# Usability of User Agents for Privacy-Preference Specification

Robert W. Proctor[1], Kim-Phuong L. Vu[2], and M. Athar Ali[1]

[1] Department of Psychological Sciences, Purdue University
703 Third St., W. Lafayette, IN 47907, USA
[2] Department of Psychology, California State University, Long Beach
1250 N. Bellflower Blvd. Long Beach, CA 90840, USA
proctor@psych.purdue.edu, kvu8@csulb.edu,
athar.ali@perficient.com

**Abstract.** The goal of this study was to determine (a) users' privacy concerns; (b) whether these privacy concerns can be checked by an existing Web-based privacy agent; and (c) whether users are able to easily specify their privacy preferences using this agent. Users were able to configure the agent correctly for about half of the desired privacy goals that could be checked by the agent. Of more significance, users thought that they had configured the agent successfully to achieve many privacy goals that cannot be accomplished with the version tested. We also examined alternative interface layouts to ascertain whether any of them allowed users to specify their preferences at a higher success rate than the current interface. We discuss implications of our findings for user agents designed to aid users' assessments as to whether a Web site's stated privacy practices are consistent with the users' preferences.

**Keywords:** privacy preferences; privacy policies; usability.

## 1 Introduction

In recent years there has been increased interest in protecting users' private information in Web transactions [1]. Surveys show that 75% of users express considerable concern about privacy issues [2, 3], especially when personally identifiable information (e.g., phone numbers and social security numbers) is used. Users are less concerned about providing information about their browsing patterns, and are quite willing to allow their personal information to be saved in order to reduce task-completion times for frequent transactions, as long as they can specify when this information will be released and to whom. Although prior surveys have documented that many users have concerns about privacy with respect to Web-based transactions, they have not provided information as to the specific concerns that users deem to be most important. The goal of our first study was to obtain such information.

Though many Web sites post privacy policies, these policies do not necessarily address consumer privacy concerns and are typically written at a reading level that is too difficult for the general user population [4]. Thus, many users do not even visit

M.J. Smith, G. Salvendy (Eds.): Human Interface, Part II, HCII 2007, LNCS 4558, pp. 766–776, 2007.

privacy policy Web pages when given the opportunity [5, 6]. Even if users visit the privacy-policy page, they may not understand the policy because it is often lengthy and may require as long as half an hour to find and analyze [7]. One solution to this problem is to employ a user agent that checks a site's privacy policy against the user's designated privacy preferences. Success of the user agent depends on the user being able to configure the agent properly. The second goal of the present study, therefore, was to evaluate whether participants can configure an existing user agent to check for a range of specified privacy preferences. We also examined whether alternative wordings for the privacy options in the interface would increase user success rates.

## 2 Study 1

The first study was a survey in which users rated whether they agreed or disagreed with each of 98 statements relating to privacy practices (or preferences). All of the statements were based on privacy practices extracted from existing privacy policies and used terminology common to many existing privacy policies.

### 2.1 Method

**Participants.** 32 students (20 males, 11 females, and one of unidentified gender) from an introductory Psychology class at Purdue University participated for experimental credits. All were experienced computer users.

**Materials.** Participants provided ratings regarding their concerns for the following categories of information, or subject types:

- Personally Identifiable Information (PII)
- Non-Personally Identifiable Information (Non-PII ) / Cookies
- Financial Information FI (FI) / Credit Card Information (CCI)
- Health Information (HI) / Personal Health Information (PHI)
- Privacy Principles (e.g., certification seals)
- Passwords
- E-mail Addresses
- Privacy Preferences
- Information About Children

These subject types were identified by examining privacy policies and conducting content and goal-mining analyses on them [8]. Within each subject type, questions about privacy preferences were modeled along the following categories [9]: Collection (the amount and type of information collected; which organization is collecting the information), Personalization (customization for the individual user or group of users), Notice/Awareness (alerts given to users to let them know that information will be collected or that there is a change in the organization's privacy practices), Transfer (conditions under which information will be exchanged with other parties), Information Storage (where the information will be kept), and Access/Participation (who has permission to view the information). The questions were grouped by subject type. Four versions of the survey were assembled with different orders of the subject types in each. Within a subject type, the questions were kept in the same order in the four survey versions.

