

Standardizing Privacy Notices

Privacy Taxonomy,
Privacy Nutrition Labels, &
Computer-Readable Policies

Lorrie Faith Cranor

February 2011

**Carnegie
Mellon
University**

CyLab 

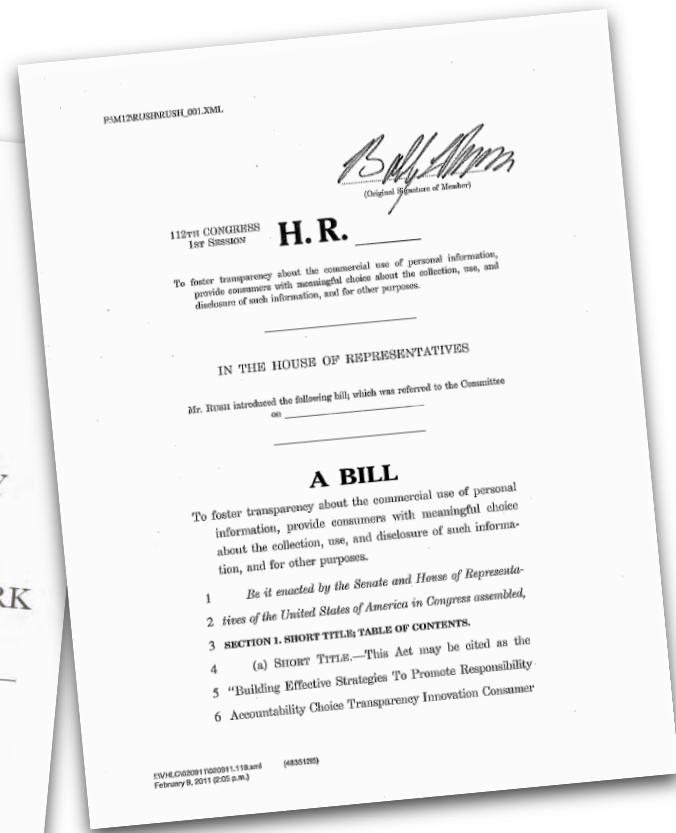
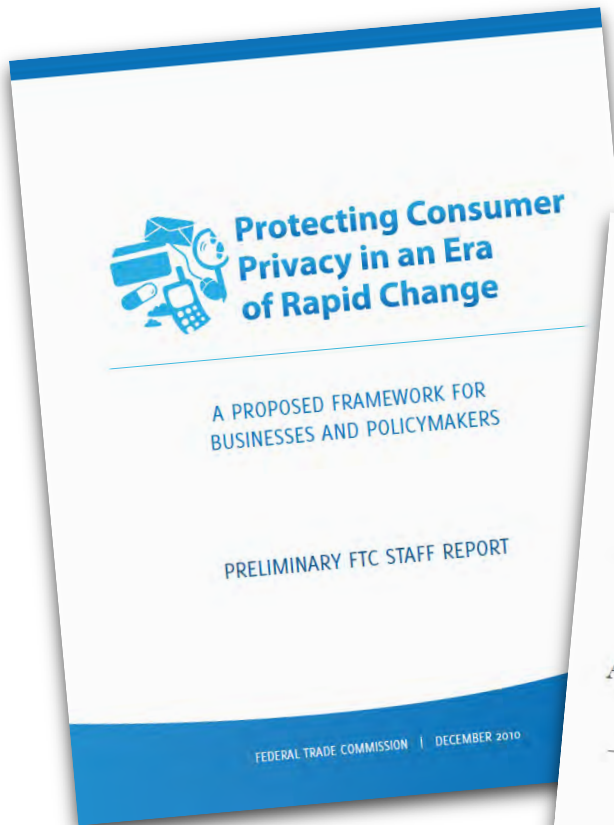
isr institute for
SOFTWARE
RESEARCH

**ENGINEERING &
PUBLIC POLICY**



Currently, the government is indeed paying substantial attention to privacy issues on several fronts. The **Federal Trade Commission is conducting a long-term Privacy Initiative** and is planning a privacy workshop to study technical tools and self-regulatory models.... the **Commerce Department... is compiling a report on the issues around privacy self-regulation.** “As a general matter,” says [the] NTIA chief counsel ..., “we favor self-regulation, but self-regulation with teeth....”there are also **several bills pending in Congress**....

