-Milne Survey on Consumers and Online Privacy Notices, 2001; Accessed: July 12, 2009. http://intra.som.umass.edu/georgemilne/pdf_files/culnan-milne.pdf.

[42] DANA BOYD, AND ELLISON, N. B. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication 13*, 1 (2007). `http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html`.

[43] DANEZIS, G., LEWIS, S., AND ANDERSON, R. How much is location privacy worth? In *Online Proceedings of the Workshop on the Economics of Information Security Series (WEIS 2005* (2005).

[44] DAVIS, F., BAGOZZI, R., AND WARSHAW, P. Extrinsic and intrinsic motivation to use computers in the workplace. *Journal of Applied Social Psychology 22* (1992), 1111 – 1132.

[45] EGELMAN, S., TSAI, J., CRANOR, L., AND ACQUISTI, A. Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators. In *Proceedings of the ACM Computer-Human Interaction Conference* (New York, NY, USA, 2009), ACM Press.

[46] FAUL, F., ERDFELDER, E., LANG, A.-G., AND BUCHNER, A. G*power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods 39* (2007), 175–191.

[47] FEDERAL TRADE COMMISSION. Financial privacy rule: Interagency notice research project, 2009. `http://www.ftc.gov/privacy/privacyinitiatives/financial_rule_inrp.html`.

[48] FISCHHOFF, B. Acceptable risk: A conceptual proposal. *Risk: Health, Safety & Environment 1* (1994), 1–28.

[49] FOGG, B., MARSHALL, J., LARAKI, O., OSIPOVICH, A., VARMA, C., FANG, N., PAUL, J., RANGEKAR, A., SHON, J., SWANI, P., AND TREINEN, M. What Makes Web Sites Credible? A Report on a Large Quantitative Study. In *Proceedings of the ACM Computer-Human Interaction Conference* (Seattle, WA, March 31 - April 4, 2001), ACM.

[50] FROMMER, D. Loopt location to update in the background on iPhone. *Business Insider* (September 4 2009). `http://www.businessinsider.com/loopt-to-run-in-the-background-on-iphone-2009-6`.

[51] GANDAL, N. The dynamics of competition in the internet search engine market. *International Journal of Industrial Organization 19*, 7 (2001), 1103 – 1117.

[52] GROSSKLAGS, J., AND ACQUISTI, A. Uncertainty, ambiguity, and privacy. In *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information* (2007).

[53] HANN, I.-H., HUI, K.-L., LEE, T., AND PNG, I. Online information privacy: Measuring the cost-benefit trade-off. In *23rd International Conference on Information Systems (ICIS '02)* (2002).

[54] HARRIS INTERACTIVE. A survey of consumer privacy attitudes and behaviors, 2001. http://www.bbbonline.org/UnderstandingPrivacy/library/ harrissummary.pdf.

[55] HARRIS INTERACTIVE. Survey shows privacy concerns a major roadblock for the adoption of location-based services and presence technology, 2007. http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=1184.

[56] HIGGINS, E. T. Knowledge activation: Accessibility, applicability, and salience. In *Social psychology: Handbook of basic principles*, E. T. Higgins and A. W. Kruglanski, Eds. New York: Guilford Press., 1996, pp. 133–168.

[57] HOCHHAUSER, M. Why patients won't understand their HIPAA notices. Tech. rep., Privacy Rights Clearinghouse, 2003. http;//www.privacyrights.org/ar/HIPAA-Readability.htm.

[58] HOCHHEISER, H. The platform for privacy preference as a social protocol: An examination within the U.S. policy context. *ACM Transactions on Internet Technology (TOIT) 2*, 4 (2002), 276–306.

[59] HOLSON, L. Privacy lost: These phones can find you. *New York Times* (October 23 2007). `http://www.nytimes.com/2007/10/23/technology/23mobile.html`.

[60] HSIEH, G., TANG, K., LOW, W., AND HONG, J. Field deployment of IMbuddy : A study of privacy control and feedback mechanisms for contextual IM. In *Ubiquitous Computing (Ubicomp '07)* (2007), pp. 91–108.

[61] HUBERMAN, B., ADAR, E., AND FINE, L. Valuating privacy. In *Proceedings of The Workshop on The Economics of Information Security* (Boston, MA, June 1-3, 2005).

[62] HUI, K.-L., THEO, H., AND LEE, S.-Y. The value of privacy assurance: An exploratory field experiment. *MIS Quarterly 31*, 1 (2007), 19–33.

[63] IACHELLO, G., SMITH, I., CONSOLVO, S., ABOWD, G., HUGHES, J., HOWARD, J., POTTER, F., SCOTT, J., SOHN, T., HIGHTOWER, J., AND LAMARCA, A. Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service. In *UbiComp 2005* (2005), Springer-Verlag, pp. 213 – 231.

[64] JENSEN, C., AND POTTS, C. Privacy policies as decision-making tools: An evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems* (Vienna, Austria, 2004), pp. 471–478.