**Procedure.** Participants signed up for the survey and were tested individually or as part of a group of up to eight people, depending on the number who signed up for the time slot. Participants were first given an instruction sheet that defined key acronyms commonly found in privacy policies. They were told to make sure that they knew the meaning of each acronym and to refer back to the sheet as needed while answering the survey questions. They then received the survey, which consisted of 98 questions. For each question, each participant was to mark an answer of strongly disagree, disagree, neither agree nor disagree, agree, or strongly agree. For data analysis, these answers were transformed to a 5-point scale, with 5 = 'Strongly agree' and 1 = 'Strongly disagree'. Example statements are listed in Tables 1 and 2.

### 2.2 Results and Discussion

Table 1 shows the 25 statements with which the participants most strongly agreed. The topic with which the participants expressed the most concern was selling or sharing their personal information with other parties. Eight of the nine highest rated concerns involved this issue: Six of the statements were with respect to credit card and financial information, and the remaining two involved personally identifiable information and health information. The other question in the top nine involved the possibility of hackers gaining access to financial and credit card information.

The remaining statements in the top 25 included the following. Users noted that they did not want their e-mail address and username/password to be transferred to an acquiring company. Users also indicated that they wanted to have the option to receive electronic and printed copies of the privacy policies, to see privacy logos on Web pages, and the ability to edit their privacy preferences. They also indicated a desire for anonymous Web browsing.

Users expressed the least concern about the eight items in Table 2. These statements generally indicate that users are relatively unconcerned about cookies or non-personally identifiable information being used to customize their browsing experience, or about buying patterns being recorded or stored when their personal information is not identified. This lack of concern applies particularly to sites at which the user is voluntarily registering or purchasing products. Users also indicated relatively little concern with personally identifiable information being transferred to a company that bought out the company that originally collected the information. Although the participants did not seem very concerned about user profiling, this tendency may be a result of their not being aware of privacy threats associated with profiling and may be restricted to college-student Internet users.

## 3 Study 2

The privacy concerns identified in Study 1 were used to develop the tasks for setting privacy preferences in Study 2. This study was an experiment in which participants were instructed to try to set specific privacy preferences on Privacy Bird$^{TM}$, Beta 1.3. Privacy Bird is a user-agent tool that enables users to filter out, or be warned about, undesirable privacy practices stated in a site's privacy policy. We

**Table 1.** Rank order and mean rating (1 = Strongly Disagree and 5 = Strongly Agree) of the 25 statements with which users most strongly agreed. Asterisk indicates a task that can be configured in Privacy Bird.