– Esther Dyson
Release 1.0.
19 February 1997



December 2010 – February 2011

Lots of talk about
standardizing privacy notices

Advertising option icon

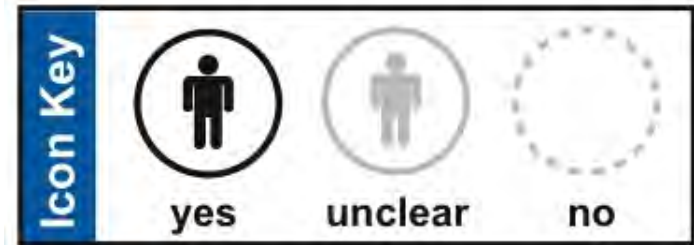












AdChoices: Learn More About This Ad

KnowPrivacy

<http://knowprivacy.org>

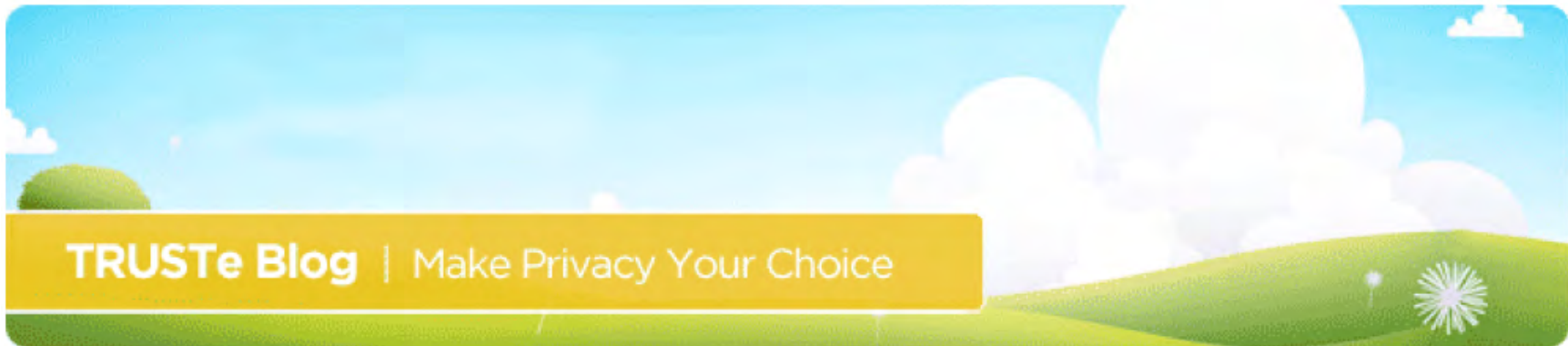
UC Berkeley student project, June 2009



TYPE OF DATA COLLECTED	GENERAL DATA PRACTICES	DATA SHARING
 <p>contact: name, mailing address, email, or phone number</p>	 <p>ad customization: user data may be used for the purpose of customizing advertising</p>	 <p>affiliates: affiliates and subsidiaries bound by the same privacy practices</p>
 <p>computer: IP address, browser type, or operating system</p>	 <p>third party tracking: site allows third parties to place advertisements that may track user behavior</p>	 <p>contractors: third party contractors bound by the same privacy practices</p>
 <p>interactive: browsing behavior or search history</p>	 <p>public display: service allows users to contribute information which may be displayed publicly</p>	 <p>third parties: third parties not subject to same data practices</p>
 <p>financial: account status or activity, credit information, or purchase history</p>	 <p>user control: users allowed to access and correct personal data collected</p>	
 <p>content: contents of personal communications, stored documents or media</p>	 <p>data retention: explicitly stated duration of retention for personal data collected</p>	

September 14, 2010

<http://www.truste.com/blog/?p=879>



At TRUSTe we've debated what privacy enhancing technology we should support to achieve a more automated system ensuring website privacy transparency and simplified user choice. We've reached an informal consensus that **machine-readable XML policies** are a relevant standard to support in the future, a position that I anticipate discussing further in a future blog post, so stay tuned.

P Privacy Icons

<http://www.azarask.in/blog/post/privacy-icons/>

2010



Your Data is Used Only for the Intended Use



Your Data May be Used for Purposes You Do Not Intend



Your data is never given to advertisers.



Site gives your data to advertisers.



Your data is never bartered or sold.



Your data may be bartered or sold.



Data is given to law enforcement only when legal process is followed.



Data may be given to law enforcement even when legal process is not followed.

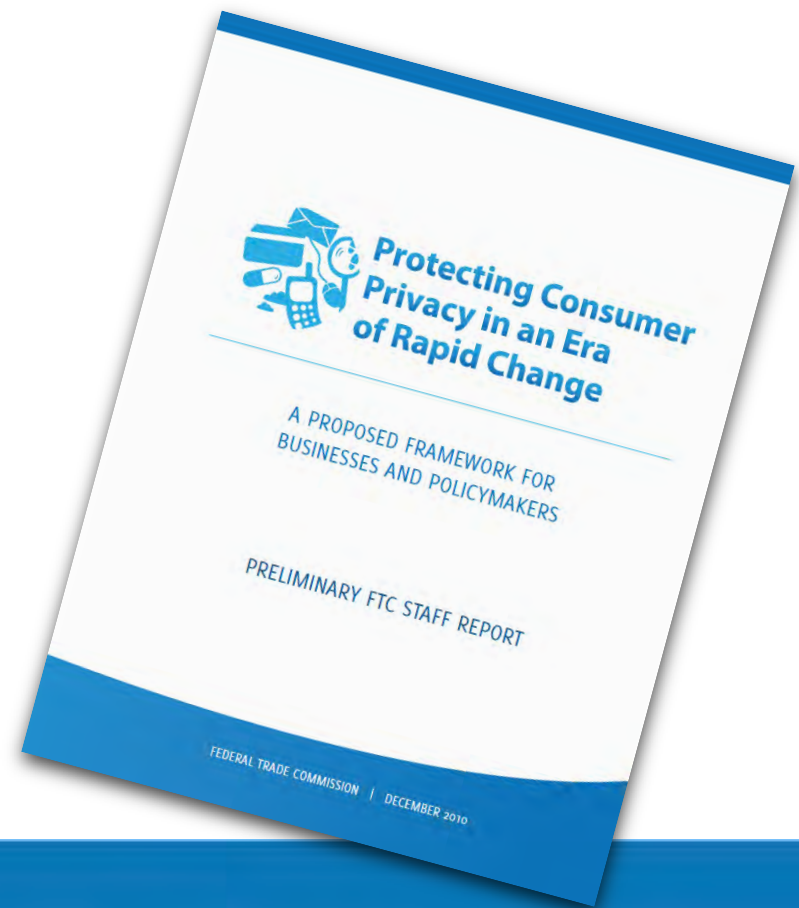


Your data is kept for less than 1 month.



