Behavior Research Methods
2007, 39 (2), 205-211

A multimethod approach to examining usability of Web privacy polices and user agents for specifying privacy preferences

ROBERT W. PROCTOR
Purdue University, West Lafayette, Indiana

AND

KIM-PHUONG L. VU
California State University, Long Beach, California

Because all research methods have strengths and weaknesses, a multimethod approach often provides the best way to understand human behavior in applied settings. We describe how a multimethod approach was employed in a series of studies designed to examine usability issues associated with two aspects of online privacy: comprehension of privacy policies and configuration of privacy preferences for an online user agent. Archival research, user surveys, data mining, quantitative observations, and controlled experiments each yielded unique findings that, together, contributed to increased understanding of online-privacy issues for users. These findings were used to evaluate the accessibility of Web privacy policies to computer-literate users, determine whether people can configure user agents to achieve specific privacy goals, and discover ways in which the usability of those agents can be improved.

Researchers in basic and applied psychology often emphasize different research methods in their work (Aaronson, 1994; Hoc, 2001). Researchers in basic psychology rely on experiments as the primary method for investigating psychological phenomena, because of the control and consequently higher internal validity that experiments allow. In contrast, researchers in applied psychology frequently use nonexperimental methods because of their greater ecological validity. Within each approach, a variety of specific methods can be employed (Zhu, Vu, & Proctor, 2005). Because the alternative methods have different strengths and weaknesses, a multimethod approach often provides the best way to understand human behavior in applied settings (Eid & Diener, 2006; Proctor & Capaldi, 2006). According to Eid and Diener (2006), "a multimethod approach offers insights into scientific phenomena and can contribute to confirming psychological theories in a way a single-method approach cannot" (p. 3).

The goal of the present article is to illustrate how a multimethod approach can provide insights into the design and performance of human computing tasks, specifically in the context of information privacy. With the advent of the Internet and the World-Wide Web, security and privacy of information have become topics of considerable concern to organizations and users of the services that the organizations provide (Cranor & Garfinkel, 2005). As one example of the level of current interest in information security and privacy, the National Science Foundation (NSF) founded the Cyber Trust program earlier in this decade to support research on security and privacy issues. As described by the NSF (2005), this program

> promotes a vision of a society in which networked computer systems are:
>
> - more predictable, more accountable, and less vulnerable to attack and abuse;
> - developed, configured, operated, and evaluated by a well-trained and diverse workforce; and
> - used by a public educated in the secure and ethical operation of such systems.

Because research in the area of information security and privacy involves expansion of the basic knowledge base in computer science and human–computer interaction (HCI) and application of this knowledge to improve the security and privacy provided by actual networked computer systems, it is ideally suited to a multimethod approach.

Usability is an important aspect of information security and privacy because of the reliance of security and privacy measures on appropriate and efficient interactions of humans with computers (Proctor, Schultz, & Vu, in press). For example, the protection provided by the standard username–password combination for user identification and authentication is reduced when users adopt bad security practices, such as writing down their passwords or selecting passwords that are easy for others to guess (Vu et al., 2007). Furthermore, stronger identifi-

R. W. Proctor, proctor@psych.purdue.edu

cation and authentication methods, such as biometric and token devices, are not widely adopted because users find them more intrusive and difficult to use than passwords (Schultz, Proctor, Lien, & Salvendy, 2001). Solutions to these types of usability problems require a multimethod approach.

We recently have employed a multimethod approach to examine usability issues associated with two aspects of online privacy, a term that refers to the practices that an organization hosting a Web site follows (or states that it follows in its privacy policy) to protect users' personally identifiable information. The first aspect concerns the information that Web sites of various types collect, and what these organizations' privacy policies state that they do with this information. Of particular concern is whether users can comprehend an organization's stated privacy practices by reading its posted privacy policy (Proctor, Ali, & Vu, in press). The second aspect concerns the usability of user agents designed to automatically detect and warn users when a privacy policy is not consistent with their preferences (Proctor, Vu, & Ali, 2007). Can users configure the user agent to accommodate specific concerns that they may have?

