NET Institute*

www.NETinst.org

Working Paper #06-29

October 2006

What's It To You?
A Survey of Online Privacy Concerns and Risks

Janice Tsai, Lorrie Cranor, Alessandro Acquisti, and Christina Fong
Carnegie Mellon University

What's It To You?

A Survey of Online Privacy Concerns and Risks

October 2006

Janice Tsai, Lorrie Cranor, Alessandro Acquisti, and Christina Fong
Carnegie Mellon University

Abstract

Finding information about privacy practices can be difficult: privacy policies often do not present this information in an accessible way. People typically do not know how or for what purpose their personal information, gathered online, will be used. When asked, people frequently express concerns about their privacy, but their behavior often does not reflect their concerns. We conducted an online survey to examine participants' online privacy concerns, focusing especially on the online shopping context. We asked participants about several scenarios related to the privacy of personal information. We found that Privacy Finder, a P3P-enhanced search engine, provides information that addresses the scenarios that participants believe are most likely to occur. We also asked participants about a wide range of items for purchase online to evaluate which types of items are more likely to raise privacy concerns.

1 Introduction

When asked, most Americans say that their right to privacy is "under serious threat," (CBS News, 2005) and express concern about companies collecting their personal data (Ackerman, *et al.*, 1999; Harris Interactive, 2001; CBS News, 2005; P&AB, 2005; Turow, *et al.,* 2005). According to a recent survey, 64% of people have "decided not to purchase something from a company because they weren't sure how their personal information would be used" (P&AB 2005). Concerns raised about privacy include the collection of personal information, unauthorized secondary use, improper access, and errors in personal information. One method industry and the government have taken to address these concerns and risks is to recommend that businesses post privacy policies to convey their privacy practices. Unfortunately, 70% of people in a recent study disagreed with the statement "privacy policies are easy to understand," (Turow, *et al*., 2005) and few people make the effort to read them (Privacy Leadership Initiative, 2001). In this paper, we conduct a survey to determine more specific types of privacy concerns that individuals have when they are shopping online.

To facilitate user access to privacy information, the Platform for Privacy Preferences (P3P), a machine-readable format for privacy policies, was developed. Users can use software tools or user agents to define their privacy preferences and determine if websites' P3P privacy policies match those privacy preferences (Cranor, 2002). P3P user agents can also translate computer-readable privacy policies into natural language and display them in their entirety or in simplified formats (Cranor, *et al.* 2006). We have developed a P3P-enabled search engine called Privacy Finder (http://search.privacybird.com) that annotates search results with privacy information derived from P3P policies and provides automatically-generated "privacy reports" for P3P-enabled web sites.

This paper reports on an online survey we conducted to examine online privacy concerns and the perceived trouble or inconvenience associated with privacy risks. We wish to determine if the concerns expressed are addressed by Privacy Finder. Additionally, this survey provides insights into the types of purchases that raise the most serious privacy concerns for online shoppers.

In Section 2 we present a brief introduction to privacy policies and privacy concerns. In Section 3 we discuss the methodology and results of our survey. In Section 4, we discuss our results and present our conclusions. We find that, consistent with previous studies, people continue to have significant privacy concerns when they use the Internet. People report that they notice privacy policies, even though they do not often read them. Based on the likelihood ratings of our online concern scenarios, we find that Privacy Finder provides information that

addresses the scenarios that participants believe are most likely to occur.

2 Background

2.1 Privacy Policies

Privacy policies are posted by businesses and organizations to inform individuals about how their personal information will be used, how long it will be retained, and what choices they have about the use of their data (Federal Trade Commission, 2000; Cavoukian and Hamilton, 2002). Ideally, this information should allow consumers to take advantage of privacy-related options and choose companies and websites based on their privacy policies.

In the United States, the regulation of privacy varies from sector to sector. Privacy policies are mandated by law in certain jurisdictions and sectors, including US government websites, companies in the healthcare and financial industries, and websites designed for children. For other sectors, such as the retail industry, privacy policies are recommended by association codes of conduct or required in self-regulatory programs in which companies can choose to participate.

The display of privacy policies has become very common. A December 2001 survey found that nearly all the "most popular" websites and 83% of a random sample of frequently visited websites posted privacy policies (Adkinson, *et al.,* 2002). The fraction of popular sites posting privacy policies more than doubled in the three years prior to that study (Milne and Culnan, 2002).