Your data may be kept indefinitely.

December 2010



GREATER TRANSPARENCY

Companies should increase the transparency of their data practices.

- Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices.



Happy New Year from the Future of Privacy Forum

January 2011

Our First Annual List of Privacy Ins and Outs

OUT

Coolnet (the tracking land)

FIPPS light

Self-Regulation

Boucher-Stevens Bill

Bored Privacy Notices

No Practices Are Acceptable

Privacy by Fortuity

Only online data protected

Global skepticism of US privacy commitment

None of your business is what data we have

IN

Cupcake (sold in a mobile truck)

The full FIPPS

Self-Regulation

Bill

Nutritional Label Privacy Notices

Commonly Accepted Practices

Privacy by Design

Business made in a fishbowl protected

Recognition of FTC in official global

Data Protection Authority group

BILL MURRAY ANDIE MACDOWELL

GROUNDHOG DAY

GROUNDHOG DAY

15th ANNIVERSARY SPECIAL EDITION



SPECIAL 15TH ANNIVERSARY EDITION

DVD



"BUILDING TRUST AND CONFIDENCE IN ELECTRONIC TRANSACTIONS"

- story
- FAQ
- members
- marks
- contact
- news
- verification
- pilot

eTRUST Mission

eTRUST's mission is to establish trust and confidence in electronic transactions. The organization seeks to promote the mass adoption of electronic commerce by creating an infrastructure to establish and evolve guidelines on issues such as privacy, security and authentication.

eTRUST's first project addresses online privacy . The organization has developed and will license recognizable and credible symbols, "trustmarks" of privacy and security to on-line merchants.

The ultimate beneficiaries of the eTRUST program will be online users who will be better able to make informed choices.



Design by [Tsuchiya Sloneker Communications](#)
Production by [Pacific Digital Interactive](#)

[| Story](#) | [FAQ](#) | [Members](#) | [Marks](#) | [Contact](#) | [News](#) | [Verification](#) | [Pilot](#) |



December 1996

2002

"The World Wide Web Consortium, the group that designs standards for the Web, is creating a new way [P3P] for Web sites to transmit the site's privacy policy automatically, and allow users to signal only the information they are willing to share."

**— *The New York Times*
2/22/2000**

"The Platform for Privacy Preferences (P3P) is the most sophisticated proposal that has been made from a technical perspective so far to enhance privacy protection on the Web... [while] it cannot replace a regulatory framework of legislation, contracts, or codes of conduct... it [can] operate within such a framework."

**— Dr. Alexander Dix, LL.M.,
Commissioner for Data
Protection and Access
to Information,
State of Brandenburg, Germany**

"P3P will help responsible online businesses empower users to choose the privacy relationship best for them."

**— Christine Varney,
former FTC Commissioner**

"In the context of proper legislation, P3P is the most promising solution to cyberspace privacy. It will make it easy for companies to explain their practices in a form that computers can read, and make it easy for consumers to express their preferences in a way that computers will automatically respect."

**— Professor Lawrence Lessig,
Stanford Law School**

Outline

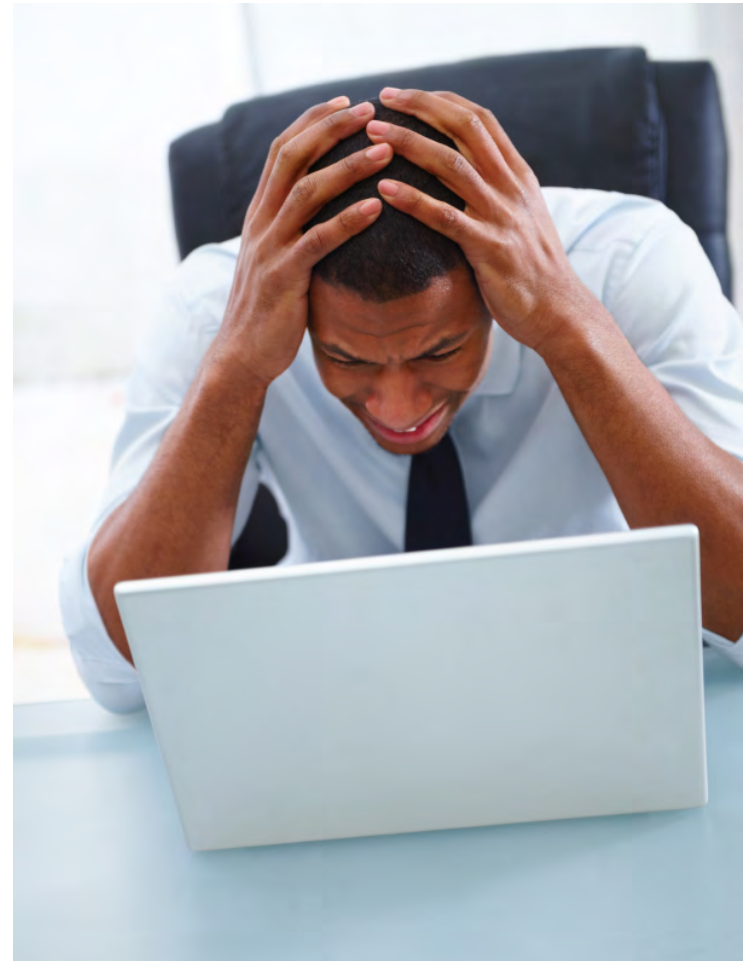
- Introduction to P3P
- A privacy taxonomy
- Privacy nutrition labels
- Adoption and enforcement
- Conclusions and recommendations