| Rank | Privacy Preference | Mean Rating |
|---|---|---|
| 1* | I want the option of refusing to allow a company to share my CCI/FI with 3rd parties and affiliates. | 4.66 |
| 2* | I mind when my CCI/FI is shared with a third party for promotions. | 4.48 |
| 3* | I want the option of refusing to allow a company to share my PII with 3rd parties and affiliates. | 4.38 |
| 4* | I mind when my email address is rented or sold. | 4.34 |
| 5 | I am concerned that hackers may be able access my PII. | 4.24 |
| 6* | I mind when my PII is shared with a third party for promotions. | 4.17 |
| 7 | I want to see privacy logos on the privacy policy Web pages. | 4.17 |
| 8* | I mind when my cookies/non-PI are rented or sold. | 4.10 |
| 9* | I mind when my HI/PHI is shared with a third party for promotions. | 4.10 |
| 10 | I want the option to receive electronic/print privacy policy. | 4.07 |
| 11 | I want the option of having a manual way of editing privacy preferences and a machine readable option. | 4.07 |
| 12 | I mind when my email address is provided to an acquiring company. | 4.03 |
| 13 | I mind when my login/password is transferred to an acquiring company. | 4.00 |
| 14 | I mind that my CCI/FI is aggregated from third parties. | 4.00 |
| 15 | I want the option to restrict the company's employees from viewing my HI/PHI. | 4.00 |
| 16 | I want the option of refusing to allow a company to use cookies/non-PI for promotional purposes. | 3.97 |
| 17 | I mind that my HI/PHI is aggregated from third parties. | 3.93 |
| 18 | I am concerned that hackers can access my email messages. | 3.93 |
| 19* | I mind that I am not allowed to update my CCI/FI. | 3.83 |
| 20 | I mind when my email account is used to monitor my purchase patterns. | 3.79 |
| 21 | I mind when my cookies/non-PI are transferred to an acquiring company. | 3.72 |
| 22* | I mind when my CCI/FI is used to customize my browsing experience. | 3.69 |
| 23* | I mind when my HI/PHI is used to contact me for health or drug promotions. | 3.69 |
| 24 | I mind that I cannot see my cookies/non-PI to verify their accuracy. | 3.62 |
| 25 | I want the option to share my privacy preferences with other Web sites. | 3.62 |

chose Privacy Bird because it is readily available and allows users the option of customizing their privacy preferences. We developed tasks reflecting the top 25 rated privacy concerns in Study 1 (see Table 1), excluding statement 11, because Privacy Bird itself is a tool for setting privacy preferences that uses machine-readable code. We determined that Privacy Bird, if set properly, can warn users if a site's privacy policy does not address any of 10 of the privacy concerns identified in Study 1 (asterisk next to task number in Table 1), but it cannot do so for the remaining 14 concerns. It should be noted, though, that Privacy Bird can check for seven of the top 10 user concerns identified in Study 1.

**Table 2.** Mean rating (1 = Strongly Disagree and 5 = Strongly Agree) of the eight statements with which users most strongly disagreed

| **Privacy Preference** | **Mean Rating** |
|---|---|
| I mind when my PII is used to customize my browsing experience. | 3.38 |
| I mind that my CCI/FI is collected when I purchase products/services. | 3.31 |
| I mind that my HI/PHI is recorded to my profile when I purchase products/services. | 3.31 |
| I mind that I am not allowed to update my HI/PHI. | 3.31 |
| I mind that my PII is collected when I purchase products/services. | 3.24 |
| I mind that my buying patterns are recorded to my profile. | 3.17 |
| I mind that my buying patterns are recorded to my cookies/non-PI. | 3.17 |
| I mind when cookies/non-PI are used to customize my browsing experience. | 3.03 |

### 3.1 Method

**Participants.** 30 new students (9 male, 20 female, and one unidentified) from the same subject pool as in Study 1 participated. Ages ranged from 18 to 21, with mean age of 19 years.

**Apparatus.** Privacy Bird was used for subjects to set specific privacy preferences. The options available for privacy preferences in Privacy Bird can be viewed by selecting “My Preferences” in the main menu and “Privacy” in the sub-menu. The privacy configuration options on this screen are divided into four parts:

1. Health or Medical Information
2. Financial or Purchase Information
3. Personally Identifiable Information
4. Non-Personally Identifiable Information