Despite the availability and increasing prevalence of privacy policies, people rarely read them (Privacy Leadership Initiative, 2001; Culnan and Milne, 2001; Jensen, *et al*., 2005). Consumers find privacy policies difficult to read and understand; they are typically written in a way that requires college-level reading skills to comprehend (Hochhauser, 2003; Jensen and Potts, 2004). Not only is the language frustrating, but privacy policies may also change without any warning. Privacy policies typically differ, significantly, from website to website, making it difficult to compare the information contained in them. Since these policies largely go unread, people may make mistaken assumptions about them. One study found that a majority of Americans who report having seen privacy policies on popular websites believe that the presence of a privacy link means that their data is protected (Turow, 2003; Turow, et al., 2005). Another study, which focused on privacy seals, found there is little understanding of what these seals mean (Moores, 2005).

Despite the large numbers of privacy policies posted, privacy information remains invisible to Internet users. Privacy policies have not been effective at making privacy

information accessible. While individuals may be aware that a company or organization has a privacy policy, they still lack enough information to make informed decisions.

Studies have shown that individuals often do not behave in ways that are consistent with their stated privacy concerns (Spiekermann *et al.*, 2001; Acquisti, 2004). There are a number of possible explanations for the dichotomy between stated privacy preferences and privacy-related behaviors. One hypothesis is that the dichotomy is caused, in part, by the fact that it is too difficult for users to obtain the information they would need to make privacy-informed decisions. If this is true, then we would expect that Internet users' behavior will become more privacy protective when privacy policy information is made more accessible to them. Indeed, our preliminary Privacy Finder laboratory studies suggest that when privacy information is available in search engines, individuals may seek out more privacy-friendly web sites and pay a small premium for privacy when they make some types of purchases (Gideon *et al.,* 2006).

2.2 Privacy concerns

We have reviewed related work to identify specific user privacy concerns in an ecommerce environment. Smith, *et al.* (1996) outlined four dimensions of privacy concern for organizational practices: *collection* of personal information, *unauthorized secondary use* of personal information, *errors* in personal information, and *improper access* to personal information. These dimensions have also been mapped to information privacy concerns relating to online marketing and purchasing. In the online marketing situation, the dimensions of concern are reframed as the *collection* of personal information, *control* over the use of personal data, and *awareness* of privacy practices and the use of personal information (Malhotra, *et al.* 2004). Control and awareness encompass unauthorized secondary use, improper access, and errors.

When examining online purchase behavior, three dimensions of concern have been defined, *unauthorized secondary use, errors* in personal information, and the *invasion of privacy* (Brown and Muchira, 2004), with consumers placing 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. In many of these dimensions of privacy concern, the consumer has little control over the practices of the organizations or businesses that are collecting their information. To make privacy practices more salient, we focus our study on the collection of personal information and the awareness of privacy practices.

3 Survey Procedure and Analysis

We developed the survey with the following high-level questions in mind:

- What types of privacy concerns do individuals have when using the Internet and when shopping online?
- Does Privacy Finder provide information related to these concerns?
- What are the greatest concerns in terms of both perceived likelihood and consequences?
- What types of purchases raise the most significant privacy concerns?

3.1 Procedure

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. The survey contained several categories of questions including risk attitudes towards online shopping and online privacy, the use of privacy policies, online scenarios, items of concern, privacy classification questions, user study purchase items, and demographics. 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.

3.2 Basic Demographics

Three hundred and sixty-two people began the survey. Of these, 7 were disqualified because they had not made at least one online purchase in the last year. People who did not complete the survey were removed from the sample. The final sample size was $n = 276$. The ages of the participants ranged from 18 to 71 years old, with a mean of 30.2 years. 62.5% of the respondents were female.

The individuals in our sample were well-educated, with 85.5% reporting that they had completed at least a college degree. Of our sample, 33.8% also had a graduate degree and 5.6% a professional degree.

The people in our sample tended to be heavy Internet users, which is not surprising since we only surveyed people with online purchasing experience. Around 75% of respondents reported spending more than 10 hours online per week. Our sample also consisted of people

who were very experienced in shopping online: 43.5% had made 2 or 3 online purchases in the previous month while 27.2% had made 4 or more purchases.

3.3 Online Concerns

We asked several open-ended questions about the types of privacy concerns that people had on the Internet, in general, and the concerns that they had specifically related to shopping online. Common Internet use concerns included the tracking of Internet use by companies, employers, and the government. Other concerns included identity theft, spyware and viruses, unwanted email, and data security. Specifically related to online shopping, respondents had a much larger focus on credit card information theft. These concerns centered on the collection of personal information, awareness of privacy practices, as well as the improper access to financial information.

3.4 Purchase Information and Privacy Policies

To control for the online purchasing experiences of different respondents, we asked them to tell us what their last online purchase was and from which online store it was made. While most of the reported purchases were probably not privacy-sensitive in nature, 7 purchases might be considered privacy-sensitive. These possible privacy-sensitive purchases include underwear (1), massage oil (2), tobacco (1), personal/medical items (2), and a "gift" from a "romantic store" (1). We found that books and clothing were the most commonly purchased items (22% and 20% respectively) followed by computer parts and CDs or DVDs (14% and 12%). The items purchased are detailed in Figure 1. The "services" category includes NetFlix (DVD movie rentals) subscriptions and magazine subscriptions. Amazon.com was the most popular store with 30.4% of the purchases followed by Ebay.com with 13% of purchases.