Platform for Privacy Preferences (P3P)

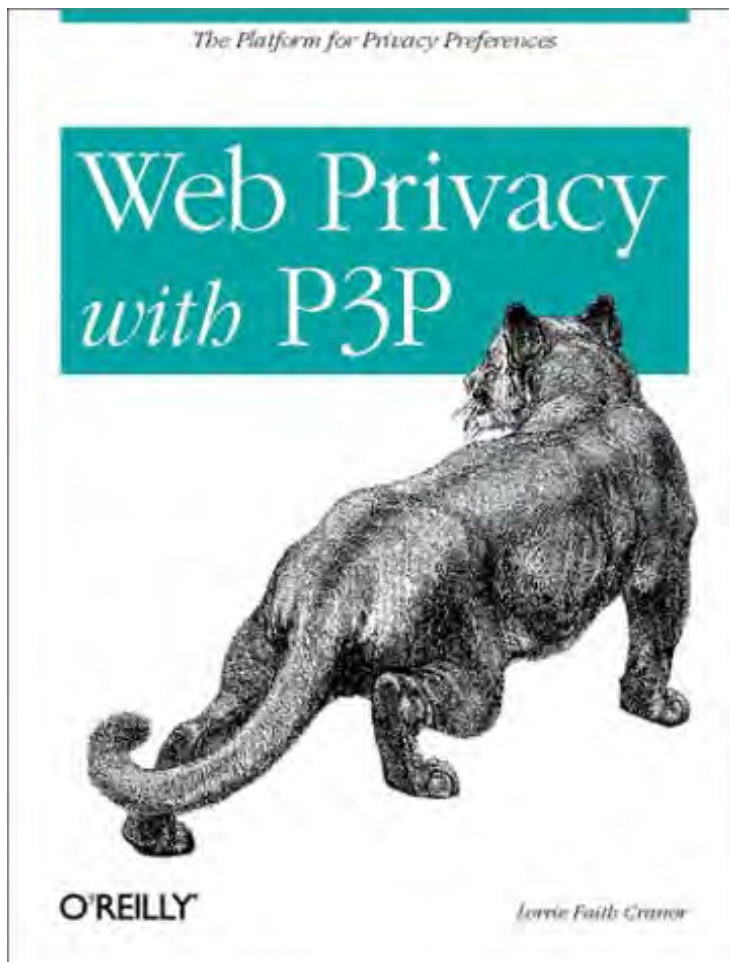
Nobody wants to read privacy policies

“the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand”

Protecting Consumer Privacy in an Era of Rapid Change. Preliminary FTC Staff Report. December 2010.



Let your computer read for you



- Platform for Privacy Preferences (P3P)
- W3C specification for XML privacy policies
- Optional P3P compact policy HTTP headers to accompany cookies
- Implemented in Internet Explorer 6, 7, 8

