

Designing a Privacy Label

Assisting Consumer Understanding of Online Privacy Practices

Patrick Gage Kelley

Overview

- Privacy policies are difficult for users to read and understand
- We are continuing to refine a privacy label based on nutrition, drug, and energy labels as well as financial privacy notifications and our earlier trials
- The Platform for Privacy Preferences, P3P, is a W3C machine readable (XML) format for website privacy policies
- For consumers to benefit from this standardized policy, end user agents must exist that present the data so that users **understand** the policy

Goals

Design a “Privacy Label” that:

- **Is actually understandable**, including privacy concepts, terminology, and symbols
- Allows users to **quickly and efficiently find information**
- **Makes comparisons easy** between different companies through a standardized form

Design Iteration

ACME Privacy Policy

WHO may use your information: Companies who help us, Other companies, People who read your public postings

HOW your information may be used: Provide service and maintain site, Research & Development, Profiling, Analyze information linked to you, Decisions affecting you (not linked to you, linked to you), Marketing, Other

1. Access log and cookies

2. Ordering Books and Conferences

- Our original design was based off of Reeder’s Expandable Grids [3]
- This included following the principle of displaying the entire policy, hierarchically, allowing users to drill down to what they believe is important
- However, we found that this design had many flaws including: unclear labels, P3P statements displayed separately, and too many confusing symbols [2]
- Additionally, we found users rarely expanded the rows and columns

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%

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

- Based on labeling literature (including drug, energy, water, nutrition, and financial privacy) we simplified the design
- We included bold labels, lines separating sections, a descriptive header, and more apparent opt-out links
- To simplify the policy information, we combined many categories together and wrote longer descriptions of each

eBay Privacy Policy

View full privacy policy | Show unused data

What we collect	How we use your information						Who shares your information	
	Provide service and maintain site	Research and development	Marketing	Telemarketing	Profiling not linked to you	Profiling linked to you	Other companies	Public forums
Contact information	!	!	OUT	OUT	!	!	in	
Content	!	!	OUT	OUT	!	!	in	!
Cookies	!	!	OUT	OUT	!	!	in	
Demographic information	!	!	OUT	OUT	!	!	in	
Social security no. and gov't ID	!							
Preferences	!	!	OUT	OUT	!	!	in	!
Purchase and financial data	!	!	OUT	OUT	!	!	in	
Web browsing information	!	!	OUT	OUT	!	!	in	!
Unique identifiers	!	!	OUT	OUT	!	!	in	!

Understanding this privacy report

! Data is collected and used in this way.

OUT You can opt-out of this data use.

in Your data will not be used in this way unless you opt-in.

! You can opt-in or opt-out of some uses of this data.

- Our early grid label reintroduced symbols for collected data, opt-in, opt-out, and mixed use, which range from light to dark based on severity
- This version again expands, with a single fully expanded state and a default view that shows most of the relevant information
- We focused on creating a single page label that is printable and designed for easy comparison of multiple policies

Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A “Nutrition Label” for Privacy. Under-review for SOUPS 2009.

Robert W. Reeder. 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.

Robert Reeder, Lorrie Faith Cranor, Patrick Gage Kelley, and Alecia McDonald. A User Study of the Expandable Grid Applied to P3P Privacy Policy Visualization. Workshop on Privacy in the Electronic Society. 2008

The Acme Policy

types of information	how we use your information					who we share your information with	
	provide service & maintain site	research & development	marketing	telemarketing	profiling	other companies	public forums
contact information	!	!	OUT	OUT	☐	IN	☐
cookies	!	!	OUT	OUT	☐	IN	☐
demographic information	☐	☐	☐	☐	☐	☐	☐
financial information	☐	☐	☐	☐	☐	☐	☐
health information	☐	☐	☐	☐	☐	☐	☐
preferences	!	!	OUT	OUT	☐	IN	!
purchasing information	!	!	OUT	OUT	☐	IN	☐
social security number & govt ID	!	☐	☐	☐	☐	☐	☐
your activity on this site	!	!	OUT	OUT	☐	IN	!
your location	☐	☐	☐	☐	☐	☐	☐

A bold title is used to set the context for the information.

Short labels are used for column and row headers, with longer definitions on our Useful Terms page.

Information that is not collected has a saturated label and a row full of the lightest symbol.

Four symbols on a scale from light to dark are used to indicate the severity of certain privacy practices.

Row and column locations are consistent so that two policies side-by-side can be easily visually compared.

understanding this privacy policy



we will use your information in this way



we will not collect or we will not use your information in this way



we will use your information in this way unless you opt-out



we will not use your information in this way unless you opt-in

contact us call 1 888-888-8888
www.acme.com

A legend provides information about what each symbol means.

User Testing

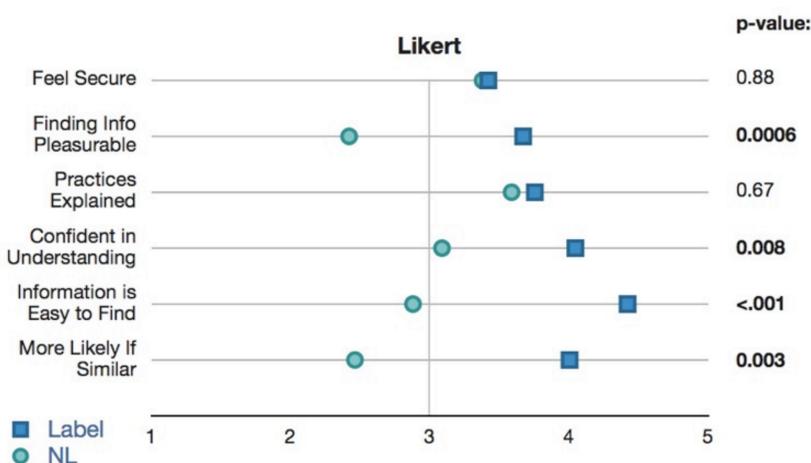
We held two, hour-long focus group sessions to explore the promise of our design possibilities

- The first was conducted to review the early grid label design
- The second compared the simple text label to our final prototype above

With the final proposed label we ran a 24-participant laboratory user study to compare the label to a text policy

- Using a within-subjects design, participants saw both text and label
- Participants completed eight tasks and were then asked a series of qualitative questions to assess the experience

Preliminary Results



Additionally, subjects were more accurate and completed the tasks in less time. [1]

Many focus group participants directly shared that they preferred the label design:

“I like the chart. [It’s] better than long sentences.”

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

Our laboratory study backs up the results showing that users of the label significantly indicated they:

- Were more confident in their understanding
- Believed information was easier to find
- Found information finding more pleasurable

Conclusion

The final label design we have proposed here:

- Allows for information to be found in the same place every time
- Removes wiggle room and complicated terminology by using four standard symbols
- Allows for quick high-level visual feedback by looking at the overall intensity of the page
- Can be printed, fits in a standard browser window
- Has a glossary of useful terms attached
- And **most importantly people who have used it** to find privacy information **have rated it as** not just more pleasurable than text, but **actually enjoyable**

Next Steps

Examine accuracy and comparison results of label vs. natural language

Run tests on a larger segment of the populace in an online study

Integrate the label with PrivacyFinder.org, a privacy-enhanced search engine, so that people are provided with privacy information as they conduct searches online

I would like to acknowledge Janice Tsai, Sungjoon Steve Won, Robert Reeder, Aleecia McDonald, Daniel Rhim, Robert McGuire, Cristian Bravo-Lillo, Norman Sadeh, and everyone who provided input throughout the design process, as well as my advisor on this project, Lorrie Cranor. Without her insights this work would never have been possible