This article is intended primarily to demonstrate the value of employing a multimethod approach to research. As a result, we focus on the unique contributions of the different research methods, both qualitative and quantitative, that we used to examine online privacy. We summarize key features of the specific methods and results; readers interested in more detail are referred to the complete published reports of these studies (Proctor, Ali, & Vu, in press; Proctor et al., 2007). Our intent is to illustrate how the results obtained with the different methods complement each other and thus increase our understanding of (1) user privacy concerns, (2) factors that influence the comprehensibility of privacy policies, and (3) the usability of privacy-specification user agents.

Usability of Web Privacy Policies

Many Web sites collect personally identifiable information about users who visit the sites (Jensen & Potts, 2004). Violations of privacy are now routinely reported in the news media. For example, a former employee of America Online sold the names and e-mail addresses of 92 million customers to an online gambling site, which then sold this information to other organizations (Oates, 2005). Due to breaches of privacy like this, users have become increasingly concerned about protecting their privacy.

The Web sites of many organizations now post privacy policies. These policies are intended to provide users with information about what types of data are collected by the organization, how that information is stored, shared, and transferred, and so forth (see, e.g., Adkinson, Eisenach, & Lenard, 2002). It should be noted, however, that a privacy policy describes the policy an organization intends to practice and not necessarily what it actually does (Moores & Dhillon, 2003). Moreover, several studies have suggested that privacy policies are complicated and may not convey critical information clearly to the users. Partly because of the complexity of the privacy policies, most users do not even visit the privacy policy sections of the Web sites (see, e.g., Jensen & Potts, 2004).

To help convey that an organization follows good privacy practices, several certification programs have been established that allow a Web site to post a privacy certification seal if the privacy policy of the site's host satisfies several basic principles (Moores & Dhillon, 2003). Among the most widely used certification programs is that of the TRUSTe Privacy Program. The TRUSTe seal can be displayed if an organization's privacy policy describes any personally identifiable information that is being collected, the means by which this is done, and whether and how that information is shared with third parties. Although the presence of a privacy seal at a Web site does not guarantee that the organization follows good privacy practices, it does provide users with a quick way of determining whether a site purports to adhere to basic privacy practices.

The purpose of the first study in our investigation (Proctor, Ali, & Vu, in press, Study 1) was to determine what personal information is collected by Web sites that fall into different categories and what features these sites include to assure users that they follow good privacy practices. In this study, we used archival research (Simonton, 2000), in which written records are analyzed, as our method. In this case, six Web sites within each of seven categories (financial, insurance, gaming, pharmaceutical, retail, technology, travel) in which users conducted online transactions involving personal information were selected for analysis. We selected these sites and categories on the basis of their popularity, determined by Alexa.com's and Ranking.com's rankings of the amount of traffic at their sites. We recorded the types and amounts of information about users collected by the sites (e-mail address, social security number, gender, driver's license number, passport number, credit card number, personal password security question, employment information, and financial information), as well as whether the sites posted privacy policies and displayed privacy or security logos.

This method allowed us to obtain data regarding which types of sites requested the most information, whether there was much consistency within and between Web site categories, and what privacy information was posted by each site. Major findings include that (1) financial sites requested the largest amount of personal information, 28 pieces on average; (2) considerable differences existed within and between categories with respect to the type and amount of information requested; (3) 80% or more of the sites in all categories had links to the site's privacy policy (except online gaming; only one of the six online game sites had a policy posted); (4) only 50% of the sites displayed a privacy certification seal.

It is not surprising that financial sites requested more personal information than did sites in the other categories, since financial sites have the highest stake in user transactions. However, when we examined the consistency of the personal information requested from different Web sites in the financial category, we found that only 56% of

the items were requested by a majority of the sites. The variability in the amount of information requested across financial sites, as well as within the other categories of sites, suggests that some sites collect more information than is needed to provide the service requested by the user. In addition, this study shows that although privacy policies were available for most of the sites, many sites did not provide privacy certification seals that could assure users that the site was following good practices.