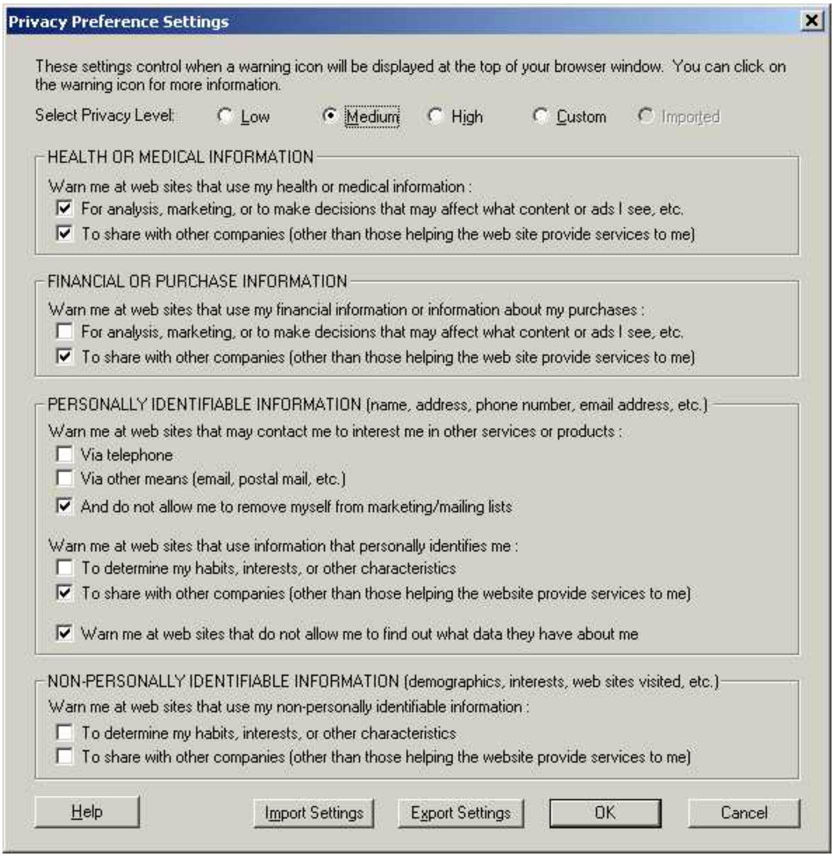
The available privacy preference options are shown in Figure 1.

**Procedure.** Participants were initially required to complete a survey with questions about their Internet usage and experience with privacy tools. The survey asked their age, gender, ethnicity, previous computer experience (from 1 = none to 4 = very experienced), how often they access the Internet (1 = never to 4 = very often), knowledge of Internet privacy policies (1 = none to 4 = very knowledgeable), and experience with privacy tools (1 = none to 4 = very experienced).

For the main study, participants were asked to configure specified privacy preferences using Privacy Bird. Participants were to select appropriate options on the Privacy Bird configuration window accessible through “My Preferences” on the main menu and “Privacy” on the sub menu. The “Select Privacy Level” was set at “Custom” to allow participants to configure the tool.

Participants were provided with a list of 24 tasks. Each task was related to one of the privacy concerns identified in Study 1, and participants had to select options from those available on this screen to indicate the privacy setting needed in Privacy Bird to achieve each task. Because the tasks were developed from the concerns identified in Study 1, the task list consisted of a mixture of tasks that could be completed using the available options in Privacy Bird and tasks that could not be completed. Participants were asked to select the option in Privacy Bird that they felt would achieve the task goal, and they were allowed to select multiple options. After completion of each task, that participant was to say "done." If the participant thought that appropriate options were not available or that the task could not be completed, s/he was to say that the task could not be completed. In such cases, the participant moved on to the next task. The order of the tasks was different for each user.

The screen activities were videotaped during performance of the tasks. The researchers reviewed the tapes to determine the accuracy of participants' performance. A task was considered to be completed (correctly or incorrectly) when the participant said that the task was "done" or "cannot be done". Time taken to complete each task was recorded using the video counter when reviewing the tapes.



Privacy Preference Settings

These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

Select Privacy Level: ○ Low ● Medium ○ High ○ Custom ○ Imported

HEALTH OR MEDICAL INFORMATION

Warn me at web sites that use my health or medical information :

☑ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.

☑ To share with other companies (other than those helping the web site provide services to me)

FINANCIAL OR PURCHASE INFORMATION

Warn me at web sites that use my financial information or information about my purchases :

□ For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.