A brief history of P3P

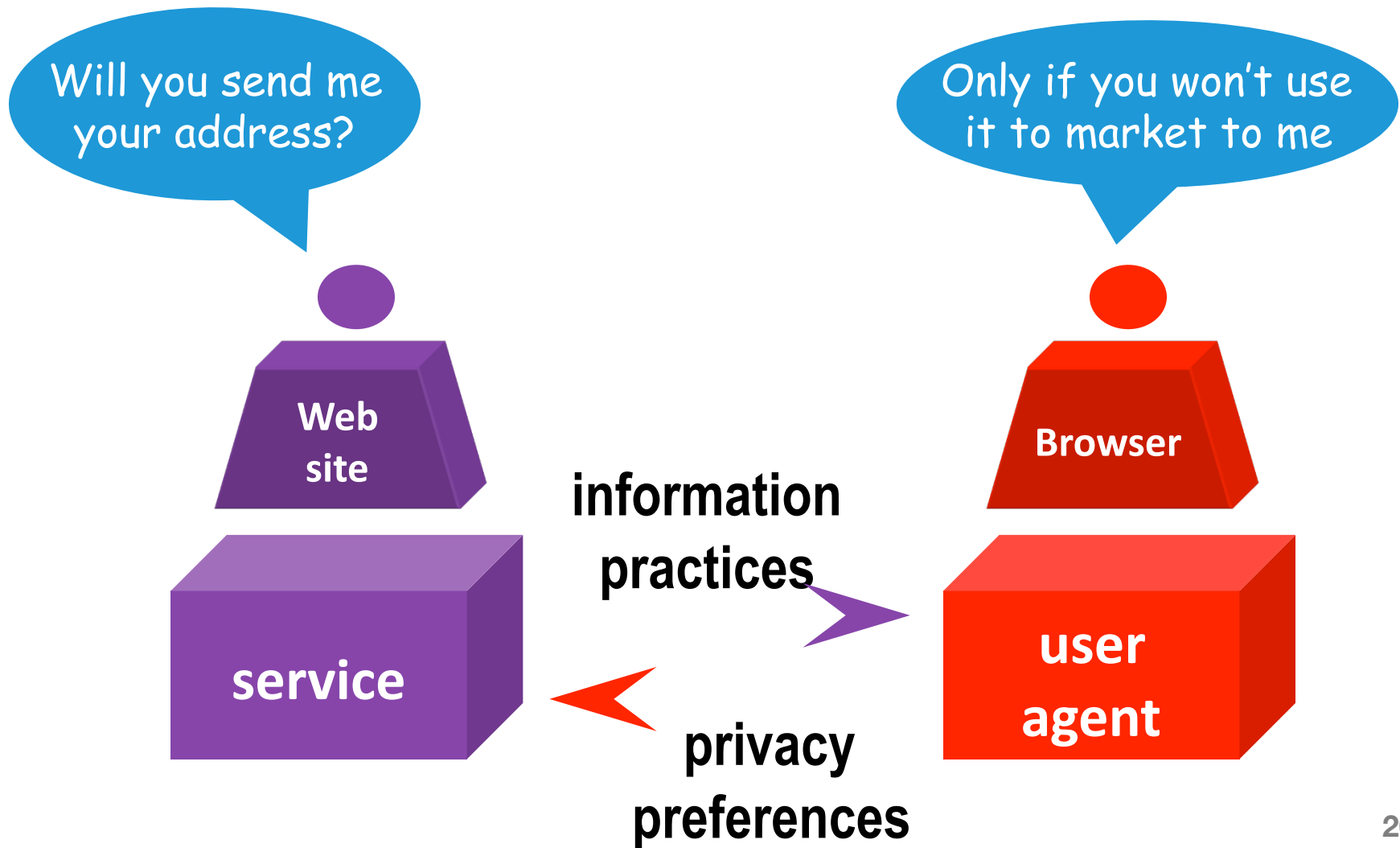
- November 1995: Idea discussed at FTC meeting
- Fall 1996: Internet Privacy Working Group convened
- Summer 1997: W3C began working on P3P
 - Several working groups chartered
 - Numerous public working drafts, changes based on feedback
 - Early ideas about negotiation and agreement ultimately removed
 - Automatic data transfer added and then removed
 - Patent issue stalled progress, but ultimately became non-issue
- April 16, 2002: P3P issued as W3C Recommendation
<http://www.w3.org/TR/P3P/>
- November 2006: P3P 1.1 working group issued Note and closed

Original Idea behind P3P

- A framework for automated privacy discussions
 - Web sites disclose their privacy practices in standard machine-readable formats
 - Web browsers automatically retrieve P3P privacy policies and compare them to users' privacy preferences
 - Sites and browsers can then negotiate about privacy terms

P3 circa 1997

Seamless Information Exchange



P3P1.0 – A first step

- Offers an easy way for web sites to communicate about their privacy policies in a standard machine-readable format
 - Can be deployed using existing web servers
- This will enable the development of tools that:
 - Provide snapshots of sites' policies
 - Compare policies with user preferences
 - Alert and advise the user

P3P1.0 spec defines

- A standard vocabulary for describing uses, recipients, data categories, and other privacy disclosures
- A standard schema for data a Web site may wish to collect (base data schema)
- An XML format for expressing a privacy policy in a machine readable way
- A means of associating privacy policies with Web pages
- A protocol for transporting P3P policies over HTTP
- A compact policy format for expressing a summarized policy for cookies, transmitted in an HTTP header