In the next study (Proctor, Ali, & Vu, in press, Study 2), we used a form of data mining to analyze the content of privacy policies from 100 sites, 25 within each of the four most popular categories (financial, insurance, pharmaceutical, and retail). Although data mining can be defined in different ways, one definition is that it is "'an essential process where intelligent methods are applied in order to extract data patterns' [Han & Kamber, 2001, p. 7] after the data are cleaned, integrated, selected, and transformed" (Hwang, 2006, p. 3077). In Study 2, goal mining, which is a technique for extracting policy goals by application of goal-based requirements methods (Antón et al., 2004), was performed on each privacy policy.

Various privacy goals in the policies (e.g., protecting credit card information) were identified and classified as involving protection (user privacy rights protections) or vulnerability (practices that threaten consumer privacy); see Antón et al. (2004). The policies tended to be either high in both protection and vulnerability goals or low in both. Pharmaceutical sites' policies contained fewer total goals than did the policies of sites in the other categories. The number of privacy goals stated in a policy increased as a function of policy length, and many policies were so long that readers could not reasonably be expected to read them in their entirety. We conducted an analysis of the readability of the policies by calculating a Flesch Reading Ease Score (FRES; Flesch, 1949) and Flesch Grade Level (FGL) for each policy. These scores provide metrics of readability based on word length and sentence length. For example, the formula for FGL is $[(0.39 \times \text{ASL}) + (11.8 \times \text{ASW}) - 15.59]$, where ASL is the average sentence length and ASW is the average number of syllables per word. The readability analysis confirmed previous reports (Jensen & Potts, 2004) that the average privacy policy is written at a level that requires a minimum of 13 years of education (i.e., at least 1 year of college) to be readable.

Four privacy policies that were written at a college freshman reading level were selected for further investigation. Two of the policies were low in both protection and vulnerability goals, and two were high in both, with one policy of each type being from the financial and retail categories. We performed a more detailed content analysis of these policies using the Internet General Inquirer (Stone, Dunphy, Smith, & Ogilvie, 1966; available at www.webuse.umd.edu:9090/), a Web-based content analysis program, to examine the types of words used (e.g., positive, negative, legal). The policies emphasized positive statements about privacy, with positive words making up about 8% of the total words and negative words only about 1%. Policy A, which was the shortest, achieved its short length mainly by having a much smaller number (29) and percentage (5.7%) of positive words than the other policies, although it had approximately the same percentage of negative words (1.2%, or 6). Policy D, which was also low on protection and privacy goals and therefore short, had a much higher number of positive words (109) than Policy A, with the percentage (8.3%) being the second highest of the four policies; its percentage of negative words was low (0.7%, or 9). The two longer policies, B and C, which were high on both privacy and protection goals, also included high numbers of positive words (10.5%, or 171, and 6.3%, or 132, respectively) and approximately twice the percentage of words relating to human aspects compared with policies A and D (4.4% and 3.9% for policies B and C, respectively; 2.5% and 2.2% for policies A and D, respectively).

These four privacy policies were used as materials in a final study (Proctor, Ali, & Vu, in press, Study 3) that employed the experimental method to determine whether undergraduate students, who were at or beyond the college freshman reading level at which these policies were written, had difficulty comprehending the policies. Difficulty in comprehension might be expected, since the policies use terminology that may not be familiar to most readers, an aspect of readability not measured by the FRES and FGL. Participants read a policy and answered multiple-choice questions about its content and their preferences concerning specific features of the policy before proceeding to the next policy. The order in which the policies were read was counterbalanced across participants.

