Privacy Policy Representation in Web-based Healthcare

Julia B. Earp
North Carolina State University
Julia_Earp@ncsu.edu

Matthew Vail
University of Massachusetts at Amherst
mvail@cs.umass.edu

Annie I. Antón
North Carolina State University
aianton@mindspring.com

Abstract

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has resulted in the presence of very descriptive privacy policies on healthcare websites. These policies are intended to notify users about the organization's privacy practices. However, these policies are typically not easy to read, and as a result, few people actually read them. Given the fact that these policies are not optional, but required by HIPAA, they should be presented in a more usable manner that encourages consumers to read them. This, in turn, could encourage users to feel more comfortable when interacting with online healthcare organizations. In this paper, we present the preliminary results of our study that compares various ways to present privacy management information to online healthcare consumers. The study involved a survey of 993 Internet users. We also provide recommendations to managers and website designers who focus on usability.

1. Introduction

Internet users in the U.S. are actively engaged in using healthcare services and healthcare information providers online [3]. Healthcare is a very personal matter that can easily present opportunities for privacy invasions when an individual interacts with such online organizations. The U.S. department of Health and Human Services' (HHS) Privacy Rule requires healthcare institutions to notify their customers about the institution's privacy practices. Web-based healthcare organizations post their privacy practices online in the form of privacy policies. Numerous surveys have shown that users think it is important for sites to present such policies; however, they are frustrated with their quality and accuracy [9, 11]). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) has resulted in the presence of very descriptive privacy policies on these websites, however, these policies are typically not easy to read [5, 13] and as a result, few people actually read them. Surveys show that users find privacy policies to be boring, difficult to read and comprehend, hard to find, and they do not provide the information of interest to the user [9, 10].

Given the fact that these policies are not optional, but required by HIPAA, they should be presented in a usable manner that encourages consumers to read them and feel comfortable interacting with the website. Usability has been identified as one of the grand challenges for security and privacy research [7, 15]. Although effective website policy representation can improve the usability and user comprehension of policies, there has been little research to address approaches to policy representation. This is a significant absence since a privacy policy is often the only medium used to explain an organization's privacy practices. Several studies have shown that many online consumers do not read policies [9, 11]. However, most consumers are concerned about website privacy management practices. One conjecture is that consumers might feel more confident about online privacy practices if they read the privacy policies [10, 11]. Our research intends to establish an effective and usable approach to policy representation. In this paper, we present the preliminary results of our study that compares various ways to present privacy policy information to online healthcare consumers.

2. Background

The role of usability in privacy management has been acknowledged as a major challenge with regard to the widespread acceptance of web-based systems [7]. Even when interfaces are well-designed, most people do not actively participate in managing their privacy [14]. Several approaches to allow users to manage their online privacy are available (e.g. Privacybird, Anonymizer), but these tools lack mainstream popularity. Attempts to overcome problems associated with privacy policies, and thus reduce the burden on users, have resulted in machine-readable policy specification languages, such as P3P [8] and EPAL [6]. EPAL is a specification language that is used exclusively by the organization to ensure an application does not violate policy. Policies enabled by P3P, on the other hand, can be read by automated user agents, such as privacy critics [2] and Privacybird [8], but

1530-1605/07 $20.00 © 2007 IEEE

only alert users of policies that are likely to cause user concern. In order to take advantage of P3P's capabilities, the website and the user must both be willing and able to use the appropriate tools. If this is done properly, it allows the user to exercise preferences about the website's privacy practices. The idea is that by filtering out the noise and focusing users' attention on the privacy elements which are in contrast to the user's previously stated preferences, users are more likely to be engaged. However, usability problems and other challenges have hindered the widespread acceptance of P3P and related tools. Although P3P is not a panacea for privacy management, it will provide some important lessons for the design of future solutions [1]. Until these solutions are user-friendly and available to the Internet population, websites need to consider restructuring required privacy policies to benefit users as they interact with the website. To date, there has been no prior research to test and compare different privacy policy representations.