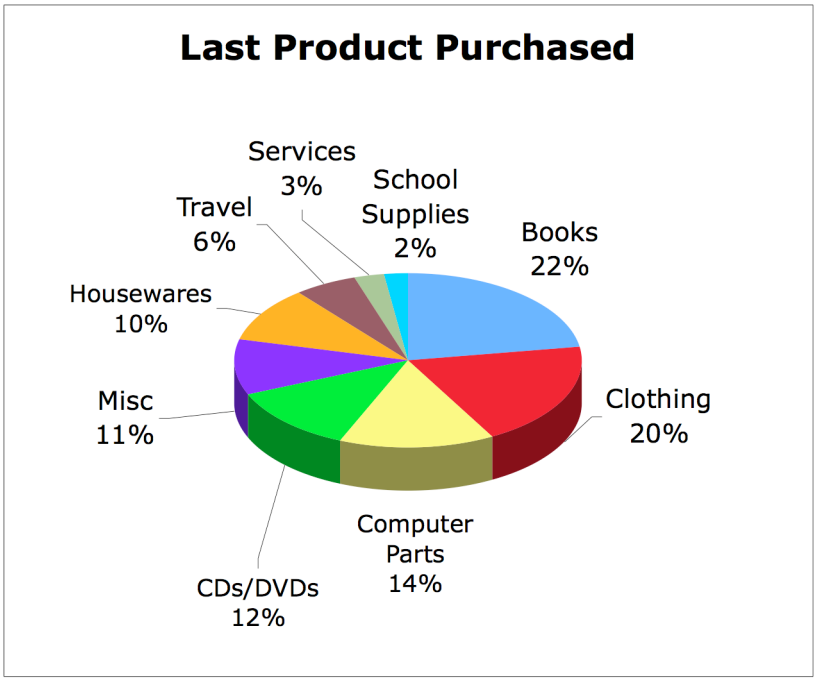

Figure 1: The last product purchased online by participants

We were also interested to see how participants' actions were linked to privacy concerns. To find out, we inquired about their 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.

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

In a paired t-test, participants reported that they are more likely to notice if a website has a privacy policy than they are to read them, $M = 3.1$ and $M = 1.85$, $t(275) = 12.57$, $p < .0001$. We also asked, on an 11-point Likert scale, "How bad is it if an online company you buy from doesn't have a privacy policy?" 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.

3.5 Risk Beliefs

We sought to determine the level of risk that people perceive when they are sharing their information online, and in particular, 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*)
- 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*)
- 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, Chronbach's α = 0.77. The Chronbach's α is a measure of the reliability of a multi-item scale. It is appropriate when the scale is constructed by averaging a set of unstandarized items which are coded consistently. Values of 0.7 or higher are desirable.

The histogram depicted in Figure 2 shows an approximately normal distribution for the risk scores. The Pearson's 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.

