Designing a Privacy Label: Assisting Consumer Understanding of Online Privacy Practices

Patrick Gage Kelley
Carnegie Mellon University
5820 Forbes Avenue,
Pittsburgh, PA 15213 USA
pgage@cmu.edu

CHI 2009, April 4 – 9, 2009, Boston, MA, USA
ACM 978-1-60558-246-7/09/04.

Abstract
This project describes the continuing development of a Privacy Label to present to consumers the ways organizations collect, use, and share personal information. Several studies have indicated the importance of privacy for consumers, yet current mechanisms to present privacy policies of websites have not been successful. This research addresses the present gap in the communication and understanding of privacy policies, by creating an information design that improves the visual presentation and comprehensibility of privacy policies. Drawing from the nutrition, warning, and energy labeling, as well as from the effort towards creating a standardized banking privacy notification, I present the process and ongoing results of the development of a usable information design for privacy policies.

Keywords
Privacy, Privacy Policies, Labeling, Information Design

ACM Classification Keywords
K.4.1 Public Policy Issues --- Privacy, D.4.6 Security and protection, H.5.2 User Interfaces

Introduction
Website privacy policies are intended to assist consumers. By notifying them of what information will be collected, how it will be used, and with whom it will

be shared, customers are, in theory, able to make informed decisions. These policies are also meant to inform customers of the choices they have in managing their information, whether specific information requests are optional, if sharing can be limited, and if it is possible to request access and changes to their information or have it purged.

However most privacy policies provided to consumers are difficult 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 [6]. It has further been established through numerous studies that people do not read privacy policies, and make mistaken assumptions about the existence of a link to a privacy policy [12]. Additionally, it has been estimated that if consumers were to read all the policies of companies they interact with, it would cost 365 billion dollars per year [9].

Finally, users do not believe they have choices when it comes to their privacy and the use of their personal information, based on a common expectation that companies have equivalent privacy policies that do not allow the consumer any control [8]. This finding has been validated again in this work.

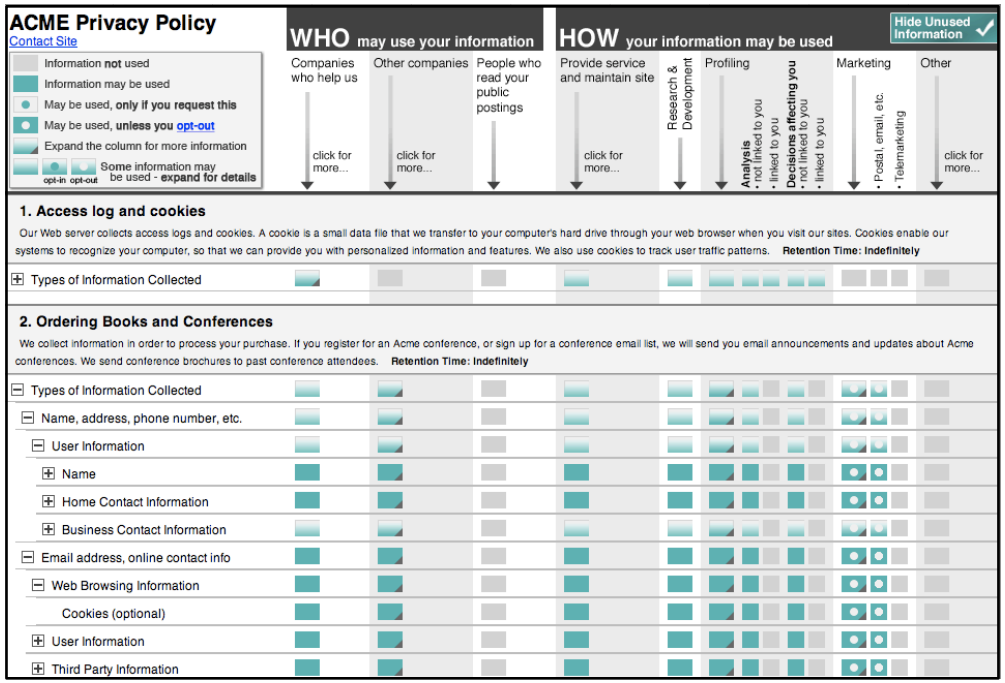
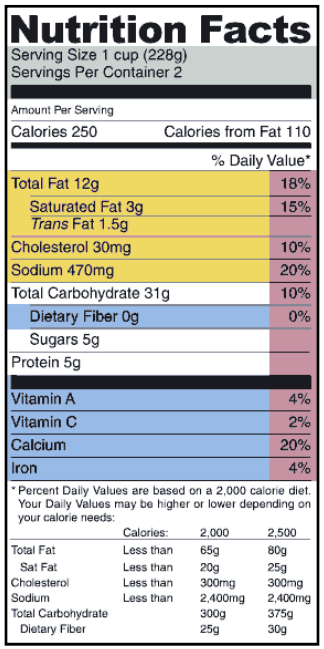


Figure 1. An image of the originally tested P3P Expandable Grid

Background

Due to the difficulties of using textual privacy policies, the World Wide Web Consortium created the Platform for Privacy Preferences or P3P [14]. P3P is a standard for encoding the online privacy policy of a company or organization into a machine-readable format. For consumers to be able to take advantage of policies converted to this format, they must use a user-agent to interpret the policy. Unfortunately, many current user-agents are currently very limited [3].