3. Methodology

3.1 Experimental Design and Hypothesis

The objectives of this study were the following: (1) to gauge user perception of various alternatives to natural language privacy policies, (2) to measure user comprehension of the alternatives, and (3) to compare user perception with user comprehension in order to determine whether they are in alignment with one another.

> When you place an order, we will ask you to set up "your account," which includes your name, e-mail address, mailing address, credit card number and expiration date, as well as certain other information when you order prescriptions. Using your account information, we will send you communications that we believe are relevant to you, including eMedalert, prescription refill and renewal reminders, newsletters or emails. If you prefer not to receive optional email or other communication from us, you may adjust your account to prevent such communications. If we receive updated account information from our shippers or other third parties, we may revise your account for you so that we can efficiently process your orders, deliver your packages or otherwise communicate with you. If you would like to review or revise the information we have in your account, you may access such information by clicking on the "your account" tab on any screen.

Figure 1: Policy Variant

To this end, we conducted an experiment using an empirical survey instrument. The type of experimental design used was a randomized complete block design. The study consisted of four ways to represent privacy policies. Although other methods to represent privacy policies are likely, we chose these four representations based on prior literature in privacy policy research. We refer to these representations as *variants* (treatments):

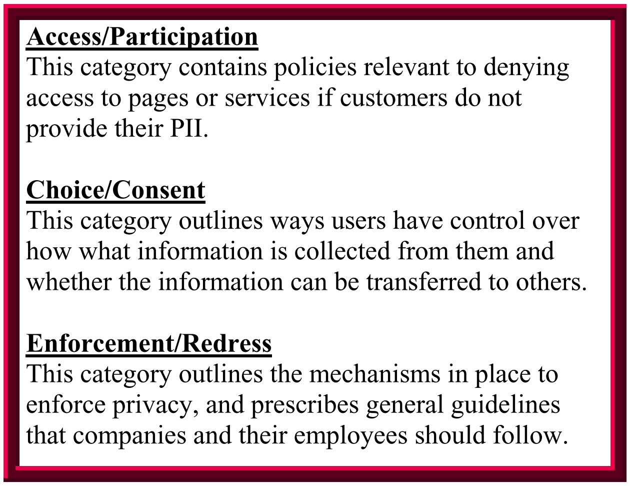
(1) Policy. The policy variant is the original natural language privacy policy that was found on the website. This is the most common approach to privacy policy representation. Figure 1 shows an example policy in this form. This is a portion of the actual natural language policy found on an active website.

(2) Goals and vulnerability statements. In the goals representation, the policy is expressed as a list of privacy goals and vulnerability statements. A privacy goal is a statement that reflects ways in which sensitive information is protected, while a vulnerability statement reflects ways in which sensitive information may be susceptible to privacy invasions or exploitation. To create the list of privacy goals and vulnerability statements, we used a goal-mining approach [4] to distill natural language goals and warnings from stated (natural language) policies. This methodology uses a list of common words of action frequently used in policies. The purpose of doing this is to eliminate unnecessary text that can either mask the true meaning of a policy or cause the policy to be too complex for the general public to understand. Figure 2 presents an example of this type of representation. *Note: the goals in this example were mined from the natural language example in Figure 1.*

- COLLECT PII when placing an order
- USE PII to offer products/services
- OPT-OUT from receiving emails from our company
- UPDATE PII automatically using information received from 3rd parties
- ALLOW customer to modify/remove their PII

Figure 2: Goals Variant (PII = personally identifiable information)

(3) Categorical. In the categorical representation, we express the policy as a list of goals and vulnerability statements that have been categorized. The goals were extracted from the original natural language policy, using goal-mining, and organized into categories based on the privacy taxonomy in [4]. The taxonomy has two classes: protection goals (notice/awareness, choice/consent, access participation, integrity/security, enforcement/redress) and vulnerability statements (information monitoring, information aggregation, information storage, information transfer, information collection, information personalization, contact). Protection goals express the desired protection of user privacy rights, whereas vulnerability statements describe requirements that potentially threaten user privacy. In this alternative, respondents are first presented with a list of the 12 taxonomy categories. Respondents can then click on a category heading hypertext link to view a list of goals/vulnerability statements, presented in bulleted form, that are relevant to the given category of interest. Figure 3 illustrates how the categories are displayed to respondents, whereas Figure 4 illustrates what respondents would subsequently see when they click on one of the category headings. Please note we have replaced the actual company name with "BrandX".