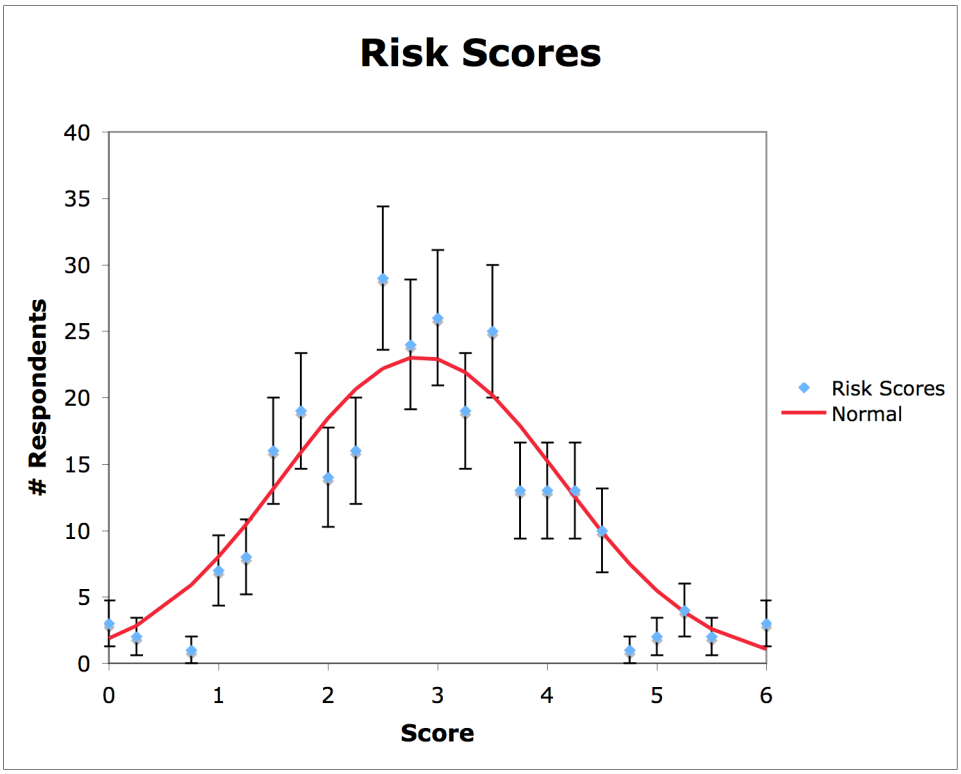

Figure 2: Histogram of risk scores.

3.6 Privacy Attitudes

To evaluate the privacy attitudes of our sample, we asked our participants the "Privacy Segmentation Index" questions developed by Dr. Alan Westin (Kumaraguru, and Cranor 2005). These questions are the following:

1. Consumers have lost all control over how personal information is collected and used by companies.
2. Most businesses handle the personal information they collect about consumers in a proper and confidential way.
3. Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today.

Participants are classified into three categories: privacy fundamentalists, privacy pragmatists, and the privacy unconcerned. The descriptions of these categories are as follows (Harris, 2001):

> Privacy Fundamentalists: At the maximum extreme of privacy concern, Privacy Fundamentalists are the most protective of their privacy. These consumers feel companies should not be able to acquire personal information for their organizational needs and think that individuals should be proactive in refusing to provide information. Privacy

Fundamentalists also support stronger laws to safeguard an individual's privacy.

Privacy Pragmatists: Privacy Pragmatists weigh the potential pros and cons of sharing information; evaluate the protections that are in place and their trust in the company or organization. After this, they decide whether it makes sense for them to share their personal information.

Privacy Unconcerned: These consumers are the least protective of their privacy - they feel that the benefits they may receive from companies after providing information far outweigh the potential abuses of this information. Further, they do not favor expanded regulation to protect privacy.

According to Westin's classification, privacy fundamentalists agree with the statement 1. and disagree with statements 2. and 3. The privacy unconcerned disagree with the statement 1. and agree with the statements 2. and 3. The remaining respondents are privacy pragmatists.

We found that 70.3% of our sample was comprised of privacy fundamentalists, 14.13% of the privacy unconcerned, and 15.6% of privacy pragmatists. The Westin classification results in this survey are very striking. In his previous privacy surveys, (1996, 2000, 2001, and 2003), Westin found that the majority of respondents were privacy pragmatists. The results of previous Westin surveys are summarized in Table 1, (Kumaraguru, 2005).

Year	Privacy Fundamentalist	Privacy Pragmatists	Privacy Unconcerned
1995 – 1999	~25%	~55%	~20%
Mid 2000	25%	63%	12%
Late 2001	34%	58%	8%
2003	26%	64%	10%

Table 1: Westin Privacy Classifications for previous surveys

Our sample may contain a greater number of privacy fundamentalists than in previous surveys due to a self-selecting phenomenon inherent in soliciting participants for an "Online Privacy Concerns" survey.

The responses of the risk attitude questions are grouped by Westin classification in Figure 3. These questions are the following:

1. Do you generally notice whether or not a website you are visiting has a privacy policy? (Never = 0 to Always = 6)
2. Risk score (Low risk = 0 to High risk = 6)

3. How often do you read websites' privacy policies? (Never = 0 to Always = 6)
4. In general, I find it risky to shop at an online store (Strongly disagree = 0 to Strongly Agree = 6)
5. How much time do you spend on the Internet per week? (Less than 1 hour, 1 – 5 hours, 6 – 10 hours, 11 – 20 hours, 21 – 30 hours, More than 31 hours.