To provide consumers with an active tool where they can investigate and explore the full policy of a website, earlier work from the Carnegie Mellon Usable Privacy and Security Lab (CUPS) created the P3P Expandable Grid. This agent was based on one of the central Expandable Grid objectives of displaying a holistic policy [10]. The interface was created to use the entire P3P specification, broken down by categories. An example of the grid is shown in Figure 1.



Nutrition Facts

Serving Size 1 cup (228g)
Servings Per Container 2

Amount Per Serving

Calories 250	Calories from Fat 110
	% Daily Value*
Total Fat 12g	18%
Saturated Fat 3g	15%
Trans Fat 1.5g	
Cholesterol 30mg	10%
Sodium 470mg	20%
Total Carbohydrate 31g	10%
Dietary Fiber 0g	0%
Sugars 5g	
Protein 5g	
Vitamin A	4%
Vitamin C	2%
Calcium	20%
Iron	4%

* Percent Daily Values are based on a 2,000 calorie diet. Your Daily Values may be higher or lower depending on your calorie needs:

	Calories:	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g

Figure 2. An example image of the Nutrition Facts panel from the FDA Center for Food Safety and Applied Nutrition [13]

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 do not enjoy reading them. When comparing three formats: the natural language policy; PrivacyFinder, a simplified human readable version based on the P3P policy; and an early version of the P3P Expandable Grid, we found that none of the three formats were found to be pleasurable to read or easy to comprehend [11].

Notably, the P3P Expandable Grid, which was expected to perform well, was found to be the worst, both in enjoyment and comprehension. To create a better privacy policy user-agent interface, I sought inspiration from already existing (and frequently legislated) labels [4]. This included a number of publications regarding the design and adoption of nutrition labels, [1,2] drug facts, and energy labeling [5].

In the United States the nutrition label seen in Figure 2 has become nearly iconic since it was mandated in 1990. In the last nineteen years its increasing ubiquity has led to a number of studies examining the costs of adoption and the ability to inform and change consumer purchasing decisions. This work and an extended report by the Kleimann group for the Federal Trade Commission on a proposed Financial Privacy Notice, [8] will be the basis of the following process.

Process & Results

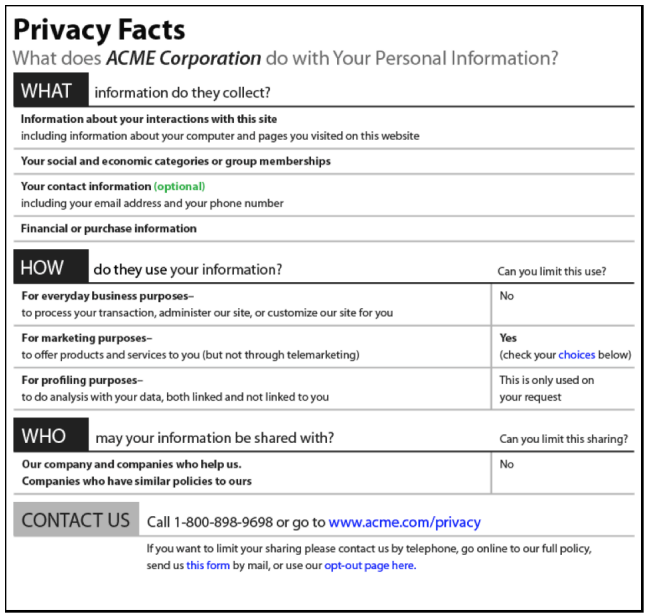
Based on the analysis of the previously mentioned privacy policy format study results and in-lab prototyping, I identified five major problems with the Expandable Grid in its current form [7]:

- Many of the P3P labels are not clear to users. For example, "Profiling" and "Miscellaneous Data" both are not terms that users encounter in the context of their use of websites.
- The legend has a large number of symbols including multiple symbols for expansion (depending on directionality) which the user may not understand.
- Multiple statements that may be related to the same types of information in a P3P policy are displayed separately, possibly requiring the user to check multiple rows, to answer a single question.
- The Hide Used Information button in the top right only condenses unused rows, not columns.
- Rows with a plus symbol may be expanded; however, many users (40.7%) never expanded any data types, a flaw with the designed user experience (recorded during the '07 survey [11]).