P3P/XML encoding

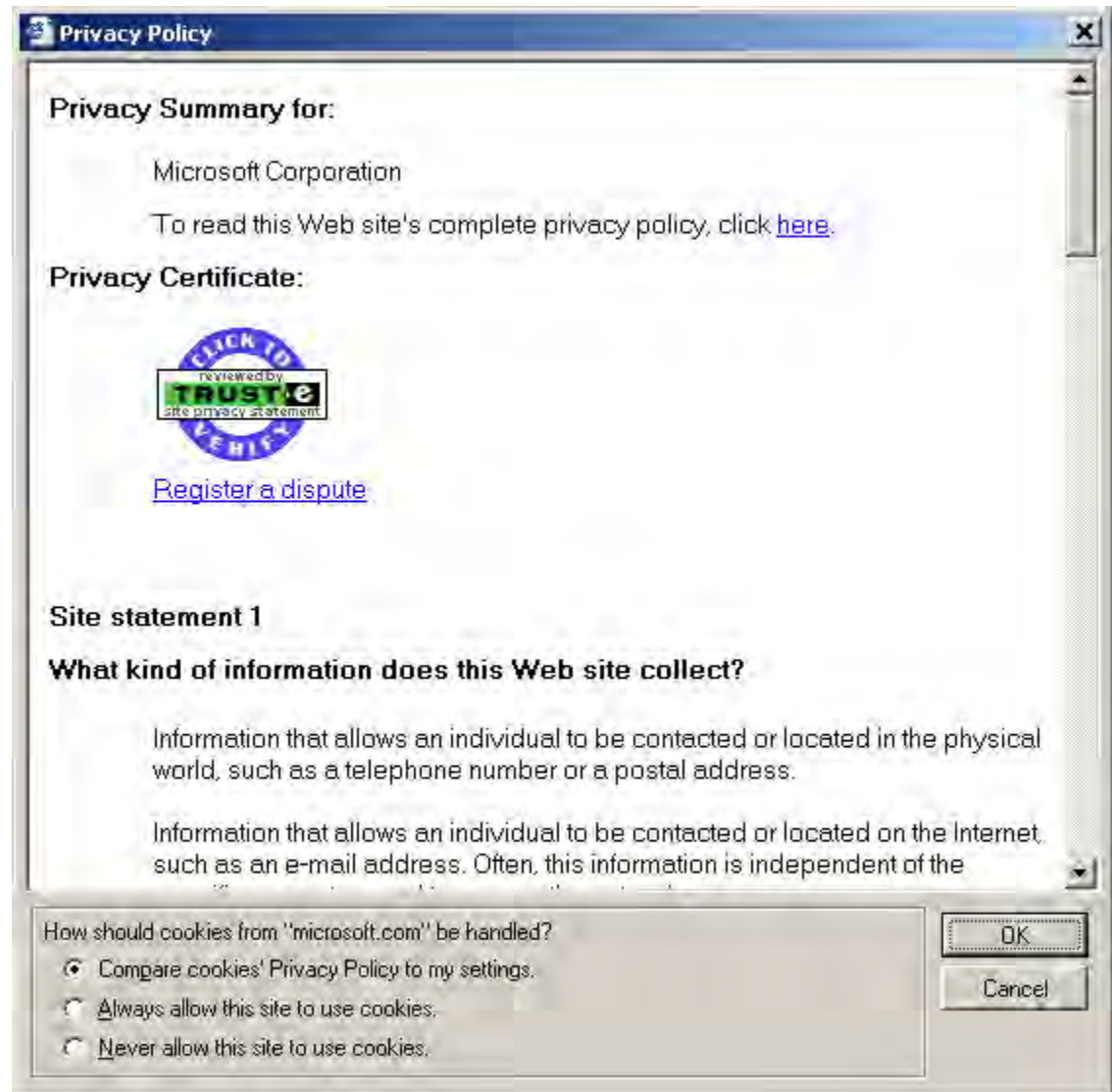
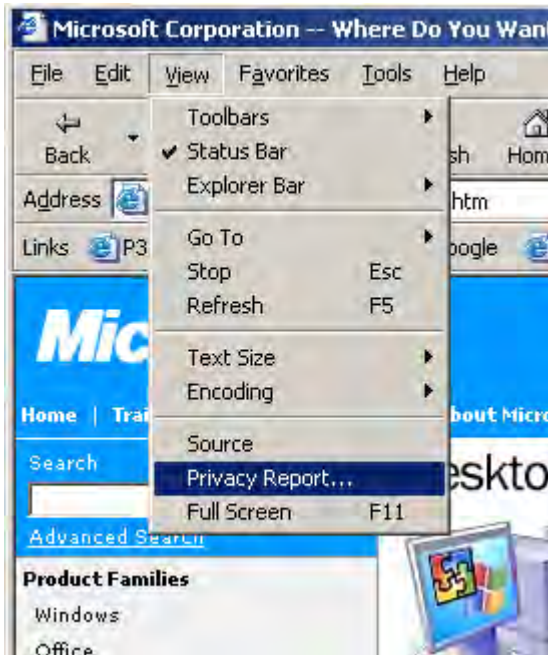
```
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
<POLICY discuri="http://p3pbook.com/privacy.html"
  name="policy">
  <ENTITY>
  <DATA-GROUP>
    <DATA
      ref="#business.contact-info.online.email">privacy@p3pbook.com
    </DATA>
    <DATA
      ref="#business.contact-info.online.uri">http://p3pbook.com/
    </DATA>
    <DATA ref="#business.name">Web Privacy With P3P</DATA>
  </DATA-GROUP>
  </ENTITY>
  <ACCESS><nonident/></ACCESS>
  <STATEMENT>
    <CONSEQUENCE>We keep standard web server logs.</CONSEQUENCE>
    <PURPOSE><admin/><current/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA ref="#dynamic.clickstream"/>
      <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
</POLICIES>
```