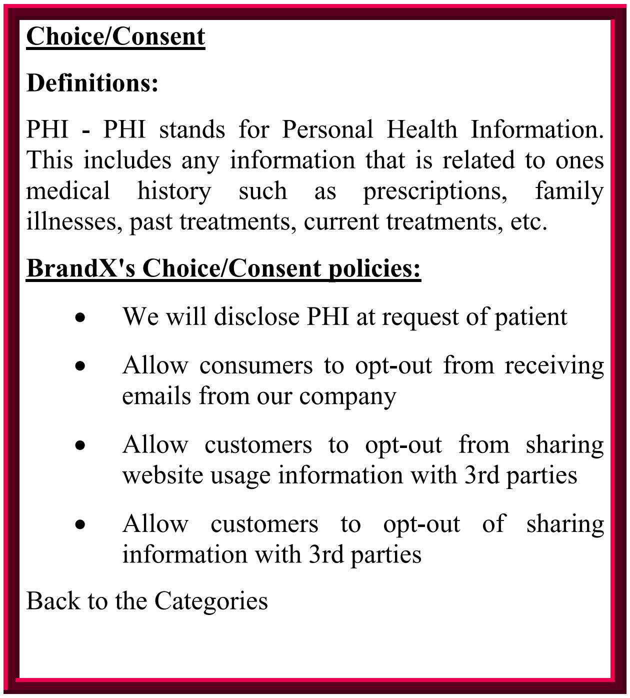
Access/Participation
This category contains policies relevant to denying access to pages or services if customers do not provide their PII.

Choice/Consent
This category outlines ways users have control over how what information is collected from them and whether the information can be transferred to others.

Enforcement/Redress
This category outlines the mechanisms in place to enforce privacy, and prescribes general guidelines that companies and their employees should follow.

Figure 3: Categorical Variant (list of categories)

(4) Goals/Vulnerabilities in Policy. In this representation, respondents are presented with the original natural language privacy policy of the website, but the format differs from the *policy* variant (treatment (1)). Within the policy, statements that contain goals or vulnerability statements relevant to user privacy are bolded and highlighted. When a respondent hovers their mouse over a statement, a popup window appears and contains the goal or vulnerability statement extracted from the statement. In this way, respondents are presented with both the natural language text and its corresponding goal or vulnerability. Figure 5 illustrates what respondents would see when they are given this variant. Notice the goal/vulnerability statements bolded and italicized within the policy, as well as the blue popup window containing the associated goal/vulnerability that appears when the respondent hovers their mouse over a given statement.



Choice/Consent

Definitions:

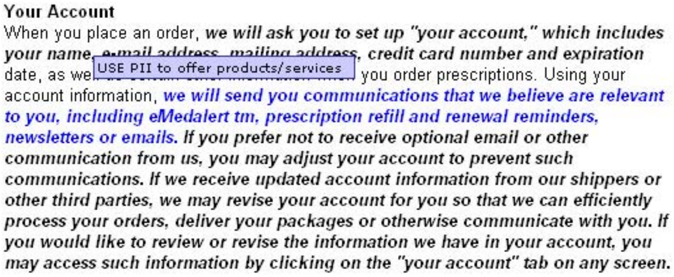
PHI - PHI stands for Personal Health Information. This includes any information that is related to ones medical history such as prescriptions, family illnesses, past treatments, current treatments, etc.