Only 50% of the content questions were answered correctly, with accuracy being no better for the policies that included few privacy goals than for those that included many goals. However, participants indicated that they perceived the shorter policies, with fewer stated goals, as providing less privacy assurance than the longer policies. Also, although the two shortest policies were judged to be less redundant than the two longer ones, one of the short policies (Policy A), which had by far the fewest positive words, was rated as the least clear of the four policies. Thus brevity does not ensure clarity.

Specifying Users' Privacy Preferences

Previous surveys have provided evidence that many users have trepidation with regard to the privacy of Web-based transactions (Spiekermann, Grossklags, & Berendt, 2001), but those surveys did not provide information about which specific concerns are most important to users. Our first study in this series (Proctor et al., 2007, Study 1) sought to address this shortcoming by examining privacy preferences among undergraduates. We asked undergraduate students to complete a survey in which they rated their disagreement or agreement (on a scale of 1 to 5) with each of 98 statements pertaining to current privacy practices. Ten of the statements are provided as examples in Table 1. The survey statements used terminology identified in our previous analyses of the content of privacy policies, and participants were allowed to refer to an instruction sheet that defined key acronyms and terms commonly found in the policies (e.g., PII for personally

Table 1
Rank Order and Mean Rating (1 = *strongly disagree*; 5 = *strongly agree*) of the 10 Statements With Which Users Most Strongly Agreed

Rank	Statement	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 to 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/nonPI 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

Note—An asterisk indicates a task that can be configured in Privacy Bird. CCI, credit card information; FI, financial information; HI, health information; PI, personal information; PHI, personal history information; PII, personally identifiable information.

identifiable information, CCI for credit card information, HI for health information, etc.). The statements referred to several categories of information: personally identifiable information, nonpersonally identifiable information (e.g., cookies), privacy principles, privacy preferences, passwords, financial and credit card information, health information, and e-mail addresses.

The 10 statements shown in Table 1 received the highest average ratings. Participants indicated that they had the most concern about sharing credit card and financial information with third parties and affiliates of an organization and about an organization's sharing or selling the users' personally identifiable information to other parties (or allowing unauthorized access to that information). Participants also answered that they did not want their cookies or nonpersonally identifiable information to be rented or sold, did not want their e-mail addresses and usernames/passwords to be transferred to an acquiring company, and did want to see privacy logos on Web pages. This group of participants did not express much concern about Web sites' collecting profiling information, but this may be because college students may not be aware of privacy threats associated with profiling.

One of the top 25 privacy issues for the participants was whether sites provided users with a way to edit privacy preferences and a machine-readable option for checking the adherence of Web sites to specified privacy preferences. Several user–agent tools exist that are intended to satisfy this concern (e.g., Privacy Bird, Privacy Companion, and P3P Proxy). These tools determine whether a site departs from a user's preferences by comparing the user's preferences to a platform for privacy preferences (P3P) representation of the privacy policy in a machine-readable extensible markup language (XML) format.

One of the most popular of these tools is Privacy Bird, a user–agent tool that provides users with a visual cue that indicates the degree to which a site's privacy policy matches the user's preferences (Cranor, Guduru, & Arjula, 2006). A green bird indicates that the site's privacy policy conforms to the user's specified preferences; a yellow bird indicates that Privacy Bird was unable to compare the specified preferences with a policy for the site (i.e., it was unable to retrieve a privacy policy for the site); and a red bird appears when the posted privacy policy does not match the user's preference settings. To use the tool, a user must open a privacy preferences settings window, like the one shown in Figure 1, and either select default options of low, medium, or high privacy or customize his or her privacy specifications. Customization requires selecting options organized within four categories: (1) health or medical information, (2) financial or purchase information, (3) personally identified information, and (4) nonpersonally identified information.

One question of interest is whether Privacy Bird allows users to configure preference settings that can address the remaining top 24 privacy concerns indicated by participants in the previously described privacy survey. We performed an evaluation of Privacy Bird's capabilities and found that it could be set to accommodate 7 of the top 10 concerns, but only 3 of the remaining 14 concerns.