☑ To share with other companies (other than those helping the web site provide services to me)

PERSONALLY IDENTIFIABLE INFORMATION (name, address, phone number, email address, etc.)

Warn me at web sites that may contact me to interest me in other services or products :

□ Via telephone

□ Via other means (email, postal mail, etc.)

☑ And do not allow me to remove myself from marketing/mailing lists

Warn me at web sites that use information that personally identifies me :

□ To determine my habits, interests, or other characteristics

☑ To share with other companies (other than those helping the website provide services to me)

☑ Warn me at web sites that do not allow me to find out what data they have about me

NON-PERSONALLY IDENTIFIABLE INFORMATION (demographics, interests, web sites visited, etc.)

Warn me at web sites that use my non-personally identifiable information :

□ To determine my habits, interests, or other characteristics

□ To share with other companies (other than those helping the website provide services to me)

**Fig. 1.** The privacy preference options in Privacy Bird. Reprinted with permission.

## 3.2 Results and Discussion

**Survey.** All participants indicated that they had some previous computer experience, with 4 indicating that they were not very experienced, 20 fairly experienced, and 6 very experienced. All had access to the Internet, with 2 indicating that they accessed the Internet not very often, 7 often, and 21 very often. One participant indicated no knowledge of privacy policies, 18 that they were not very knowledgeable, and 11 that they were fairly knowledgeable. Three indicated that they had no experience with privacy tools, 22 very little experience, 4 a fair amount of experience, and 1 a lot of experience. In sum, the participants were relatively experienced with computers and using the Internet but not very knowledgeable about privacy policies and tools.

**Performance with Privacy Bird.** A configuration was considered correct if the participant selected the right settings for the tasks that could be configured, and said that the configuration cannot be set for the tasks that could not be configured. There was no difference in time to complete configurable ($M = 23.3$ s) and non-configurable ($M = 20.7$ s) tasks, $t(29) = 1.19$, $p > .24$. The percent correct was 66% for the 10 tasks that could be configured and 31% for the 14 tasks that could not be configured. For the tasks that could be configured, Table 3 shows the total number of errors for which participants responded “can’t be configured” and for which they provided an incorrect configuration. The frequency of incorrect configurations was greater than that of non-configurations, $\chi^2(1) = 15.75$, $p < .001$, indicating that participants often thought they had set Privacy Bird appropriately when they had not. There was an interaction of this effect with task, $\chi^2(9) = 22.85$, $p < .01$, with 8 of the tasks showing more incorrect configurations than cannot-be-configured errors.

The three most popular erroneous settings for the tasks that could be configured were users selecting one or the other setting for Financial Information and the second setting for Personally Identifiable Information. These same settings were three of the four most frequently used for those tasks that could not be configured. The fifth setting of Personally Identifiable Information was the other frequently used setting.

**Table 3.** Total Number of Incorrect Configurations for Each of the 10 Tasks for which Privacy Bird could be Configured, and the Numbers of “Cannot be Configured” and Incorrect Configurations. *The task numbers correspond to the privacy concerns ranked in Table 1.

| Task* | Total Incorrect | Cannot be Configured | Incorrect Configuration |
|---|---|---|---|
| 1 | 9 | 1 | 8 |
| 2 | 9 | 2 | 7 |
| 3 | 8 | 0 | 8 |
| 4 | 14 | 5 | 9 |
| 6 | 10 | 3 | 7 |
| 8 | 9 | 3 | 6 |
| 9 | 8 | 0 | 8 |
| 19 | 22 | 6 | 16 |
| 22 | 6 | 3 | 3 |
| 23 | 17 | 12 | 5 |