BrandX's Choice/Consent policies:

- We will disclose PHI at request of patient
- Allow consumers to opt-out from receiving emails from our company
- Allow customers to opt-out from sharing website usage information with 3rd parties
- Allow customers to opt-out of sharing information with 3rd parties

Back to the Categories

Figure 4: Categorical Variant (goals within a category)



Your Account
When you place an order, ***we will ask you to set up "your account," which includes your name, e-mail address, mailing address, credit card number and expiration*** date, as we you order prescriptions. Using your account information, ***we will send you communications that we believe are relevant to you, including eMedalert tm, prescription refill and renewal reminders, newsletters or emails. If you prefer not to receive optional email or other communication from us, you may adjust your account to prevent such communications. If we receive updated account information from our shippers or other third parties, we may revise your account for you so that we can efficiently process your orders, deliver your packages or otherwise communicate with you. If you would like to review or revise the information we have in your account, you may access such information by clicking on the "your account" tab on any screen.***

Figure 5: Goals/Vulnerabilities in Policy Variant

To address two of our three research questions stated above, we propose that:

HYPOTHESIS 1: Internet users comprehend *categorical* healthcare privacy policies (as in treatment (3)) better than other representations.

> HYPOTHESIS 2: Internet users feel more comfortable about sharing their information with sites that implement *categorical* healthcare privacy policy representation (as in treatment (3)).

The experiment employed a 3 x 4 factorial design with 3 websites and 4 policy variants. Each of the three websites had a different privacy policy containing a different ratio of vulnerability statements to protection goals. These policies came from the following websites: Novartis.com, Drugstore.com and HealthCentral.com. The number of vulnerability statements and number of goals provide a straightforward way to measure how protective or how dangerous a website might be to the user. The Novartis.com policy contained more protection goals (23) than vulnerability statements (9), and the Drugstore.com policy contained more vulnerability statements (36) than protection goals (19). The HealthCentral.com policy served as our *control* factor because it contained the same amount of vulnerability statements (12) as protection goals (12). The resulting experimental matrix is presented in Table 1.

		Variant			
		Orig. Policy	**Goals**	**Cat.**	**Goals in Policy**
Policy	*Drugstore (more vulnerable)*	*76*	*80*	*77*	*93*
	HealthCentral (control)	*86*	*87*	*81*	*83*
	Novartis (more protective)	*77*	*81*	*83*	*89*
	Total	***239***	***248***	***241***	***265***

Table 1. Experimental Treatments and Blocking Factors

Table 1 shows the 12 possible policy/representation combinations that respondents could have received, and the number of respondents receiving each policy/variant survey combination. Each column represents a different treatment (natural language policy, goals and vulnerability statements, categorical, goals/vulnerabilities in policy), while each row represents a different blocking factor (more vulnerable policy, more protective policy, control policy).

To prevent name-brand recognition bias from influencing the results of the experiment, we removed all references to the names of the original policy authors and replaced them with “BrandX”. To further prevent bias, we randomly assigned respondents to one of the 12 policy representations. Before each policy, we presented the respondent with a textual scenario to provide context for reading the policy. The given scenario places the respondent in a situation of obtaining healthcare services online. Respondents were asked to read the privacy policy with the intention of engaging in a transaction with the organization.

Once users finished reading the policy, they were presented questions based on the content of the policy. The question types could be classified into three categories: perception, comprehension, and demographic. The *perception* questions gauged how users felt about what they read and were presented using a 5-point Likert scale anchored by “Strongly Disagree” (1) and “Strongly Agree” (5). The *comprehension* questions measured how well users comprehended the content of the policy and were presented in the form of multiple choice quiz questions. The *demographic* questions measured the demographic makeup of the sample and were presented in the form of drop-down, multiple choice questions.

The same perception and demographic questions were asked of all respondents, regardless of which of the 12 policy representations they received. The comprehension questions differed depending on the policy that was viewed. For each policy, we derived a single question for each taxonomy category if the policy contained a statement in this category. For example, if the Drugstore.com policy contained a statement that was categorized as an *information transfer* statement, we would ask a question about the information transfer practices of Drugstore.com; otherwise, if no such policy statement existed, we did not ask a question about the information transfer practices of Drugstore.com. Each one of these questions was accompanied by five possible answers, only one of which was correct. Each taxonomy category question was worded the same for each policy. However, since each policy (i.e., Drugstore.com, HealthCentral.com, Novartis.com) contained different content, the correct answer was different for each policy. Rather than providing respondents with 12 comprehension questions (one for each taxonomy category), the survey instrument would randomly selected three questions from the set of all possible comprehension questions for that policy. For example, given the HealthCentral.com policy, the instrument would randomly select three questions from the set of HealthCentral.com comprehension questions. Let us assume that the instrument randomly chose *information transfer*, *notice/awareness*, and *information monitoring* as our questions. We would then ask a single question for each of these categories about the content of the HealthCentral.com policy.