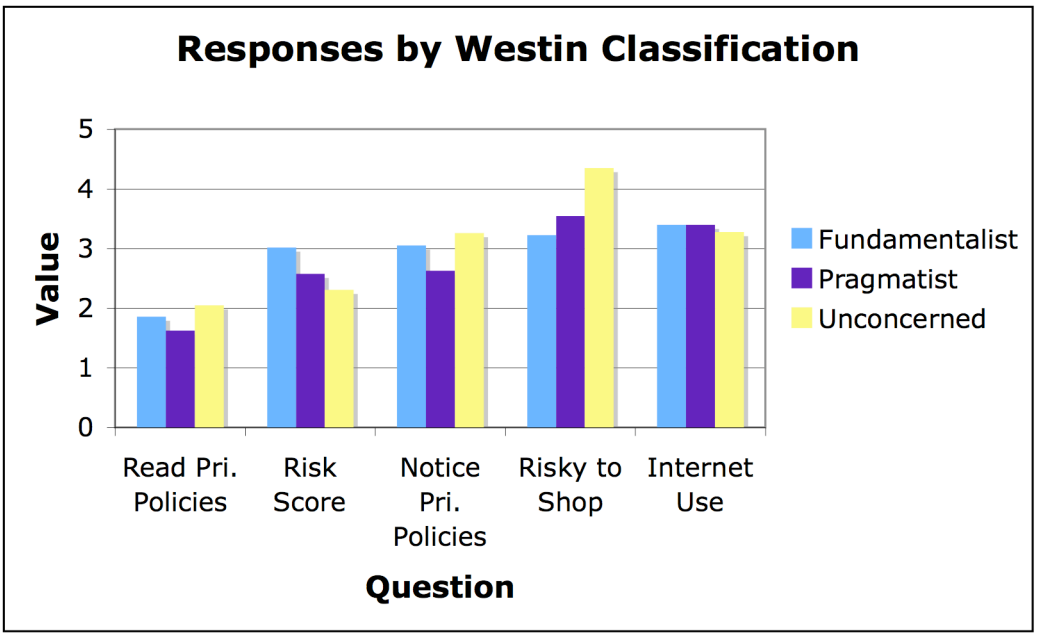

Figure 3: Risk Attitude Responses by Westin Classification

Based on 2-sample t-tests of responses to the questions displayed in Figure 3, separated by Westin classification, privacy fundamentalists (M = 3.02) had statistically significantly greater risk scores than the privacy pragmatists (M = 2.58) and the privacy unconcerned (M = 2.31), t(231 (pragmatist)) = 2.43, p = .005; and t(226 (unconcerned)) = 3.67, p = .0003. This indicates that privacy fundamentalists have a higher assessment of risk related to their personal information when they are shopping online. While these differences are statistically significant, none of the three classifications perceive unusually high levels of risk related to the sharing of personal information.

Additionally, when responding to the question "In general, I find it risky to shop at an online store," a 2-sample t-test indicates that the privacy unconcerned (M = 4.35) had statistically significantly greater values than the privacy fundamentalists (M = 3.22) and the privacy pragmatists (M = 3.54), t(226 (fundamentalists)) = -4.40, p < .0001; and t(77 (pragmatist))=-2.89, p = .005. This suggests that people who are privacy unconcerned have a higher perception of risk of shopping online than that of simply sharing personal information that is unrelated to financial transactions.

All three groups of participants tend to have a similar tendency to read privacy policies (not very often); purchase about 2 or 3 items online in the last 30 days; notice privacy policies, on average; spend about 11 to 20 hours on the Internet per week; and feel that it is bad if an online company that they buy from doesn't have a privacy policy. The use of the Westin classifications may also not be completely applicable to the sample population. Based on the availability heuristic in rational choice theory (Hastie and Dawes, 2001) people's assessment of risk can be biased due to the ease of which they can recall a situation or the frequency that they have heard or read about a certain situation. In this case, that is the scenarios of use or abuse of personal information. The more people read about threats to privacy, the more concerned they are (EPIC, 2005), and the more likely they are to be categorized as privacy fundamentalists, even though they do not adopt actions that would warrant this classification.

3.7 Scenarios

We asked participants to evaluate the likelihood of certain online scenarios as well as to provide a rating on a 11-point Likert scale of how 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 continue to receive email from an online store even after you've asked them to take you off their mailing list? (Continued Contact)
- If an online store sold your name and contact information to other companies after you made an online purchase? (Information Sold)
- If an online store keeps track of all the items you click on at their website? (Track items)
- If an online store inferred information about your habits or interests after you make a purchase? (Infer Information)
- If your search engine history was made public? (Search History)
- If your purchase history from multiple online stores was combined with other personal information to produce a detailed profile about you? (Dossier)
- If your family members or friends accessed your online purchase records without your permission? (Family/Friends)

- If current, perspective, or future employers learned about your online purchase history? (Employers)
- If your purchase history from an online store was made available during a lawsuit you are involved in? (Lawsuit)

The responses to the online concern scenarios are detailed in Figure 4. 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.