With these five problems in mind, and the design guidelines given in the above mentioned label designs, I began a series of rapid iteration and prototyping. From these iterations I present the following design principles abstracted from the labeling literature.

- Defining a maximum width of 760px the label will fit in a browser window on all common resolutions, and a length that, when printed, will fit on a single sheet of standard 8.5" x 11" paper.
- Putting a box around the label, defines its territory, making certain that it clearly identifies the boundaries of the information.
- Hiding data types that are not collected or irrelevant purposes for data, the complexity of the label is reduced.

- Using bold rules to separate sets of information, gives the reader an easy roadmap through the label.
- Providing a clear and boldfaced title for the Privacy Label communicates the content and purpose of the label specifically, and assists in recognition.



Privacy Facts

What does ***ACME Corporation*** do with Your Personal Information?

WHAT information do they collect?

Information about your interactions with this site
including information about your computer and pages you visited on this website

Your social and economic categories or group memberships

Your contact information (optional)
including your email address and your phone number

Financial or purchase information

HOW do they use your information? | Can you limit this use?

For everyday business purposes–
to process your transaction, administer our site, or customize our site for you | No

For marketing purposes–
to offer products and services to you (but not through telemarketing) | **Yes** (check your choices below)

For profiling purposes–
to do analysis with your data, both linked and not linked to you | This is only used on your request

WHO may your information be shared with? | Can you limit this sharing?

Our company and companies who help us.
Companies who have similar policies to ours | No

CONTACT US Call 1-800-898-9698 or go to www.acme.com/privacy

If you want to limit your sharing please contact us by telephone, go online to our full policy, send us this form by mail, or use our opt-out page here.

Figure 3. This intermediate design, clearly informed by the proposed Financial Privacy Notice and the Nutrition Facts label was rejected for being too simple.

Another design consideration represented in Figure 3, is using a Yes or No declaration for the statements, simplifying the label. However, the Yes or No format as well as the list format vs grid were both reversed as they could not adequately represent the complexity of privacy policies.

Our final proposed label (Figure 4), reintroduces symbols for collected data, opt-in, opt-out, and mixed use, which range from light to dark based on severity, allowing advanced users to quickly glimpse at the label to obtain a high-level overview. This version is also interactive, allowing users to see the full policy, including personal information that is not collected, a failing of the version in Figure 3. Additionally, each cell can be clicked on for more information and explanations of the terms used. Compared to the original P3P Expandable Grid, this label is much simpler, fitting on a single page, with tuned defaults to help users.

As a first formal test, I put together a focus group with ten participants to walk through the newest design and discuss their impressions and questions. While the focus group was able to provide answers to questions similar to those that were asked in the previous study, there are still clear issues with understanding many of the privacy concepts. For example, the differences between opt-out and opt-in confused several participants, who asked why there was a clear way to opt-out, but no method for opting-in.

The focus group demonstrated that the current design allows for easy privacy policy comparisons for consumers. Both the Nutrition Facts panel and the proposed Financial Privacy Notices were designed to promote easy comparison, in order to help consumers decide between two similar products. In the focus group I found that our participants were able to easily isolate and describe differences between two policies. We have yet to validate if comparisons are easier than with traditional text policies.