In addition to these three questions, respondents who received the *categorical* variant were also presented with two additional comprehension questions based on the first and last categories they chose to view.

3.2 Survey Distribution and Data Collection

Prior to distributing the survey, we pilot tested the initial survey using an online format. Based on some preliminary analysis and comments from the respondents, we deleted some items and reworded some others. The resulting instrument had seven scale items, eleven demographic items and between three and five multiple choice questions, depending on the variant being applied.

The final survey was linked from an NSF-sponsored website and was advertised to a variety of Internet users worldwide. Respondents were solicited through a variety of outlets, including links to the survey from various university webpages, general news sites, alumni mailing lists, professional mailing lists, email and word of mouth. To increase the variability in the data and generality of the survey, we launched a marketing campaign designed to target all demographic audiences. Participants of the survey were offered an entry into a prize drawing, to take place at the conclusion of the survey. The survey was available October 25, 2005 to December 10, 2005 via the Web at an NSF-sponsored project site.

We received 1,215 total responses, but used some built-in mechanisms to distinguish between valid and invalid responses. Based on the pilot study, it was relatively certain that respondents could not read the directions, as well as the policy, in less than 30 seconds. Therefore we eliminated respondents who spent a combined total of 30 seconds or less reading the instructions and policy. This eliminated 212 responses.

We eliminated 10 additional responses by analyzing the responses to some carefully formed validation items included in the survey. After eliminating the invalid responses from the dataset, we ended up with 993 usable responses.

4. Results and Discussion

The overall objective of this study was to glean valuable information about the user perception and comprehension of alternatives to natural language privacy policies. We discovered that there is a statistically significant disparity between the perceptions of the various policy expressions, as well as the comprehension of the various policy expressions.

An in-depth ANOVA test shows that our first hypothesis, *Internet users comprehend categorical healthcare privacy policies better than other representations*, is supported by our data ($p<0.0001$). Our second hypothesis, *Internet users feel more comfortable about sharing their information with sites that implement categorical healthcare privacy policy representation*, is not supported by our data. The data, on the other hand, shows that Internet users feel more secure sharing their information with sites that implement a combination of natural language policies where relevant privacy goals and vulnerabilities are highlighted ($p<0.0001$).

4.1 User Perception

Users feel more secure sharing personal information with the website that displays the natural language policies (including the natural language policy by itself and the natural language policy with the privacy goals and vulnerabilities highlighted). When asked whether they feel secure sharing personal information with the website, after viewing their privacy policy, users tend to feel more secure after viewing the natural language privacy policy with the goals and vulnerabilities highlighted. There is a difference ($p < 0.0001$) between the *goals/vulnerabilities in policy* variant and the *categorical* and *goals/vulnerabilities* variants. This may be because users feel comfortable with the natural language policy that strives to present a warm and caring impression. Most of the natural language policies begin with language that encourages the user to feel positively toward the website. For example, the following text is found at the beginning of an actual policy posted by HealthCentral.com[1] during a prior study:

Dear Friends,
First and foremost, HealthCentral is deeply committed to preserving your privacy. We have established stringent rules of privacy and responsibility in order to protect the rights of HealthCentral users.

At the same time, users may enjoy lessening the burden of reading the policy by having someone highlight the important goals and vulnerabilities found in the policy. The average response for each variant is presented in Table 2.

Users feel that the companies using the 'goals/vulnerabilities in policy' variant will protect their information the most. Based on the statement "*I believe BrandX will protect my personal information* ***more*** *than most other companies*", Table 3 illustrates that users feel more confident that the policies that were expressed using natural language (*policy* and *goals/vulnerabilities in policy*) would protect their information more than the policies using the goal-based variants (*goals/vulnerabilities in policy* and *categorical*).