[65] JENSEN, C., POTTS, C., AND JENSEN, C. Privacy practices of internet users: Self-reports versus privacy practices of internet users: Self-reports versus observed behavior observed behavior. *International Journal of Human-Computer Studies 63* (2005), 203–227.

[66] JOHN, L. K., ACQUISTI, A., AND LOEWENSTEIN, G. F. The Best of Strangers: Context Dependent Willingness to Divulge Personal Information. *SSRN eLibrary* (2009).

[67] JUNGLAS, I., AND WATSON, R. Location-based services. *Communications of The ACM 51*, 3 (March 2008), 65–69.

[68] KAHNEMAN, D., AND TVERSKY, A. Prospect theory: An analysis of decision under risk. *Econometrica 47* (1979), 263–291.

[69] KAHNEMAN, D., AND TVERSKY, A. Choices, values and frames. *American Psychologist 39*, 4 (1984), 341–350.

[70] KHALIL, A., AND CONNELLY, K. Context-aware telephony: Privacy preferences and sharing patterns. In *CSCW '06* (2006).

[71] KIM, M., FIELDING, J. J., AND KOTZ, D. *Risks of Using AP Locations Discovered Through War Driving*. Springer Berlin / Heidelberg, 2006, pp. 67 – 82.

[72] KRECH, D., AND CRUTCHFIELD, R. S. *Theory and Problems of Social Psychology*. New York: McGraw-Hill, 1948.

[73] KUMARAGURU, P., AND CRANOR, L. F. Privacy indexes: A survey of westin's studies. Tech. Rep. CMU-ISRI-5-138, Carnegie Mellon University, December, 2005. http://reports-archive.adm.cs.cmu.edu/anon/isri2005/abstracts/05-138.html.

[74] LEBO, H. Surveying the Digital Future: Year Seven. Tech. rep., USC Annenberg School Center for the Digital Future, 2008.

[75] LEBO, H. The digital future report 2009. Tech. rep., USC Annenberg School Center for the Digital Future, 2009.

[76] LEDERER, S., MANKOFF, J., AND DEY, A. K. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03* (2003), no. 724-725.

[77] MALHORTA, N., KIM, S., AND AGARWAL, J. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research 15*, 4 (2004), 336–355.

[78] MAXON. Gps locator phones help you reach out and track someone, October 21 2006. http://seattletimes.nwsource.com/html/businesstechnology/2003315216_ptgpsphones21.html.

[79] MCCARTHY, C. The mobile social: Not ready for prime time? *News.com* (February 13 2008). `http://www.news.com/8301-13577_3-9870611-36.html`.

[80] MCCULLAGH, D. RFID tags: Big brother in small packages. *CNET News.com* (January 13 2003). http://news.com.com/2010-1069-980325.html.

[81] MCKNIGHT, D. H., AND CHERVANY, N. L. What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *Int. J. Electron. Commerce 6*, 2 (Winter 2001), 35–59.

[82] MEDIA, B. Online privacy still a consumer concern, February 2009. http://www.burstmedia.com/assets/newsletter/items/2009_02_01.pdf.

[83] MIKLAS, A. G., GOLLU, K. K., CHAN, K. K. W., SAROIU, S., GUMMADI, K. P., AND DE LARA, E. Exploiting social interactions in mobile systems. In *UbiComp 2007* (2007), vol. 4717/2007, pp. 409–428.

[84] MILNE, G. R., AND CULNAN, M. J. 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.

[85] MILNE, G. R., AND CULNAN, M. J. Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices. *Journal of Interactive Marketing 18*, 3 (Summer 2004), 54–61.

[86] MILNE, G. R., AND GORDON, M. E. Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy Marketing 12*, 2 (1993), 206–215.

[87] MORGAN, M. G., FISCHHOFF, B., BOSTROM, A., AND ATMAN, C. *Risk Communication: A Mental Models Approach*. Cambridge University Press, New York, 2001.

[88] NEWS, C. RFID and privacy: Tracking your patterns?, 2006. http://www.cbc.ca/news/background/privacy/.

[89] PATIL, S., AND LAI, J. Who gets to know what when: Configuring privacy permissions in an awareness application. In *CHI '05* (2005), pp. 101 – 110.

[90] PRIVACY LEADERSHIP INITIATIVE. Privacy notices research final results, December 2001; Accessed: December 17, 2007. `http://www.ftc.gov/bcp/workshops/glb/supporting/ harris%5C%20results.pdf`.

[91] RAENTO, M., OULASVIRTA, A., PETIT, R., AND TOIVONEN, H. Contextphone: A prototyping platform for context-aware mobile applications. In *Pervasive '05* (2005), pp. 51 – 59.

[92] RIEGELSBERGER, J., SASSE, M. A., AND MCCARTHY, J. D. The mechanics of trust: a framework for research and design. *International Journal of Human-Computer Studies 62*, 3 (2005), 381–422.