Privacy Bird warns users of potential privacy threats to their preferences only if it is configured correctly. Thus, an important question is whether the privacy preferences settings interface is intuitive to users. To examine whether users can set the 10 privacy preferences correctly and then realize that the remaining privacy concerns cannot be addressed through any of the preference settings, we conducted a laboratory study in which undergraduate students were instructed to try to configure specific privacy preferences in Privacy Bird, version Beta 1.3, for tasks corresponding to each of the 24 major privacy concerns (Proctor, Vu, & Ali, 2007, Study 2). For example, one task was to set the privacy preference so that personally identifiable information would not be shared with third parties for promotions.

Participants averaged 65% correctness in configuring the settings of Privacy Bird appropriately for the 10 tasks that Privacy Bird was capable of addressing. A more serious finding, however, was that for tasks that could not be accomplished by any preference configuration made available through Privacy Bird, participants nonetheless thought that they had configured appropriate settings 70%

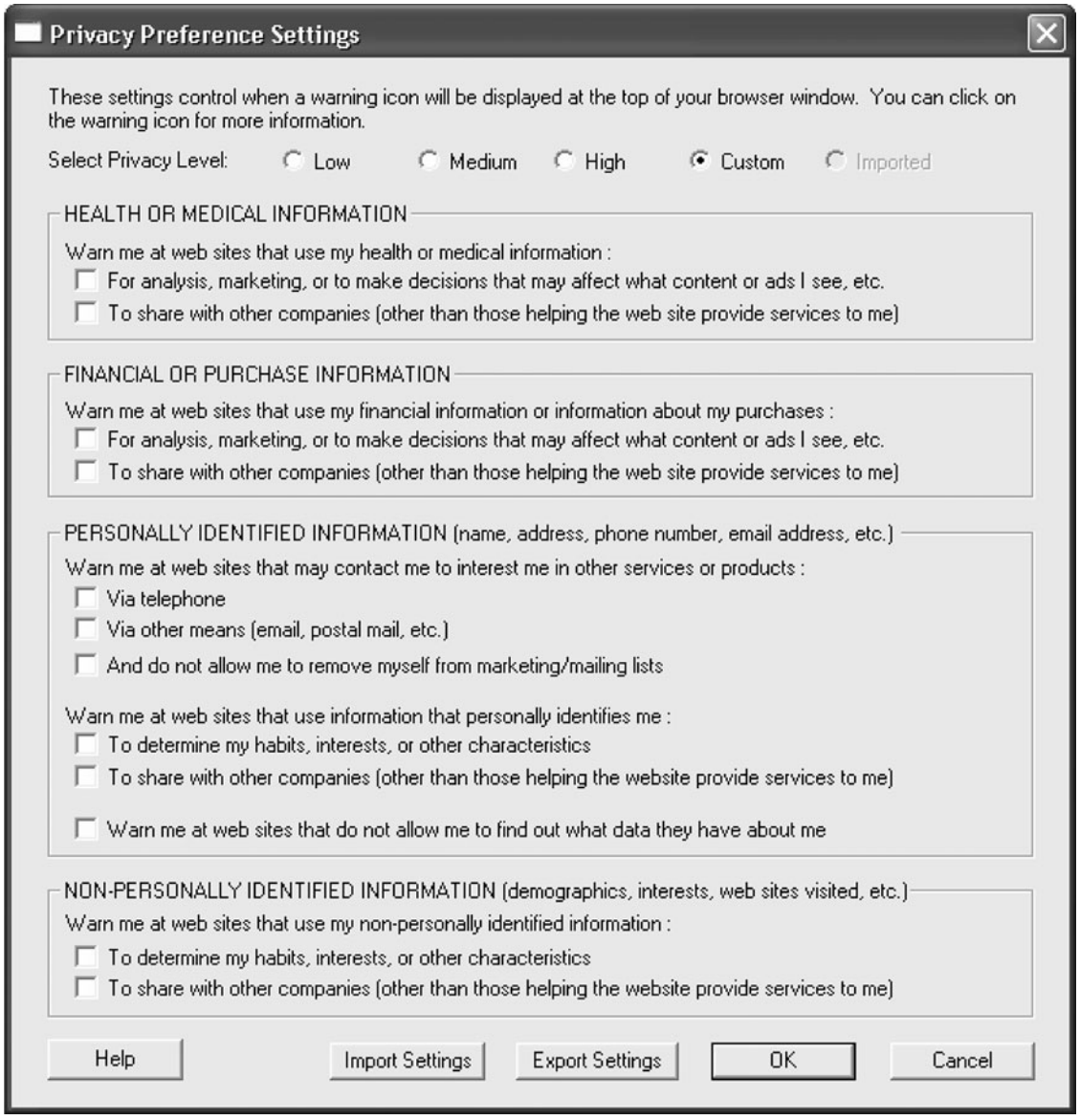

Figure 1. Screen shot for custom setting of the Privacy Bird interface.

of the time. Thus, users who routinely use the Web and are relatively knowledgeable about computers exhibited considerable uncertainty about the protection provided by particular settings of Privacy Bird. This finding indicates that users knowledgeable about computers and the Web in general may not be knowledgeable about how to set privacy specifications.

In a final study (Proctor et al., 2007, Study 3), we evaluated whether preference-setting performance could be improved by altering the presentation of the options to make Privacy Bird's capabilities more obvious to users. For these studies, we employed the experimental method, using paper mock-up versions of alternative interfaces that contained minor changes of wording and organization from the originals. The mock-ups were used as a simple way to evaluate the impact of different presentations of the same privacy specification features on the usability of the interface. We manipulated the groupings of privacy features and the wordings of specific features in ways that could potentially benefit performance.