[1] "HealthCentral.com Privacy Policy". http://www.healthcentral.com. Downloaded on September 19, 2003.

Variant	Average
Natural Language Policy	2.72
Goals/Vulnerabilities	2.44
Categorical	2.58
Goals/Vulnerabilities in Policy	2.85

Table 2. Average response to "I feel secure sharing my personal information with BrandX after viewing their privacy practices" for each policy representation.

Variant	Average
Natural Language Policy	2.71
Goals/Vulnerabilities	2.60
Categorical	2.60
Goals/Vulnerabilities in Policy	2.80
Average	2.68

Table 3. Average response to "I believe BrandX will protect my personal information more than other companies" for each policy representation.

Users feel that the two variants that use the natural language approach (natural language policies and policies with goals/vulnerabilities highlighted in the natural language) are explained more thoroughly than alternative expressions. See Table 4. This result is to be expected because natural language privacy policies are generally more verbose than the categorical or goal/vulnerability list policies ($p < 0.0001$). A longer policy may provide the illusion of being more thorough but it may not be more protective in terms of how user information is used by the website.

Variant	Average
Natural Language Policy	3.24
Goals/Vulnerabilities	2.77
Categorical	2.88
Goals/Vulnerabilities in Policy	3.33
Average	3.06

Table 4. Average response to "I feel that BrandX's privacy practices are explained thoroughly in the policy I read" for each policy representation.

Users feel confident in their understanding of the two variants that use the natural language approach (natural language policies and policies with goals/vulnerabilities highlighted in the natural language). See Table 5. Respondents were statistically ($p < 0.0002$) more confident in understanding all of the policies except for the *goals/vulnerabilities* variant. However, the average confidence level is strongest with the *goals/vulnerabilities in policy* variant.

Users also felt the least confident ($p < 0.008$) with what they read in the Drugstore.com policy (see Table 6). This may be due to the Drugstore.com having the longest policy, making it difficult for users to comprehend it in its entirety.

Variant	Average
Natural Language Policy	3.27
Goals/Vulnerabilities	2.95
Categorical	3.22
Goals/Vulnerabilities in Policy	3.31
Average Overall	3.19

Table 5. Average response to "I feel confident in my understanding of what I read of BrandX's privacy policy" for each policy representation.

Policy	Average
Drugstore.com (vulnerable)	3.05
Novartis (protective)	3.24
HealthCentral (control)	3.27
Average Overall	3.19

Table 6. Average response to "I feel confident in my understanding of what I read of BrandX's privacy policy" for each organization's policy

4.2 User Comprehension

The user comprehension questions were presented in the form of a multiple choice quiz. For each respondent, a quiz score was calculated based on the number of questions answered correctly. The formula for the score was as follows: score = (questions correct / total questions asked) * 100. This yielded a numeric value between 0 and 100 and represented the user's true comprehension, not their perception of comprehending.

The results (Table 7) clearly illustrate that the natural language privacy policy was the most difficult representation to comprehend ($p < 0.0001$). In fact, users only answered a third of the privacy related questions correctly when given the *policy* variant.

The comprehension of the natural language privacy policy increased when privacy statements were highlighted within the policy and accompanied by goal statements, as in the *goals/vulnerabilities in policy* variant. This illustrates that the natural language policy alone may not be sufficient for conveying policy information to the average user. The comprehension scores increased further when users were presented with the policy expressed as a list of goal statements, as in the *goals/vulnerabilities* variant. This is fairly intuitive, given that goal statements are uniform and eliminate extraneous and unnecessary information. For example, in the Drugstore.com policy, the *goals/vulnerabilities* variant contained a fourth of the total words than the *policy* variant. With less information to read and try to retain, users do not experience information overload and can retain essential information regarding the uses and disclosures of their personally identifiable information (PII).

