Intentional Design of Privacy Policies

Patrick Gage Kelley
Carnegie Mellon University
me@patrickgage.com

Lucian Cesca
Carnegie Mellon University
ljcesca@gmail.com

Joanna Bresee
NASA Ames Research Center
joanna.bresee@nasa.gov

Lorrie Faith Cranor
Carnegie Mellon University
lorrie@cs.cmu.edu

CHI 2011, May 7–12, 2011, Vancouver, BC, Canada.
ACM 978-1-4503-0268-5/11/05.

Abstract
Through an iterative design process, including focus groups and a laboratory study, we developed a standardized, tabular, "nutrition label" for online privacy policies. We tested the standardized format, two variants, and two real-world policy formats in a large, online user study to show that this label helps consumers. It was this intentional, iterative process that we believe led to our successes. By exploring people's current understanding of their information transactions online and migrating familiar concepts from the labeling and warning literature, we were able to create a more effective privacy-centered user interaction.

Keywords
Privacy policy, design, process, nutrition label, information design, standardization

ACM Classification Keywords
H.5.2 Information Interfaces and Presentation: User Interfaces; K.4.1 Computers and Society: Public Policy Issues-Privacy

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, consumers are, in theory, able to make informed decisions.

However, policies are commonly long, textual explanations of data practices, most frequently written by lawyers to protect companies against legal action. It has been established through numerous studies that people do not read privacy policies [9] and make mistaken assumptions based upon seeing that a site has a link to a privacy policy [10]. A recent study estimated that if consumers were somehow convinced to read the policies of all the companies they interact with, it would cost an estimated 365 billion dollars per year in lost productivity [8]. In addition, research has shown that consumers do not actually believe they have choices when it comes to their privacy. Based solely on expectations, they believe there are no options for limiting or controlling companies' use of their personal information [6].

In short, today's online privacy policies are failing consumers because finding information in them is difficult, consumers do not understand that there are differences between privacy policies, and policies take too long to read. The design of privacy policies has not matured in the past two decades. Our series of design investigations [5] and large scale testing [4] created a provably better format, yet we must now leverage those findings to bring this research to consumers.

Our Approach to Design

Our goal was to design a "Privacy Label" that is actually understandable, allows users to quickly find information, makes comparisons easy, and makes the experience of reading a privacy policy more enjoyable.

While many designs were tested and eventually re-factored or abandoned, each of the examples given below (Figure 1) show one of many variants of a similar vein. We have selected examples that we believe are representative of the major stages of our process. We applied in our designs many lessons from the labeling literature [1,2,3,11,12]. For example, putting a box around the label identifies the boundaries of the information, establishing a zone of trust; using bold rules to separate sets of related information defines each space, and providing a clear and boldface title communicates the label's purpose.

We held four, hour-long focus group sessions to review designs and discuss participants' impressions and questions. Our participants compared several of the designs below alongside full text, status-quo policies. The participants reacted positively to the tabular formats. For example, one participant stated, "This is more convenient than scrolling through reams and reams of paragraphs. I mean who reads them?" and another participant said, "I like the chart. [It's] better than long sentences." We found that even in simpler formats, some participants still had problems understanding privacy concepts. For example, one participant asked, "What is the difference between opt-in or opt-out?" As an example, most participants were familiar with profiling, but did not understand the difference between "Profiling linked to you" and "Profiling not linked to you." We focused on their understandings of these commonly used terms from real-world privacy policies, and from this vein of feedback, including a list of useful terms/definitions.

After the first two focus groups we performed a 24-participant laboratory user study comparing a standard full text privacy policy with privacy policies presented in our privacy nutrition label style. At a high level, people were able to answer more questions correctly with the