Interface A was similar to that of Privacy Bird's own interface, except that the word "my" was added before the health, financial, and personal information categories to indicate that the information being collected was personal. For Interface B, the words "warn me" in the Privacy Bird interface were replaced with the words "DO NOT" to indicate that an action should be taken by Privacy Bird. Also, examples of each type of information (health, financial, or personal) were provided for more clarity. For Interface C, the options were grouped into different categories that used four action verbs ("use," "share," "contact," and "collect") to describe how the information would be used. Within

each verb category, options were distinguished by the type of information being collected. As in Interface A, health, financial, and personal information was prefixed with the word "my" in Interface C. For Interface D, the options in Privacy Bird's interface were subdivided to make the categories more obvious. Under each category of information type, the sentence began with the words "warn me when . . . ," but the options themselves did not have "warn me when" written before each of them. User preferences for the different interfaces were also obtained.

Participants rated Interface C, which used the action verb organization, as easiest to use and Interface B, which used "do not," as the most difficult. However, there were no significant differences among the participants' performances with the four interfaces, with the settings for all of them being at a level of accuracy similar to that for a paper version of the Privacy Bird interface. Thus, simple changes in wording and organization were not sufficient to improve participants' performance substantially. An implication of this study is that improvements in usability will require more transparent mappings of specific privacy preferences to interface options so that users will not be confused about which violations of their privacy preferences will trigger a warning.

Conclusion

In applied areas of research, such as human–computer interaction, it is most beneficial to use a multimethod approach to increase our understanding of various issues as well as to develop solutions to specific problems. In the studies that we have described, each method used yielded unique information that increased our understanding of user privacy concerns, and this information was used to determine whether user agents for specifying privacy preferences can achieve the goals of users and have usable interfaces.