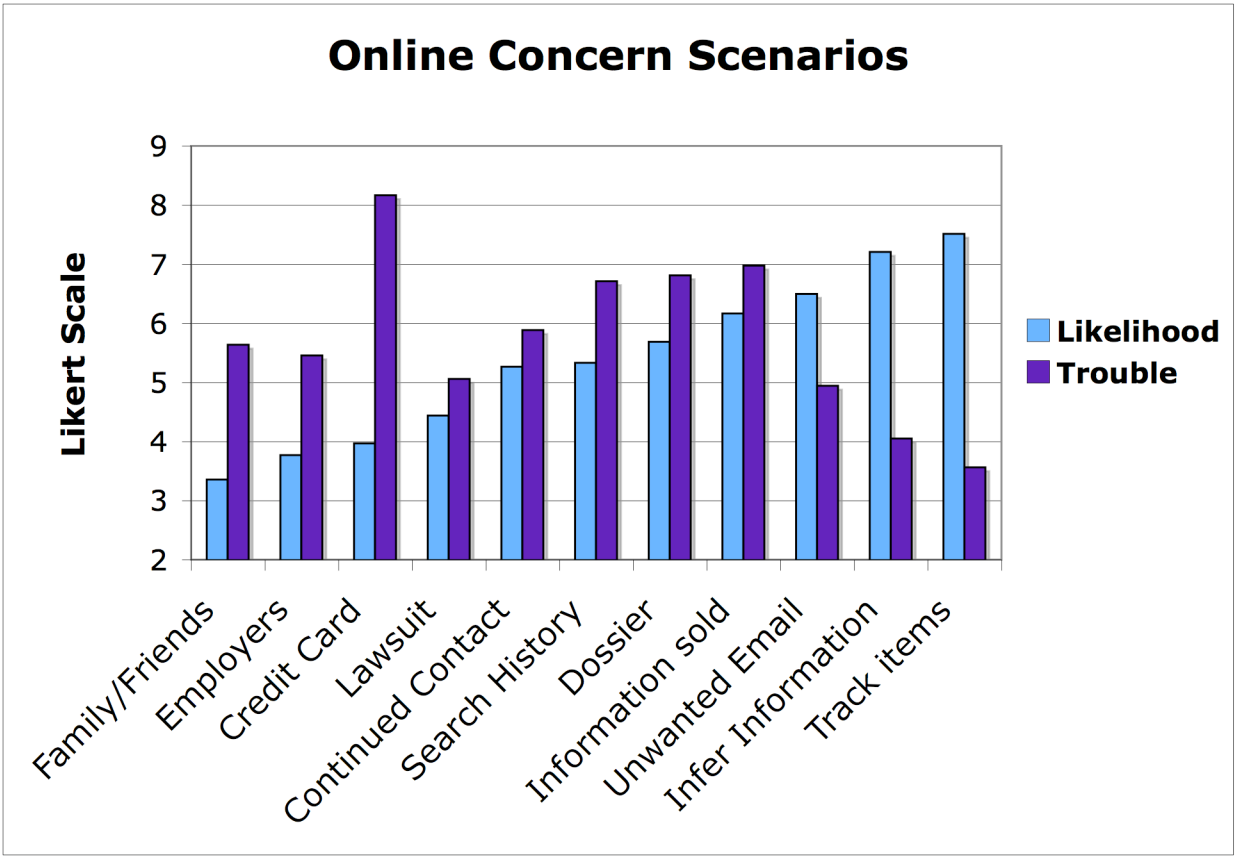

Figure 4: Online Concern Scenarios

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.

Privacy policies, and Privacy Finder, our P3P-enhanded search engine, address the following concerns: continued contact, dossier, information sold, unwanted email, infer information, and track items. These scenarios are also the ones rated with the highest likelihood.

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. 73.8% of respondents who made their last purchase from Amazon.com rated both the tracking of information and the inferring of information with high (greater than a 5 on the Likert scale) likelihood. For the total population, 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), $t(275) = 21.74$, $p < .0001$.

3.8 Components of Privacy Concern

We were interested in how much trouble it would be if certain items of information were publicly available on the Internet. We asked "How much trouble would it cause you if the following information was publicly available on the Internet?" on a scale from zero, "No trouble at all," to 10, "A large amount of trouble." A principle component analysis was conducted on these items, and four components of concern were identified.

- Unconcerned: Public Information
    1. TV show
    2. Favorite snack
    3. Height
    4. Age
    5. Weight
- Low Concern: Contact Information
    1. Name
    2. Home address
    3. Business address
    4. Cell phone number
- Medium Concern: Personal Records
    1. Grocery purchase history
    2. Debt report

3. Medical Records
4. Salary history
5. Bank statement
6. Online purchase history
7. Search term history
8. Tax records
9. Employment history

- High: Highly Sensitive Information
    1. Social Security Number
    2. Credit card number

With the grouping of the items into these four components, 69.7% of the variance in the linear transformation of the components is explained for the original variables. Figure 5 displays the level of concern for our components: the higher the Likert value, the greater the amount of trouble to the participant.

