Design of a Privacy Label for P3P Policies

Patrick Gage Kelley, Sungjoon Steve Won, Lorrie Faith Cranor
Carnegie Mellon University
5000 Forbes Ave.
Pittsburgh, PA USA
pgage@cmu.edu, swon@andrew.cmu.edu, lorrie@cs.cmu.edu

1. INTRODUCTION

In this poster submission we describe the ongoing development of a new approach to displaying privacy policies. Privacy has become a key issue for internet consumers. Several studies have indicated the growing importance of privacy for consumers of web sites, yet current mechanisms to present privacy policies of web sites to consumers have not succeeded.

Website privacy policies are intended, in part, to assist consumers, by notifying them what information will be collected, how it will be used, and with whom it will be shared, as well as informing customers of the choices they have in managing their information, including: what data is optional, if sharing can be limited, and if it is possible to request their information or have it purged. However most privacy policies provided for consumers are written by lawyers and are hard for consumers to understand. This is largely due to the use of specific terms that many people do not understand how to relate to their own use of the website, a readability level that is congruent with a college education, and a general non-committal attitude towards specific details. It has further been established through numerous studies that people do not read privacy policies. [8]

In response to the difficulties of textual privacy policies the World Wide Web Consortium created P3P. [11] P3P or the Platform for Privacy Preferences is a standard for encoding the website privacy policy of a company or organization into a machine readable format. For consumers to be able to take advantage of the benefits, user-agents must interpret the P3P policy to the consumers, many of which are currently limited. [3]

We believe that we should focus on providing a technology that is similar in ways to nutritional labels that are on food products. Consumers are very aware that when selecting an item at the grocery store there are a number of choices and their nutritional values differ. Because there is a legislated standard label consumers are able to easily compare different products and make an informed decision on what will stock their pantries.

Our objective is to address this gap in communications by providing a mechanism that improves the visual presentation and comprehensibility of privacy policies. Using a mechanism modeled using design features found in nutrition labeling, drug labeling, and energy labeling, as well as other efforts involved in creating a standardized banking privacy notification we present a Privacy Label to present privacy policies. Finally, we present results from two small studies carried out to test the new design.

2. RELATED/PREVIOUS WORK

Much research in information design has been focused on providing consumers with easily accessible information. This information has been applied to nutrition labels [1,2,10], pharmaceutical and medical labels, and energy usage labels on electronics [5]. As we see with the Kleimann report [7] we are just beginning to apply these methods to privacy.

In order to provide consumers with an active tool where we could begin to test many of the design lessons learned from the research mentioned above, we created the P3P Expandable Grids Viewer [6,9]. This first draft was based around one of the central Expandable Grid objectives of displaying a holistic policy. An example of the grid can be shown in Figure 3.

Based on an online survey of over 800 people in the summer of 2007, we found further evidence that people generally do not comprehend privacy policies and also people do not enjoy reading them. In comparing three formats: natural language, PrivacyFinder, which is a simplified human readable version directly from the P3P xml, and an early version of P3P expandable grids, none of the three formats were pleasurable to read or comprehensible.

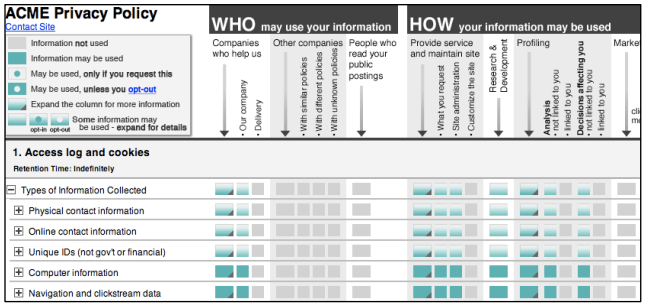

Figure 1. The P3P Expandable Grid Viewer.

From the analysis of the above study we found five main problems with the Expandable Grid in its current form [6]:

- Many of the labels for data and purposes are not clear to users; for example, "Profiling" and "Miscellaneous Data."
- The legend has a large number of symbols which the user may not understand, including multiple symbols for expansion.
- Multiple statements in a P3P policy are displayed separately, requiring the user to check multiple rows.
- The Hide Used Information button in the top right only condenses unused rows, not rows and columns.
- Rows with a plus symbol can be expanded; however, many users (40.7%) never expanded any data types.

It was with these five problems, and specifically the first that we thought about other approaches. People were not understanding the labels, partially because expressing a privacy policy is complicated and partially because they do not have enough context to understand what they are being shown.

3. DESIGN ITERATIONS & GUIDELINES

With these five problems in mind, and the extended research from information and warning design [4], and the above mentioned

label designs, we began a series of rapid iteration and prototyping. From these iterations we present the following seven design principles that guide the label below.