Analyses of the information requested by Web sites in different categories revealed not only that the sites collect a good deal of personal information but also that not all of the information collected may be necessary for the site to provide its services. Moreover, although most Web sites do post a privacy policy to explain to users how the host organization collects, stores, and uses their personal information, many sites do not provide privacy certification seals to allow users to quickly determine that these sites purportedly adhere to good privacy practices. These certification seals can be helpful to users because content analyses of the privacy policies showed that they were written at a high reading level. Examinations of user performance indicated that even for highly educated users, the privacy policies were difficult to comprehend, regardless of whether a policy had a high or low number of stated goals. This comprehension difficulty is due in part to the policies' use of specialized terminology, with which many computer users are not familiar.

Because the findings from the first series of studies showed that users had difficulty extracting an organization's stated privacy practices from its privacy policy, the second series of studies examined whether user agents could help users determine whether a site's privacy policy was consistent with their specified privacy preferences. Users' top privacy concerns were identified through a survey in which users rated whether they agreed or disagreed with statements regarding the use of personally identifiable and nonidentifiable information. Of the top 10 concerns identified by the survey, an existing user agent, Privacy Bird, was able to address 7 of them. However, users had to be able to configure Privacy Bird correctly in order for it to work. Experiments showed that users had difficulty setting the Privacy Bird interface appropriately for specific privacy concerns; they also seemed confused regarding which violations of their privacy preferences Privacy Bird would warn them about. Research with mock-ups of alternative interface layouts showed that presenting and specifying the privacy preferences in different ways had at most a limited effect on performance. Thus, for user agents to be able to perform their intended role, usability must be taken into account in developing the content for options to specify privacy preferences, in addition to the presentation of the options within the user interface.

There has been a tendency in recent years to pit qualitative methods against quantitative methods and to advocate use of one over the other (see Proctor, 2005, for a discussion of this issue). For example, Bamberg (2003) stated that he views "qualitative methods as the preferred inquiry method in psychology" (p. ix). We disagree with advocating a single approach and think that using a multimethod approach to obtain data regarding different aspects of a topic of concern is much more fruitful. That is, emphasis should be placed on the role that each method can play in furthering our understanding of topics of interest, rather than on claiming that one type of method is better than another for most if not all purposes. In the studies reported in this article, we found the qualitative methods to be particularly useful in identifying global issues that could then be examined more systematically by using a more quantitative, experimental approach. Researchers need to appreciate the benefits of using multiple research methods in the study not only of human–computer interaction but in the study of psychology and human factors as well.

AUTHOR NOTE

This research was supported by Grant 0430274 from the NSF ITR Cyber Trust. R.W.P. is an affiliated faculty member of the Center for Education and Research in Information Assurance and Security at Purdue University. Correspondence regarding this article should be addressed to R. W. Proctor, Department of Psychological Sciences, Purdue University, 703 Third Street, W. Lafayette, IN 47907-2081 (e-mail: proctor@psych.purdue.edu).

REFERENCES

AARONSON, D. (1994). Computer-based driving systems for research, assessment, and advisement: An introduction. *Behavior Research Methods, Instruments, & Computers*, **26**, 181-182.

ADKINSON, W. F., EISENACH, J. A., & LENARD, T. M. (2002). *Privacy online: A report on the information practices and policies of commercial Web sites* [Special Report]. Washington, DC. Progress and Freedom Foundation.

ANTÓN, A. I., EARP, J. B., VAIL, M. W., JAIN, N., GHEEN, C., & FRINK, J. M (2004). *An analysis of Web site privacy policy evolution in the presence of HIPAA* (Tech. Rep. No. 2004-21). Raleigh: North Carolina State University. Computer Science Department.

BAMBERG, M. (2003). Foreword. In P. M. Camic, J. E. Rhodes, & L. Yardley (Eds.), *Qualitative research in psychology: Expanding perspectives in methodology and design* (pp. ix-xi). Washington, DC: American Psychological Association.

CRANOR, L. F., & GARFINKEL, F. (2005). *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly.

CRANOR, L. F., GUDURU, P., & ARJULA, M. (2006). User interfaces for privacy agents. *ACM Transactions on Computer–Human Interaction*, **13**, 135-178.