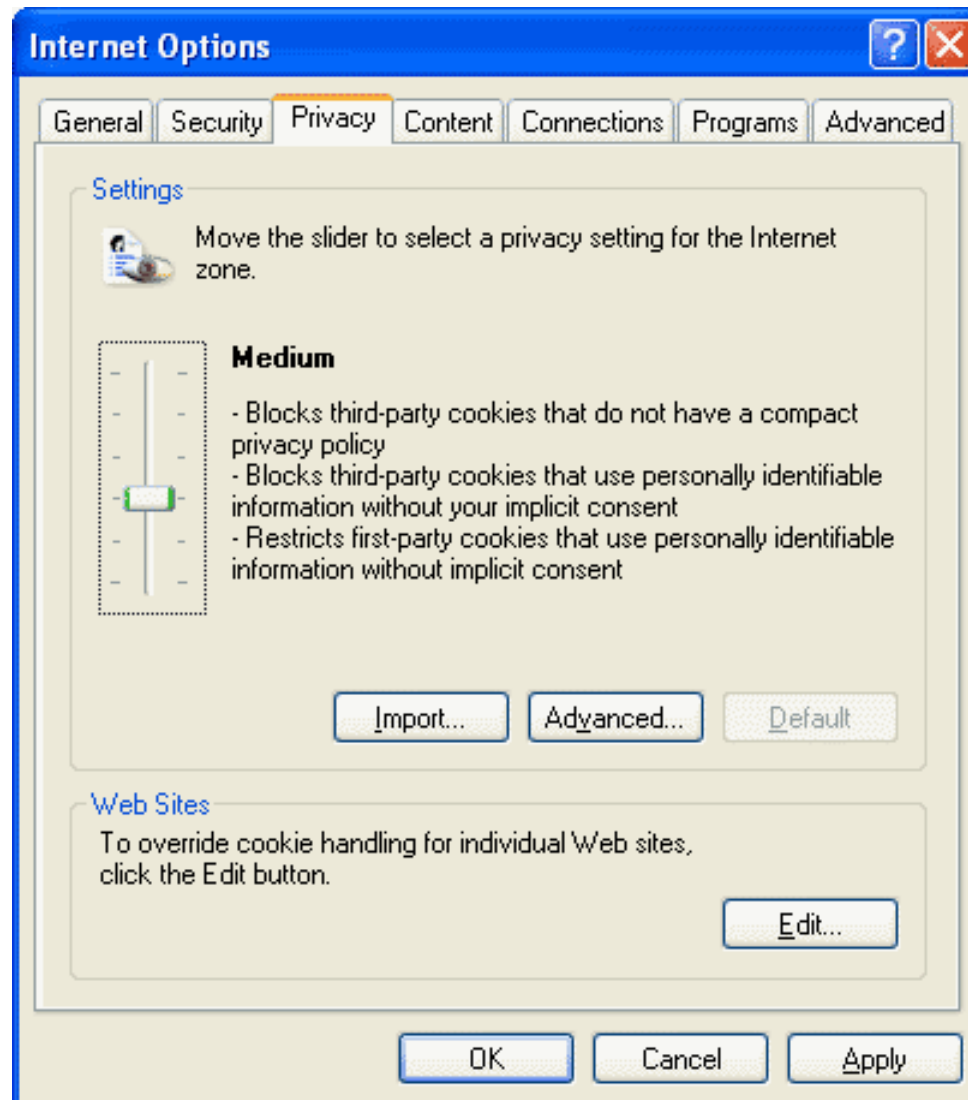
P3P in IE6

The screenshot shows a Microsoft Internet Explorer 6 browser window displaying the Gigalaw.com website. A "Privacy Report" dialog box is open, showing a table of blocked cookies. The table has two columns: "Site" and "Cookies".

Site	Cookies
http://rcm.amazon.com/e/cm?t=gigalawcom&l=st1&...	Blocked
http://rcm-images.amazon.com/images/P/00286422...	Blocked
http://rcm-images.amazon.com/images/G/01/rcm/1...	Blocked

The dialog box also includes a "Show:" dropdown menu set to "Restricted Web sites", a "Summary" button, and a "Settings..." button. The background website features various legal topics like "Crime", "Politics", and "Privacy".





Privacy Finder

- Privacy Finder search engine
- Checks each search result for computer-readable P3P privacy policy, evaluates against user's preferences
- Composes search result page with privacy meter annotations and links to "Privacy Report"
- Allows people to comparison shop for privacy
- <http://privacyfinder.org/>



PrivacyFinder

http://www.privacyfinder.org/ nutrition label

[Win prizes and help our research](#)
[Login here](#) if you already signed up



shoes Search

Search Engine: Google Yahoo! Shopping

Preference Level: Medium

Install the Privacy Finder [search bar!](#)
Compatible with Firefox 2 and Internet Explorer 7

[Frequently Asked Questions](#) | [Privacy Policy](#) | [Add A Site](#) | [Download Privacy Bird® Software](#) | [Privacy Finder 日本語版](#)


Privacy Finder is a public service provided by [CMU Usable Privacy and Security Laboratory](#)

Demo

PrivacyFinder Search for: shoes

http://www.privacyfinder.org/?q=shoes&Search=Search&a nutrition label

[Win prizes and help our research](#)
[Login here](#) if you already signed up

 shoes

Search Engine: Google Yahoo! Shopping

Preference Level:

[Dress, Casual & Athletic Shoes | Zappos.com](#)
[Privacy Report](#) Online shoe store selling a variety of brand name men's and women's footwear.
<http://www.zappos.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)

[Nike.com - Shop the Official NikeStore](#)
[Privacy Report](#) Designs, develops, and markets footwear, apparel, equipment, and accessory products. Explore Nike's site to shop online, customize products, and find a local store.
<http://www.nike.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)

[Onlineshoes.com - official site](#)
[Privacy Report](#) Shop online for name brand shoes at Onlineshoes.com. Choose from over 170 brands. Enjoy free shipping and exchanges, plus 110% price guarantee on all shoes.
<http://www.onlineshoes.com/> - No Cache - [Privacy Policy](#) - [Similar Pages](#)

[Shoes from Shoebuy.com - Free Shipping & Return Shipping](#)
[Privacy Report](#) Sells mens' and womens' shoes, sandals, boots, and sneakers.
<http://www.shoebuy.com/> - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

