Designing a Privacy Label

Assisting Consumer Understanding of Online Privacy Practices

Patrick Gage Kelley

Overview

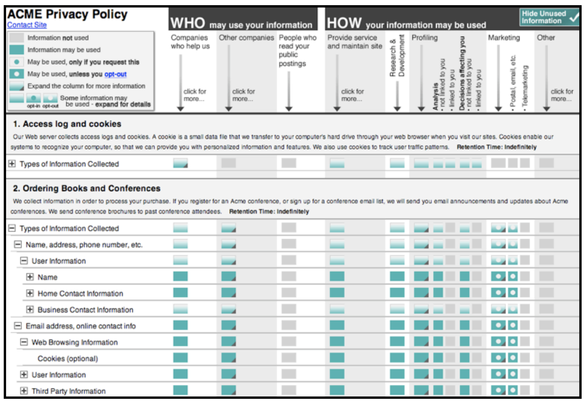
- Privacy policies are difficult for users to read and understand
- We are continuing to refine a privacy label based on nutrition, drug, and energy labels as well as financial privacy notifications and our earlier trials
- The Platform for Privacy Preferences, P3P, is a W3C machine readable (XML) format 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

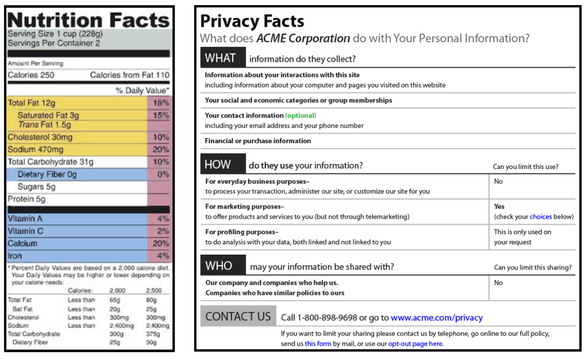
Design a "Privacy Label" that:

- **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

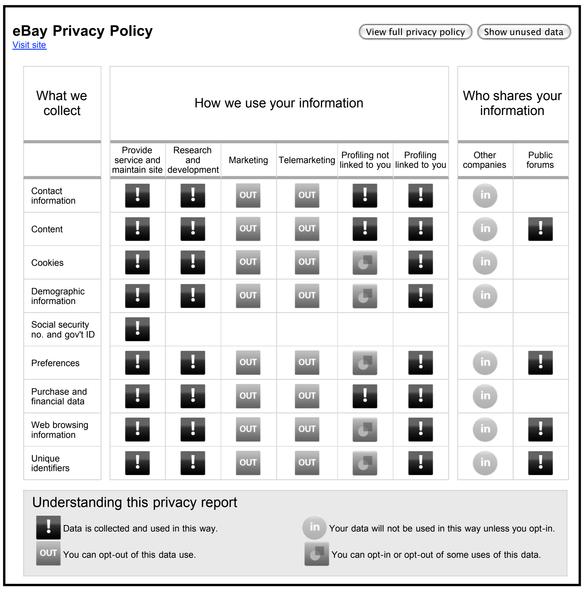
Design Iteration



- 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



- 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



- 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 Aleecia 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: provide service & maintain site	research & development	marketing	telemarketing	profiling	who we share your information with: 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							

understanding this privacy policy

- ! — we **will** use your information in this way
- OUT — we **will** use your information in this way unless you opt-out
- (light) — we **will not** collect or we **will not** use your information in this way
- IN — we **will not** use your information in this way unless you opt-in

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

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.

A legend provides information about what each symbol means.

User Testing

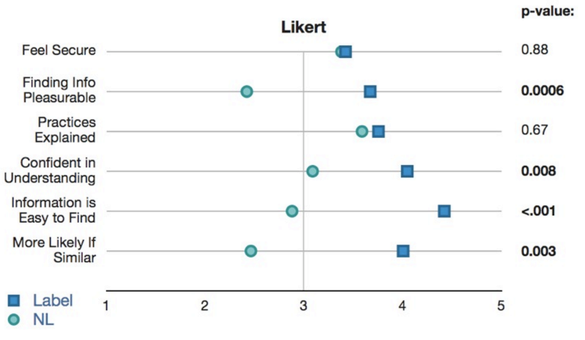
We held two, hour-long focus group sessions to explore the promise of our design possibilities

- 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

CMU Usable Privacy & Security Laboratory
HTTP://CUPS.CS.CMU.EDU