EID, M., & DIENER, E. (Eds.), (2006). *Handbook of multimethod measurement in psychology*. Washington, DC: American Psychological Association.

FLESCH, R. (1949). *The art of readable writing*. New York: Macmillan.

HAN, J., & KAMBER, M. (2001). *Data mining: Concepts and techniques*. San Francisco: Morgan Kaufmann.

HOC, J.-M. (2001). Toward ecological validity of research in cognitive ergonomics. *Theoretical Issues in Ergonomics Science*, **2**, 278-288.

HWANG, W. (2006). Data mining in ergonomics. In W. Karwowski (Ed.), *Encyclopedia of ergonomics and human factors* (pp. 3077-3081). Boca Raton, FL: CRC Press.

JENSEN, C., & POTTS, J. (2004). Privacy policies as decision-making tools: An evaluation of online privacy notices. *Proceedings of the Special Interest Group on Human–Computer Interaction Conference on Human Factors in Computing Systems,* **6**, 471-478.

MOORES, T. T., & DHILLON, G. (2003). Do privacy seals in e-commerce really work? *Communications of the ACM,* **46**, 265-271.

NATIONAL SCIENCE FOUNDATION (2005). Cyber Trust 2005. Retrieved October 21, 2006, from www.nsf.gov/pubs/2005/nsf05518/nsf05518.htm.

OATES, J. (2005, February 7). AOL man pleads guilty to selling 92m email addies. *The Register*. Retrieved October 29, 2006, from www.theregister.co.uk/2005/02/07/aol_email_theft/.

PROCTOR, R. W. (2005). Methodology is more than research design and technology. *Behavior Research Methods*, **37**, 197-201.

PROCTOR, R. W., ALI, M. A., & VU, K.-P. L. (in press). Examining usability of Web privacy policies. *International Journal of Human–Computer Interaction*.

PROCTOR, R. W., & CAPALDI, E. J. (2006). *Why science matters: Understanding the methods of psychological research*. Malden, MA: Blackwell.

PROCTOR, R. W., SCHULTZ, E. E., & VU, K.-P. L. (in press). Human factors in information security and privacy. In J. Gupta & S. Sharma (Eds.), *Handbook of research on information security and assurance*. Hershey, PA: Idea Group Reference.

PROCTOR, R. W., VU, K.-P. L., & ALI, M. A. (2007). Usability of user agents for privacy-preference specification. In M. J. Smith & G. Salvendy (Eds.), *Human Interface: Part II. HCII 2007* (Lecture Notes in Computer Science No. 4558, pp. 766-776). Berlin: Springer.

SCHULTZ, E. E., PROCTOR, R. W., LIEN, M.-C., & SALVENDY, G. (2001). Usability and security: An appraisal of usability issues in information security methods. *Computers & Security*, **20**, 620-634.

SIMONTON, D. K. (2000). Archival research. In A. E. Kazdin (Ed.), *Encyclopedia of psychology* (pp. 234-235). Washington, DC: American Psychological Association.

SPIEKERMANN, S., GROSSKLAGS, J., & BERENDT, B. (2001, October). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM Conference on Electronic Commerce* (pp. 38-47). New York: ACM.

STONE, P. J., DUNPHY, D. C., SMITH, M. S., & OGILVIE, D. M. (1966). *The General Inquirer: A computer approach to content analysis.* Cambridge, MA: MIT Press.

VU, K.-P. L., PROCTOR, R. W., BHARGAV-SPANZEL, A., TAI, B.-L., COOK, J., & SCHULTZ, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human–Computer Studies*, **65**, 744-757.

ZHU, W., VU, K.-P. L, & PROCTOR, R. W. (2005). Evaluating Web usability. In R. W. Proctor & K.-P. L. Vu (Eds.), *Handbook of human factors in Web design* (pp. 321-337). Mahwah, NJ: Erlbaum.

(Manuscript received November 6, 2006;
revision accepted for publication March 13, 2007.)