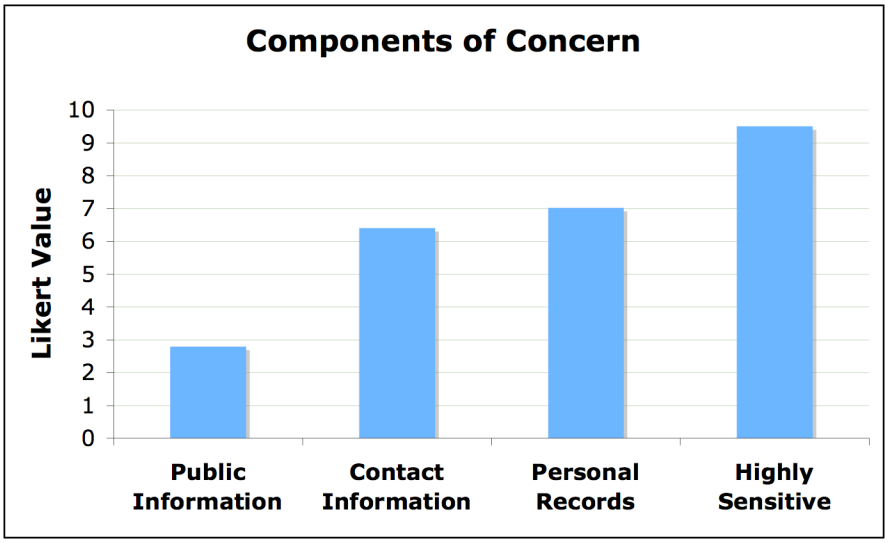

Figure 5: The Components of Concern

Examining our components of concern, we find that people have the highest level of concern or estimated trouble with the public availability of their Social Security number and credit card information, followed by a concern for tax, employment, bank, and medical information. Respondents are slightly less concerned about the release of their contact information, including their home and business addresses, and completely unconcerned about their name, age, weight, favorite snack and favorite television show.

3.9 User Study Insights

To determine what items to have users purchase in our upcoming privacy user study, we posed the following question to our participants,

> 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 response options on a 4-point scale to compute an average purchase likelihood score for each product. Figure 6 includes the list of items presented as well as their purchase likelihood scores.