[93] ROBERTS, P., AND CHALLINOR, S. IP address management. *BT Technology Journal 18*, 3 (July 2000), 127–136.

[94] ROSE, E. 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* (2005).

[95] SADEH, N. *M-Commerce: Technologies, Services, and Business Model*, 1st ed. Wiley, 2002.

[96] SADEH, N., HONG, J., CRANOR, L., FETTE, I., KELLEY, P., PRABAKER, M., AND RAO, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* (Forthcoming 2008).

[97] SHERMAN, E. Privacy policies are great—for phds, September 4 2008. http://industry.bnet.com/technology/1000391/privacy-policies-are-great-for-phds/.

[98] SHIH-FEN S. CHEN, KENT B. MONROE, Y.-C. L. The effects of framing price promotion messages on consumers' perceptions and purchase intentions. *Journal of Retailing 74*, 3 (1998), 353–372.

[99] SHOSTACK, A. Paying for privacy: Consumers and infrastructures. In *Proceedings of The 2nd Annual Workshop on Economics and Infomation Security (WEIS '03)*

(2003).

[100] SMITH, H. J., MILBERG, S., AND BURKE, S. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly 20*, 2 (1996), 167–196.

[101] SMITH, I., CONSOLVO, S., LAMARCA, A., HIGHTOWER, J., SCOTT, J., SOHN, T., HUGHES, J., IACHELLO, G., AND ABOWD, G. Social disclosure of place: From location technology to communication practices. In *Pervasive '05* (2005), Springer-Verlag, pp. 134 – 151.

[102] SOLOVE, D. A taxonomy of privacy. *University of Pennsylvania Law Review 154*, 3 (2006), 477. http://ssrn.com/abstract=667622.

[103] SPIEKERMANN, S. *User Control in Ubiquitous Computer: Design Alternatives and User Acceptance*. Shaker Verlag, 2008.

[104] SPIEKERMANN, S., GROSSKLAGS, J., AND BERENDT, B. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. In *Proceedings of EC'01: Third ACM Conference on Electronic Commerce* (Tampa, Florida, 2001), pp. 38–47. http://www.sims.berkeley.edu/ jensg/research/ eprivacy_acm.html.

[105] STEWART, K. A., AND SEGARS, A. 2002. *An empirical examination of the concern for information privacy instrument 13*, 1 (2002), 36–49.

[106] STONE, B., AND STETLER, B. Facebook withdraws changes in data use. *The New York Times* (February 18 2009). http://www.nytimes.com/2009/02/19/technology/internet/19facebook.html.

[107] SULLIVAN, D. Where Are They Now? Search Engines We've Known & Loved, March 4 2003. http://searchenginewatch.com/2175241.

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

[109] TAYLOR, C. R. Consumer privacy and the market for customer information. *Rand Journal of Economcis 35*, 4 (2004), 631–651.

[110] TAYLOR, S. E., AND FISKE, S. T. Salience, attention, and attribution: Top of the head phenomena. In *Advances in experimental social psychology*, L. Berkowitz, Ed., vol. 11. New York: Academic Press, 1978, pp. 249–288.

[111] TEDESCHI, B. Everybody talks about online privacy, but few do anything about it. *The New York Times* (June 3, 2002), C6.

[112] TRUSTE. Consumers have a false sense of security about online privacy – actions inconsistent with attitudes, December 2006. http://www.truste.org/about/press_release/12_06_06.php.

[113] TSAI, J., EGELMAN, S., CRANOR, L., AND ACQUISTI, A. The effect of online privacy information on purchasing behavior: An experimental study. In *Proceedings of the 2007 Workshop on the Economics of Information Security (WEIS'07)* (Pittsburgh, PA, USA, 2007).

[114] TSAI, J., EGELMAN, S., CRANOR, L., AND ACQUISTI, A. The effect of online privacy information on purchasing behavior: An experimental study. *Information Systems Research* (Forthcoming).

[115] TSAI, J., KELLEY, P., CRANOR, L., AND SADEH, N. Location-sharing technologies: Privacy risks and controls. In *37th Research Conference on Communication, Information and Internet Policy (TPRC '09)* (2009).

[116] TSAI, J. Y., KELLEY, P., DRIELSMA, P., CRANOR, L. F., HONG, J., AND SADEH, N. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems* (New York, NY, USA, 2009), ACM, pp. 2003–2012.

[117] TUROW, J., FELDMAN, L., AND MELTZER, K. Open to exploitation: American shoppers online and offline. Tech. rep., Annenberg Public Policy Center of the University of Pennsylvania, 2005.

[118] WATHIEU, L., AND FRIEDMAN, A. An empirical approach to understanding privacy valuation. In *Proceedings of The Forth Annual Workshop on Economics and Information Security (WEIS '05)* (Cambridge, MA, 2005).

[119] WESTIN, A. F., AND ASSOCIATES., H. L. . Harris-equifax consumer privacy survey (1996). Tech. rep., Equifax, Inc., 1996.