## 4 Study 3: Usability Testing for Alternative Interfaces

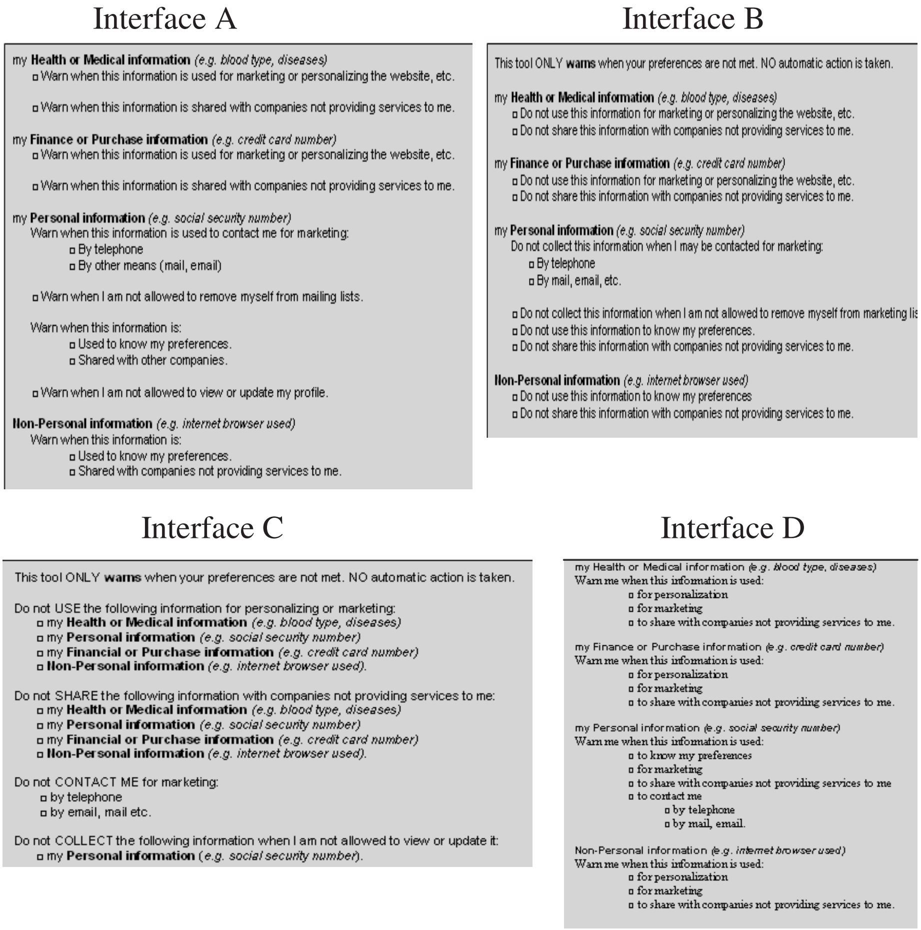
Performance at setting Privacy Bird to address specific privacy concerns was not particularly good in Study 2. Participants' responses were incorrect for approximately 50% of the tasks they were asked to perform. Participants often thought that they had set Privacy Bird to accomplish goals that it could not and did not set it appropriately to accomplish goals that it could. Study 3 was designed to determine whether performance could be improved using alternative presentations for specifying privacy preferences on the Privacy Bird interface that used simple organizational or wording changes.

### 4.1 Method

**Participants.** 100 new students from the same subject pool as the previous studies participated.

**Materials.** Paper versions of four alternatives to the Privacy Bird interface were tested (see Figure 2), along with one that resembled the original Privacy Bird interface (Interface E). Interface A was similar to the Privacy Bird interface, with the main difference being that the names of all information types except non-personally identified information were prefixed with "my" to indicate that the information type is personal. For Interface B, the words "warn me" in the original interface were replaced with "DO NOT" to indicate an action verb. This interface's heading warns that the tool does not take any automatic action and only "warns". For Interface C, the options were categorized based on the action verb. Action verbs provided on the interface were USE, SHARE, CONTACT, and COLLECT. Within each action verb, options were categorized using the type of information such as financial or health. Again, personal information was prefixed with "my." For Interface D, the original options in the Privacy Bird interface were subdivided to provide more options. Thus, certain privacy preferences that were originally grouped together as one option in Privacy Bird were available as separate options. Under each category of information type, the sentence began with "warn me when…", but the options themselves did not have "warn me" written before them. Examples of the information types were provided, and some words were simplified from the original Privacy Bird interface.