- Defining a minimum type point size, of 12px, and framing our design in relative units we allow users the ability to modify the size of the label in a browser. We also define a width of 760px which fits on all common resolutions in a browser window.
- Putting a rule around the label, we define its territory, making certain that it clearly identifies the boundaries of the information.
- Using a binary [Yes | No] declaration for the statements sharing and usage sections, we minimize the subjects' need to transform information into a usable form and provide clear answers (removing legal and ambiguous wiggle room).
- Using bold rules to separate sets of information, we give the reader an easy roadmap through the label.
- Not displaying data types that are not collected or purposes that data will not be used for reduce the complexity of the label.
- Color coding the information elements that are 'optional', assists readers in being able to clearly identify the distinction between mandatory and optional information elements.
- Providing a clear and boldfaced title for the Privacy Label, communicates the content and purpose of the label more specifically, and assists in recognition.

4. RESULTS

While this work is still in progress, we believe we are converging on a design that will test better with users than a natural language privacy policy and more beneficially allow for direct comparison between policies, a task we have yet to test.

As for design guidelines, we believe the seven bullet points above can be seen as more general design guidelines that should apply to designing informational labels relating to privacy as well as other areas, and as we proceed we continue to refine these.

As a final design consideration it is likely evident from the above work that we chose to maintain a similar look and feel for the Privacy Label as the Nutrition Label or Drug labeling since most users in the United States are familiar with these, and would be comfortable with the presentation of the information. We believe that consistency both between labels displaying privacy as well as across types of information labels is beneficial in providing a trusted foundation.

5. CONCLUSION

As stated privacy is becoming more relevant to consumers and we need to provide technologies that help consumers understand the control they have surrounding their information as they push harder for such knowledge. We have demonstrated an ongoing design project that we believe will eventually be more successful in both contextually explaining privacy to users and also in helping compare privacy policies, paving the way for informed consumer decisions.

6. ACKNOWLEDGMENTS

We would like to thank Rob Reeder, Seshadri Iyer, and Aleecia McDonald for their assistance in providing feedback, suggestions, and guidance as this work progressed.

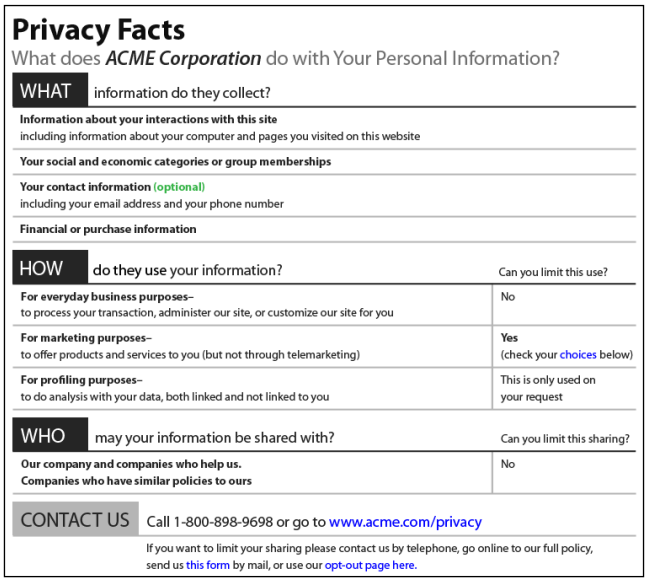

Figure 2. Proposed Large Scale Testing Design.

7. REFERENCES

[1] Belser, Burkey. Designing the Food Label: Nutrition Facts. AIGA Journal. 2007. http://greenfieldbelser.com/big_ideas/?NewsID=58. Accessed November 13, 2007.

[2] Buckley, Paul and Richard Shepherd. Ergonomic factors: The clarity of food labels. British Food Journal. 1993. 95 (8).

[3] Cranor, L., S. Egelman, S. Sheng, A. McDonald, and A. Chowdhury. P3P Deployment on Websites. To be published in Electronic Commerce Research and Applications, 2008. Available: http://lorrie.cranor.org/pubs/p3p-deployment.html

[4] DeJoy, D.M., Cameron, K.A., & Della, L.J. (2006). Post-exposure evaluation of warning effectiveness: A review of field studies and population-based research. The Handbook of Warnings (pp. 35-48). Mahwah, NJ: Erlbaum.

[5] The Energy Label. 2007. http://www.energyrating.gov.au/con3.html. Accessed on November 25, 2007.

[6] Kelley, P., A. McDonald, R. Reeder, and L. Cranor. P3P Expandable Grids. Poster at Privacy MindSwap Carnegie Mellon University. October 2007.

[7] Kleimann Communication Group, Inc. Evolution of a Prototype Financial Privacy Notice. February 2006. Available: http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf

[8] McDonald, A. Toward Privacy Policies That Work. Pre-Qualifier Talk, Carnegie Mellon University. October 2007.

[9] Reeder, R. Expandable Grids. Thesis Proposal. January 2007.

[10] U.S. Food and Drug Administration. A Food Labeling Guide. Center for Food Safety & Applied Nutrition. 1999. http://vm.cfsan.fda.gov/%7Edms/flg-toc.html. Accessed on November 10, 2007.

[11] W3C. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. Available: http://www.w3.org/TR/P3P/ Accessed November 2007.