The comprehension scores were the highest for the *categorical* variant. This policy variant organizes the goal statements found in the *goals/vulnerabilities* variant into the privacy taxonomy category it belongs to. Since this variant is comprised of the same goals and vulnerability statements that are found in the *goals/vulnerabilities* variant, we expected to see similar comprehension results. What we found is that the comprehension of the policies actually increased when they were categorized. This may suggest that users will retain information better when it is presented to them in an organized manner.

Variant	**Average**
Natural Language Policy	35.70
Goals/Vulnerabilities	43.82
Categorical	52.14
Goals/Vulnerabilities in Policy	43.27
Average Overall	43.74

Table 7. Average comprehension score by users reading each policy representation (all respondents)

By omitting all users who did not read the entire set of privacy policies, we could further analyze the readability of the policy variants. The average comprehension score for each variant for users who read the entire policy is presented in Table 8. First, it did not matter whether users read the entire policy or not, the *categorical* variant was always the easiest to comprehend (based on the quiz score) and the *policy* variant was always the most difficult ($p < 0.0001$). Second, even among users who read the entire privacy policy, only about half of the comprehension questions were answered correctly.

Variant	**Average**
Natural Language Policy	40.00
Goals/Vulnerabilities	55.46
Categorical	65.67
Goals/Vulnerabilities in Policy	49.38
Average Overall	52.88

Table 8. Average comprehension score by users reading each policy representation (only respondents who read the entire policy)

4.3 Other Observations

As mentioned earlier, we asked users, "Why didn't you read the entire set of privacy policies of the website?" In each variant, the majority of users read the entire set of privacy policies. The most common reason why users did not read the entire set of privacy policies was that the policy was too long. One important observation is that users most often read the entire set of privacy policies when given the *categorical* variant. As a result, there were a lesser percentage of users who felt that the *categorical* policies were too long.

4.3.1. No correlation between demographic factors and comprehension exist, similarly, no correlation between demographic factors and perception exist. After analyzing the data, we concluded that demographics make no statistical difference in the user perception of the various variants and policies. Furthermore, with the exception of a single age group, demographics had no affect on the comprehension scores of the various variants and policies. All age groups scored the same, with the exception of users ages 57 and higher. This group scored lower on the comprehension questions than the other age groups.

4.3.2. User perception is not in alignment with user comprehension. Though users feel most secure and protected by the *goals/vulnerabilities in policy* variant, their comprehension of the content is not as good as with other variants. Even among users who read the entire policy, users who read the *policy* variant only answer a little over a third of the questions correctly. However, despite not feeling as secure or protected by the categorical policies, user comprehension scores were much greater when given these policies. This misalignment of user perception with user comprehension is disconcerting because users may be more inclined to trust a company with a policy that lacks clarity and readability. This leads to less informed decisions that could result in the increase of unanticipated and unwanted uses and disclosures.

5. Conclusion

Our respondents have an average education level of more than a college degree. Specifically, they tend to have taken at least one class in a graduate program. Although this does not parallel to the average education level of Internet users over age 25 (14.4 years, or two years of college), we can still make important inferences from this study. Table 7 shows the exceptionally low "quiz" scores of our sample respondents. It is likely that a more average sample would score even lower on this portion of the survey. We can undoubtedly suggest that additional work is needed in the area of how organizations should communicate privacy management practices to users.

As with any survey, there was concern that respondents would not be completely honest in their responses [12]. Several measures were taken to avoid incorporating dishonest users' responses into the respondent dataset, including: preventing users from revisiting the policy to look up answers to comprehension questions by detecting such actions and sending the user back to the beginning of the survey with a completely different policy; requiring that the questionnaires be completed before submission; ensuring the anonymity of respondents would be preserved; and identifying and removing responses from the dataset that were identified as being invalid.

As a result of this study, we discovered that there is a disparity between user perception of the various privacy policy expressions and how well users comprehend each of the various policies. Even though users felt more secure with, protected by, and comfortable with the *goals/vulnerabilities in policy* variant, they did not comprehend them as well as the categorical privacy policies. Recognizing that users comprehend categorical policies better than natural language policies, researchers need to find ways to exploit this idea and communicate privacy management practices in a more usable manner. This is especially important in the healthcare environment where many users are searching for solutions to the most sensitive types of problems.