**Procedure.** Participants were randomly assigned to receive one of the five paper versions of the Privacy Bird interface. Each of the interface versions had a list of 10 tasks to be completed in sequence with the interface sheet. The tasks were those from Study 2 that could be accomplished with appropriate settings of the interface. Participants were instructed to read each task in the list and select the options necessary to set the indicated privacy preference. The options were then to be noted alongside the task. If the participant felt that the options were not sufficient and that



Interface A

my **Health or Medical information** *(e.g. blood type, diseases)*
□ Warn when this information is used for marketing or personalizing the website, etc.
□ Warn when this information is shared with companies not providing services to me.

my **Finance or Purchase information** *(e.g. credit card number)*
□ Warn when this information is used for marketing or personalizing the website, etc.
□ Warn when this information is shared with companies not providing services to me.

my **Personal information** *(e.g. social security number)*
Warn when this information is used to contact me for marketing:
□ By telephone
□ By other means (mail, email)

□ Warn when I am not allowed to remove myself from mailing lists.

Warn when this information is:
□ Used to know my preferences.
□ Shared with other companies.

□ Warn when I am not allowed to view or update my profile.

**Non-Personal information** *(e.g. internet browser used)*
Warn when this information is:
□ Used to know my preferences.
□ Shared with companies not providing services to me.

Interface B

This tool ONLY **warns** when your preferences are not met. NO automatic action is taken.

my **Health or Medical information** *(e.g. blood type, diseases)*
□ Do not use this information for marketing or personalizing the website, etc.
□ Do not share this information with companies not providing services to me.

my **Finance or Purchase information** *(e.g. credit card number)*
□ Do not use this information for marketing or personalizing the website, etc.
□ Do not share this information with companies not providing services to me.

my **Personal information** *(e.g. social security number)*
Do not collect this information when I may be contacted for marketing:
□ By telephone
□ By mail, email, etc.

□ Do not collect this information when I am not allowed to remove myself from marketing lis
□ Do not use this information to know my preferences.
□ Do not share this information with companies not providing services to me.

**Non-Personal information** *(e.g. internet browser used)*
□ Do not use this information to know my preferences
□ Do not share this information with companies not providing services to me.

Interface C

This tool ONLY **warns** when your preferences are not met. NO automatic action is taken.

Do not USE the following information for personalizing or marketing:
□ my **Health or Medical information** *(e.g. blood type, diseases)*
□ my **Personal information** *(e.g. social security number)*
□ my **Financial or Purchase information** *(e.g. credit card number)*
□ **Non-Personal information** *(e.g. internet browser used).*

Do not SHARE the following information with companies not providing services to me:
□ my **Health or Medical information** *(e.g. blood type, diseases)*
□ my **Personal information** *(e.g. social security number)*
□ my **Financial or Purchase information** *(e.g. credit card number)*
□ **Non-Personal information** *(e.g. internet browser used).*

Do not CONTACT ME for marketing:
□ by telephone
□ by email, mail etc.

Do not COLLECT the following information when I am not allowed to view or update it:
□ my **Personal information** (*e.g. social security number*).

Interface D

my Health or Medical information *(e.g. blood type, diseases)*
Warn me when this information is used:
□ for personalization
□ for marketing
□ to share with companies not providing services to me.

my Finance or Purchase information *(e.g. credit card number)*
Warn me when this information is used:
□ for personalization
□ for marketing
□ to share with companies not providing services to me.

my Personal information *(e.g. social security number)*
Warn me when this information is used:
□ to know my preferences
□ for marketing
□ to share with companies not providing services to me
□ to contact me
□ by telephone
□ by mail, email.