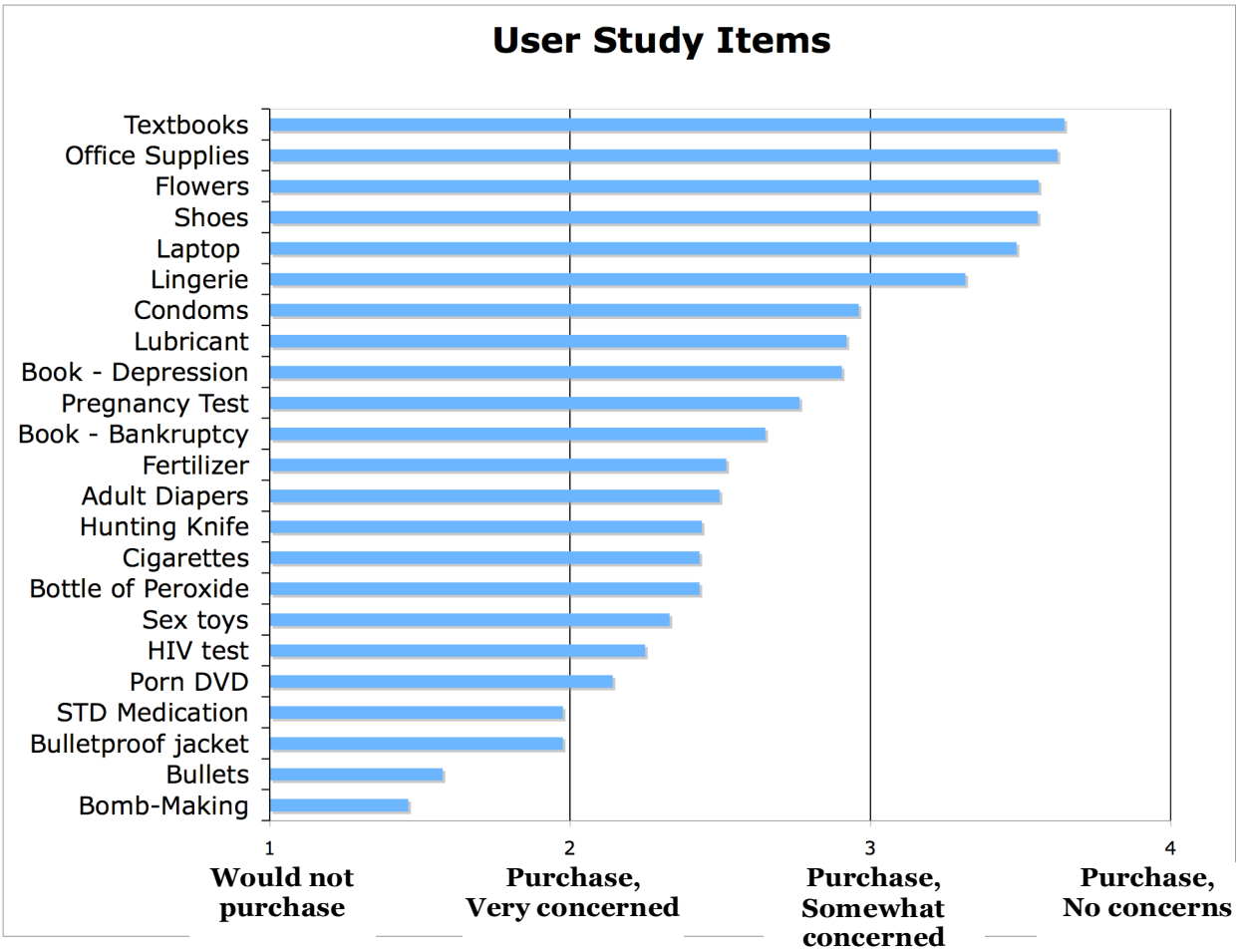

Figure 6: User Study Items, Levels of Privacy-Sensitivity

For common products such as office supplies, there was little hesitance toward buying the product online. As we moved to items that involved personal values and physical state, such

as items related to sex, books related to depression, and adult diapers, we saw increasing hesitance. When the items were indicative of behavior that could be associated with criminals or terrorists, such as a book on making bombs and bullets, we saw very large reservations and reluctance to purchase online.

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 that 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. This makes sense since so many people reported that they bought the last item that they purchased online from Amazon.com. If you register for an Amazon.com account, Amazon recommends similar products to ones you have previous purchased on their main page and in email messages.

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.

Of note was the high percentage of people who were classified as privacy fundamentalists. Our participants were solicited from an online message board, Craigslist, and were very highly educated. This population may have more experiences with privacy violations or a better understanding of what privacy is available online. Despite this high percentage of privacy fundamentalists, there was a varied distribution of risk scores. This indicates that despite people's feelings about their personal control about how their information is collected, how businesses handle this information, and the level of protection provided by laws and organizational practices (asked in the Westin Privacy Segmentation Index), people can still feel lower or higher levels of risk with regards to their personal information. The Westin

classifications may not be applicable for this population. The general knowledge or awareness of information abuse and privacy concerns of the population may have led participants to respond in a way that classify them as privacy fundamentalists, even they do not act in a way that would reflect this classification.

Based on this survey, we see that P3P tools may have a significant impact in helping people find information relevant to their privacy concerns. Our future work includes conducting users studies to examine online purchasing behavior with our Privacy Finder P3P search engine. We hope to find that by lowering the barrier to finding privacy information, people will be able to make better, and more informed decisions regarding their use of their personal information online.

References

Ackerman, M., Cranor, L., and Reagle, J. 1999. Privacy in e-commerce: Examining user scenarios and privacy preferences. *Proceedings of the ACM Conference on Electronic Commerce (EC'99)*, 3-5 November 1999, Denver, Colorado, p. 1-8.

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

Adkinson, W.F., Eisenach, J.A., and Lenard, T.M. 2002. *Privacy online: A report on the information practices and policies of commercial websites*. Progress & Freedom Foundation, Washington, DC. http://www.pff.org/publications/privacyonlinefinalael.pdf.

Antón, A., Earp, Vail, M., Jain, N., Gheen, C., and Frink, J. 2004. *An Analysis of Website Privacy Policy Evolution in the Presence of HIPAA*. North Carolina State University Computer Science Technical Report # TR-2004-21. http://www.theprivacyplace.org/papers/hipaa_7_24_submit.pdf

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

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

Enterprise Privacy Information Centre. 2005. "Public Opinion on Privacy." http://www.epic.org/privacy/survey/default.html.

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

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

Hastie, R. and Dawes R. M. 2001. *Rational Choice in an Uncertain World: The Psychology of Judgement and Decision Making*. Sage Publications.

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

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

Kumaraguru, P., and Cranor, L. 2005. Privacy Indexes: A Survey of Westin's Studies. *Carnegie Mellon University*, December 2005, CMU-ISRI-5-138.

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

Milne, G.R. and Culnan, M.J. 2004. Strategies for Reducing Online Privacy Risks: Why Consumers Read (Or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing* (18)2, 15-29.

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

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

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

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

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