The disparity between user perception and comprehension may be due to HCI factors, in which the users are simply not comfortable with the manner in which the goal and categorical policies are presented to them. To support this claim, one need only note the marked improvement in comprehension scores between the *goals/vulnerabilities* variant and the *categorical* variant. The *categorical* variant does nothing more than present the goal statements to the user in an organized fashion. If research efforts were invested in addressing the HCI issues surrounding these policies, the misalignment between user perception and user comprehension may be rectified.

6. ACKNOWLEDGMENTS

This work was partially funded by NSF grant *ITR: Encoding Rights, Permissions and Obligations: Privacy Policy Specification and Compliance* (NSF #032-5269) and partially funded by Purdue CERIAS. We would like to acknowledge members of The Privacy Place (http://theprivacyplace.org/). Additionally, we would like to thank IBM for their support in encouraging survey participants.

7. REFERENCES

[1] Ackerman, M. (2004) Privacy in pervasive environment: next generation labeling protocols. *Pers Ubiquit Comput* 8: 430-439.

[2] Ackerman, M. and Cranor, L. (1999) Privacy Critics: UI Components to Safeguard Users' Privacy, *Extended abstracts of ACM Conference on Human Factors in Computing Systems CHI'99*, 2, 258-259.

[3] K. Aiken (2004) Patient and Physician Attitudes and Behaviors Associated With DTC Promotion of Prescription Drugs - Summary of FDA Survey Research Results, November 19. 2004, Last accessed February 23, 2006 at http://www.fda.gov/cder/ddmac/researchka.htm.

[4] Antón, A.I. and J.B. Earp (2004) A Requirements Taxonomy to Reduce Website Privacy Vulnerabilities. *Requirements Engineering Journal*, Springer Verlag, 9(3), pp.169-185.

[5] Antón, A., J.B. Earp, D. Bolchini, Q. He, C. Jensen and W. Stufflebeam (2004) The Lack of Clarity in Financial Privacy Policies and the Need for Standardization, *IEEE Security and Privacy,* 2(2), pp.36-45.

[6] Ashley, P. and Schunter, M. (2002) The Platform for Enterprise Privacy Practices". *Information Security Solutions Europe*, Paris France.

[7] Computer Research Association (CRA) (2003) Conference on Grand Research Challenges in Information Security and Assurance, http://www.cra.org/Activities/grand.challenges/security/. November 16-19, 2003.

[8] Cranor, L., Arjula, M., and Guduru, P (2002) Use of a P3P User Agent by Early Adopters. *Proceedings of the ACM Workshop on Privacy in the Electronic Society*, November 21, 2002, Washington, DC.

[9] Culnan, M. J. and Milne, G. R. (2001) The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses. Last accessed on February 28, 2005 at http://intra.som.umass.edu/georgemilne/pdf_files/culnan-milne.pdf. Washington DC: FTC.

[10] Earp, J.B, Antón, A.I, Aiman-Smith, L and Stufflebeam, W.H. (2005) Examining Internet Privacy Policies Within the Context of User Privacy Values in *IEEE Transactions on Engineering Management,* Vol. 52., No. 2.

[11] Earp and Baumer (2003) Innovative web use to learn about user behavior and online privacy. Communications of the ACM, vol. 46, no. 4, pp. 81-83.

[12] Jensen C. and C. Potts (2005) Privacy Practices of Internet Users: Self-report versus Observed Behavior, *International Journal of Human Computer Studies*. July 2005.

[13] Jensen C. and C. Potts (2004) Privacy Policies as Decision-Making Tools: A Usability Evaluation of Online Privacy Notices *Proceedings of CHI'04* Vienna, Austria, April 2004

[14] Weirich D. and Sasse, M.A. (2001) Pretty Good Persuasion: A first step towards effective password security for the Real World *Proceedings of the New Security Paradigms Workshop 2001* (Sept. 10-13, Cloudcroft, NM), pp. 137-143. ACM Press.

[15] Whitten, A. and Tygar, J.D. (1999) "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," *Proceedings of the 8th USENIX Security Symposium.*