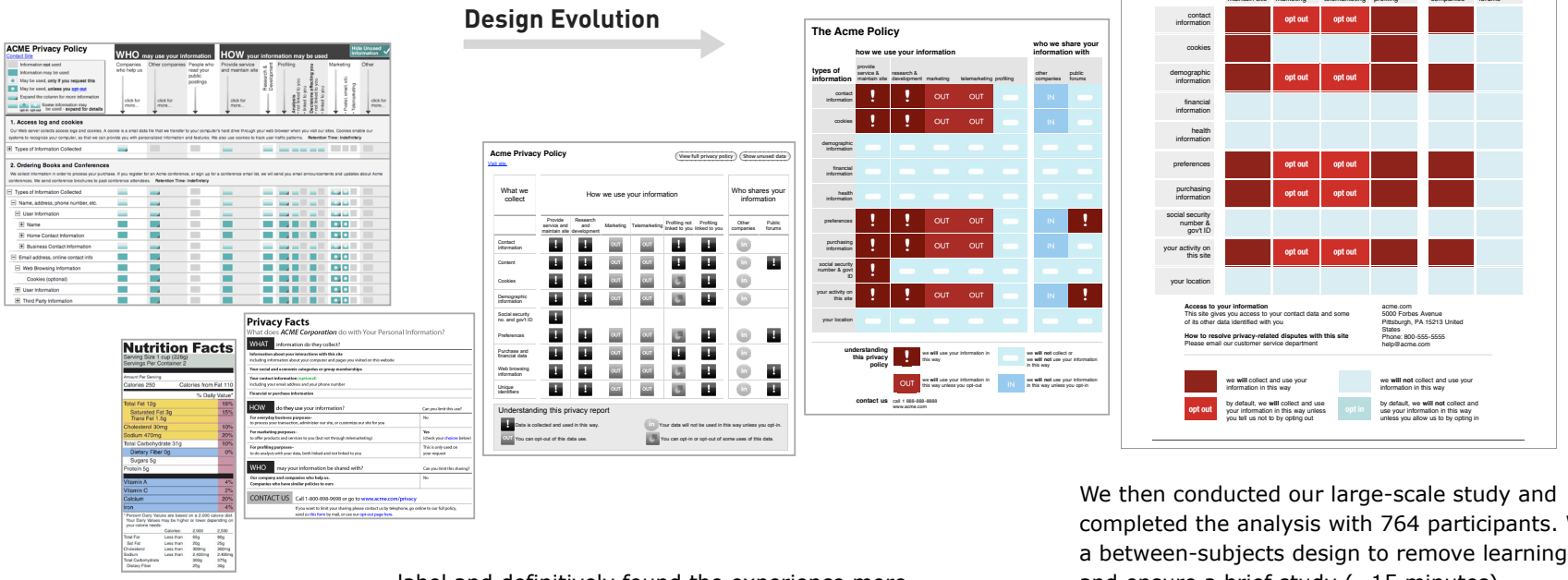

Figure 1: Our design evolution through the course of focus groups, laboratory studies, informal testing, and a large-scale test.

Nutrition Facts Panel courtesy of the U.S. Food and Drug Administration. www.fda.gov.

label and definitively found the experience more pleasurable, even given their familiarity with text policies against their first experience using our label.

To follow up our design process and testing with a full-scale experiment, we tested five privacy policy formats, three of our own standardize label-style formats, and two that exist online today. We conducted an online user study using Amazon's Mechanical Turk. In preparation for this study we first performed three smaller pilot tests of our survey framework. We ran ourpilot studies with approximately thirty users each, across 2-3 conditions. Our pilot studies added another level of iteration, and real interaction with users, helping us to finalize remaining design decisions surrounding the standardized short table, refine our questionnaire, and test our survey framework.

We then conducted our large-scale study and completed the analysis with 764 participants. We chose a between-subjects design to remove learning effects and ensure a brief study (~15 minutes).

Participants in each condition followed the same protocol; only the policy format differed. In terms of accuracy, the three standardized formats scored 62-69%, while the two real-world text policies, scored 43-46%. The standardized policies significantly outperformed the full-text policy. Our standardized formats also significantly outperformed the full text policy in overall time to answer questions.

The comments provided by participants at the end of the study provide insights into their enjoyment. Participants who saw the full text described privacy policies as a "torture to read and understand" and likened them to "Japanese Stereo Instructions." On the other hand, participants in the standardized-format

conditions were more complimentary, one said: "This layout for privacy policies is MUCH more consumer friendly. I hope this becomes the industry standard."

Conclusion

Now, we are confronted with making this participant's hope a reality, making the industry-standard privacy policy designed with the consumer's experience in mind. The final label design allows for information to be found in the same place every time. It removes wiggle room and complicated terminology by using four standard symbols that can be compared easily. It allows for quick high-level visual feedback by looking at the overall intensity of the page, can be printed, fits in a browser window, and has a glossary of useful terms.

Our design approach allowed us to explore other efforts in standardizations, labeling, and designing privacy policy formats, while quickly and iteratively building a library of testable formats, resulting in a better experience for consumers to understand privacy policies. Yet before this label can truly benefit the people it was designed for, we must convince industry to support our methodology and the resultant design.

Acknowledgements

The design team included Aleecia McDonald, Robert Reeder, and Sungjoon Steve Won. Thanks to Cristian Bravo-Lillo, Robert McGuire, Norman Sadeh, Clare-Marie Karat, and Janice Tsai. This work was supported in part by U.S. Army Research Office contract DAAD19-02-1-0389 to Carnegie Mellon University's CyLab, by NSF Cyber Trust grant CNS-0627513, by Microsoft through the Carnegie Mellon Center for Computational Thinking, ICTI, and the IBM OCR project on Privacy and Security Policy Management.

References

[1] Balasubramanian S. and C. Cole. Consumers' search and use of nutrition information: The challenge and promise of the nutrition labeling and education act. In *Journal of Marketing*, 2002.

[2] Belser, B. Designing the Food Label: Nutrition Facts. *AIGA Journal*. 1994.

[3] Drichoutis AC, Lazaridis P, Nayga RM. Consumers' use of nutritional labels: a review of research studies and issues. *Acad Marketing Sci Rev*. 2006.

[4] Kelley, P.G., L. Cesca, J. Bresee, and L. Cranor. Standardizing privacy notices: An online study of the nutrition label approach. *CHI* 2010.

[5] Kelley, P.G., J. Bresee, L.F. Cranor, and R.W. Reeder. A "Nutrition Label" for Privacy. *SOUPS*, 2009.

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

[7] Levy, A. and Hastak, M. Consumer Comprehension of Financial Privacy Notices. December 2008. http://www.ftc.gov/privacy/privacyinitiatives/Levy-Hastak-Report.pdf.

[8] McDonald, A, and Cranor, L. The Cost of Reading Privacy Policies. *TPRC*, 2008.

[9] Privacy Leadership Initiative. Privacy Notices Research Final Results, 2001, http://understandingprivacy.org.

[10] Turow, J. Feldman, L., and Meltzer, K. Open to Exploitation: American Shoppers Online and Offline. The Annenberg Public Policy Center. 2005.

[11] 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.

[12] U.S. Food and Drug Administration. "Guide to Nutrition Labeling and Education Act Requirements" 1994. http://www.fda.gov/ora/inspect_ref/igs/nleatxt.html.