Non-Personal information *(e.g. internet browser used)*
Warn me when this information is used:
□ for personalization
□ for marketing
□ to share with companies not providing services to me.

**Fig. 2.** The four modified versions of the Privacy Bird interface used in Study 3

the settings could not be completed, then s/he would write NA (for Not Applicable) alongside the task.

### 4.2 Results and Discussion

Across the five interfaces and 10 questions, the correct option was selected 54% of the time, including configurations for which additional options were also selected. Though the percent correct was highest for interface A (60%), lowest for interfaces E (the original Privacy Bird interface; 51%), B (52%), and D (52%), and intermediate for interface C (57%), an ANOVA indicated no significant difference, $F < 1.0$. Because interface A was the most similar to the Privacy Bird interface (interface E), it is likely that the higher percentage correct for it is due to sampling error. Regardless of whether there is indeed a small, real difference across the tested interfaces, it is clear that the relatively simple changes we made in organization and wording did not make much difference. Sizeable improvement in task performance apparently would require more than just surface changes to the Privacy Bird interface.

## 5 Conclusion

The privacy issue that users indicated to be of most concern in Study 1 was selling or sharing information with other parties. They also specified concern about hackers possibly gaining access to their financial information and with their e-mail addresses and username/passwords being transferred to an acquiring company. Users also indicated that they wanted a manual way of editing privacy preferences, which Privacy Bird is designed to do. Privacy Bird includes options that can address 7 of the 10 top privacy concerns endorsed by the users in Study 1. However, users showed evidence of confusion regarding exactly what they will be warned about with the various settings of Privacy Bird, both with the original interface and variations of it. For the privacy concerns that could be accommodated by Privacy Bird, users set the interface correctly only about 60% of the time, and they often thought that they had set Privacy Bird to provide protection that it could not provide. Thus, Privacy Bird provides a good start toward allowing users to determine whether Web sites adhere to their privacy preferences. However, because experienced computer users with little knowledge of online privacy issues show confusion about what can be accomplished with particular settings, it may be more effective users to rely on the default values (low, medium, or high privacy) rather than on custom settings of the user agent.

## Acknowledgments

This research was supported in part by NSF ITR Cyber Trust grant #0430274.

## References

1. Cranor, L.F., Garfinkel, F.: Security and usability: Designing secure systems that people can use. O’Reilly Media, Inc., Sebastopol, CA (2005)
2. Ackerman, M.S., Cranor, L.F., Reagle, J.: Privacy in E-commerce: Examining user scenarios and privacy preferences. In: E-commerce 99, pp. 1–8. ACM, New York (1999)
3. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd generation E-commerce: Privacy preferences versus behavior. In: EC’01, pp. 38–47. ACM, New York (2001)
4. Proctor, R.W., Ali, M.A., Vu, K.-P.L.: Examining usability of Web privacy policies. International Journal of Human-Computer Interaction (in press)
5. Earp, J.B., Baumer, D.: Innovative Web use to learn about consumer behavior and online privacy. Communications of the ACM 46(4), 81–83 (2003)
6. Jensen, C., Potts, J.: Privacy policies as decision-making tools: An Evaluation of online privacy notices. In: CHI 2004, vol. 6, pp. 471–478 (2004)

7. Byers, S., Cranor, L.F., Kormann, D.: Automated analysis of P3P-enabled Web sites. In: ICES, Pittsburgh, PA, pp. 326–338 (2003)
8. Antón, A.I., Earp, J.B., He, Q., Stufflebeam, W., Bolchini, D., Jensen, C.: The lack of clarity in financial privacy policies and the need for standardization. IEEE Security and Privacy 2(2), 36–45 (2004)
9. Earp, J.B., Anton, A.I., Aiman-Smith, L., Stufflebeam, W.H.: Examining Internet privacy policies within the context of user privacy values. IEEE Transactions on Engineering Management 52, 227–237 (2005)