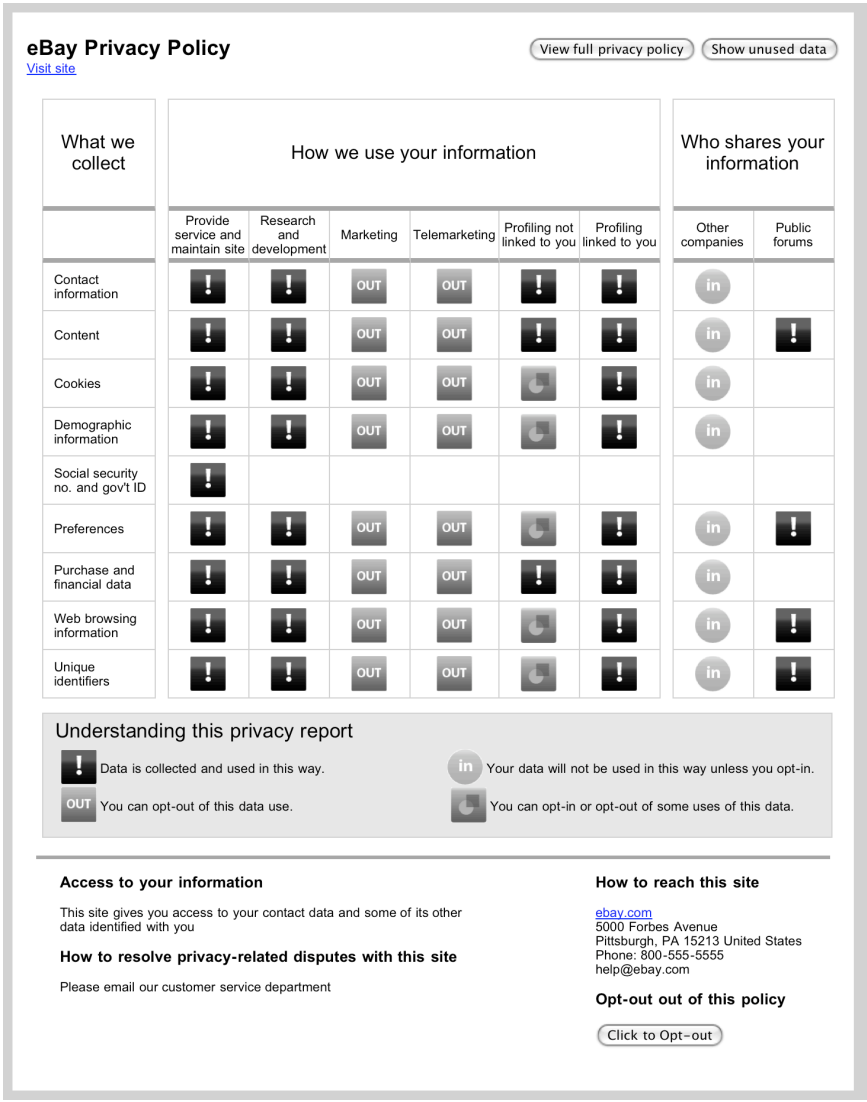


Figure 4. The most recent label design which was last tested in a ten person focus group, and is currently under-revision before more testing this spring.

"For me they say you can opt-in or opt-out of some uses of this data... It is not really confusing, but it is hiding something."

"This is more convenient than scrolling through reams and reams of paragraphs. I mean who reads them?"

"From an eye-sight standpoint, the exclamation marks really scared me. Warning!"

"I like the chart. [It's] better than long sentences."

– input from the focus group conducted on this, the present version of the Privacy Label.

Conclusion

As privacy becomes more relevant to consumers, and existing methods of communicating privacy policies are not successful, a new method of making this privacy policy information accessible must be developed. I presented an ongoing project that seeks to develop a usable privacy policy interface to empower consumers. By successfully, contextually explaining businesses' privacy policies to users, providing a trustworthy and consistent display of information, and assisting users in comparing online privacy policies, this work will allow consumers to better protect their privacy. However, for this to truly be successful it must be easy to understand and use. Continued efforts in refining, testing, and tuning the experience will be the key to creating an effective label for online privacy practices.

Acknowledgments

I would like to thank Rob Reeder, Joanna Bresee, Steve Won, and Aleecia McDonald, as well as my advisor on this project, Lorrie Cranor, for all of their assistance in providing feedback, suggestions, and guidance.

References

[1] Belser, B. Designing the Food Label: Nutrition Facts. *AIGA Journal.* 2007.

[2] Buckley, P. and Shepherd, R. Ergonomic factors: The clarity of food labels. *British Food Journal.* 1993. 95

[3] Cranor, L., Egelman, S., Sheng, S., McDonald, A., and Chowdhury, A. P3P Deployment on Websites. *Electronic Commerce Research and Applications*, Volume 7, Issue 3, Autumn 2008, Pages 274-293.

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

[5] The Energy Label. 2007. www.energyrating.gov.au

[6] Jensen, C. and Potts, C. Privacy policies as decision-making tools: an evaluation of online privacy notices. SIGCHI. 2004.

[7] Kelley, P., A. McDonald, R. Reeder, and L. Cranor. P3P Expandable Grids. Poster at Privacy MindSwap Carnegie Mellon University. 2007. http://cups.cs.cmu.edu/soups/2008/posters/kelley.pdf

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

[9] McDonald, A, and Cranor, L. The Cost of Reading Privacy Policies. Telecommunications Policy Research Conference, 2008.

[10] Reeder, R.W. *Expandable Grids: A user interface visualization technique and a policy semantics to support fast, accurate security and privacy policy authoring.* PhD thesis, Carnegie Mellon. 2008. http://www.robreeder.com/pubs/ReederThesis.pdf

[11] Reeder, R., Cranor, L., Kelley, P., and McDonald, A. A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. *Workshop on Privacy in the Electronic Society.* 2008

[12] Turow, J. Feldman, L., and Meltzer, K. Open to Exploitation: American Shoppers Online and Offline. The Annenberg Public Policy Center. 2005. http://www.annenbergpublicpolicycenter.org/NewsDetails.aspx?myId=31

[13] 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.

[14]W3C. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. http://www.w3.org/TR/P3P/