[Footwear Shopping in the Yahoo! Directory](#)
[Privacy Report](#) Browse through footwear shops and official company sites in the Yahoo! Directory. Find retailers selling shoes, boots, and accessories from Nike, adidas, Puma, Timberland, Converse, Reebok, Skechers, and others.
http://dir.yahoo.com/Business_and_Economy/Shopping... - [Cached](#) - [Privacy Policy](#) - [Similar Pages](#)

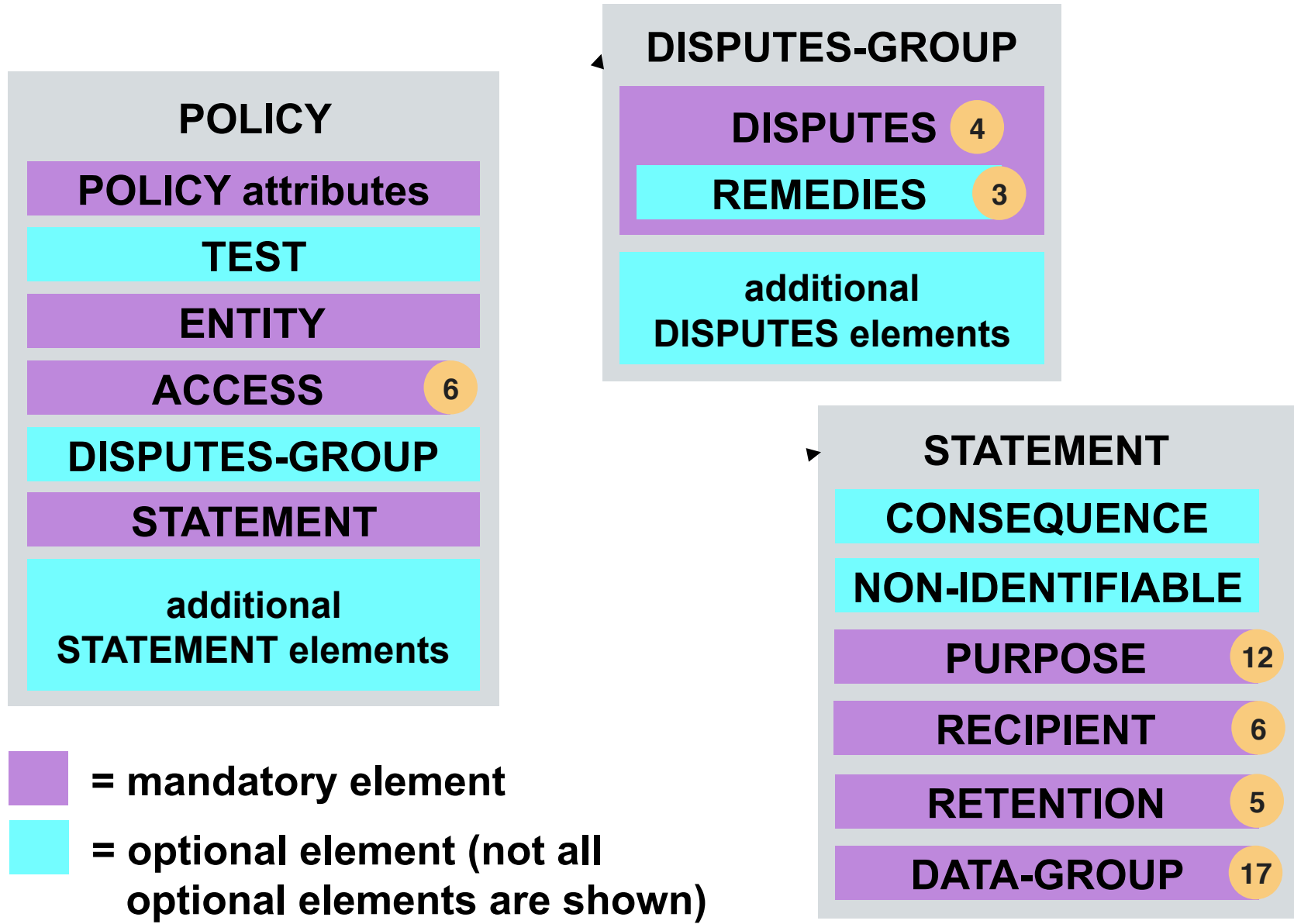
[Shoes.com - Womens. Mens. and Childrens Shoes](#)

A privacy taxonomy

What's in a P3P policy?

- Name and contact information for site
- The kinds of data collected
- How collected data is used, and whether individuals can opt-in or opt-out of any of these uses (secondary uses only!)
- Whether/when data may be shared, whether there is opt-in or opt-out
- Data retention policy
- The kind of access provided
- Mechanisms for resolving privacy disputes

Structure of a P3P policy

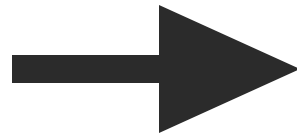
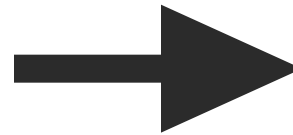


Difficulties in P3P vocabulary development

- Different stakeholder objectives
 - Privacy advocates vs. industry
 - Different privacy laws in different countries
- Disagreements about definitions
 - What is PII?
 - Is IP address PII?
- What is in scope?
 - Statements about security? Negotiation? Data transfer?
- Finding the right degree of granularity

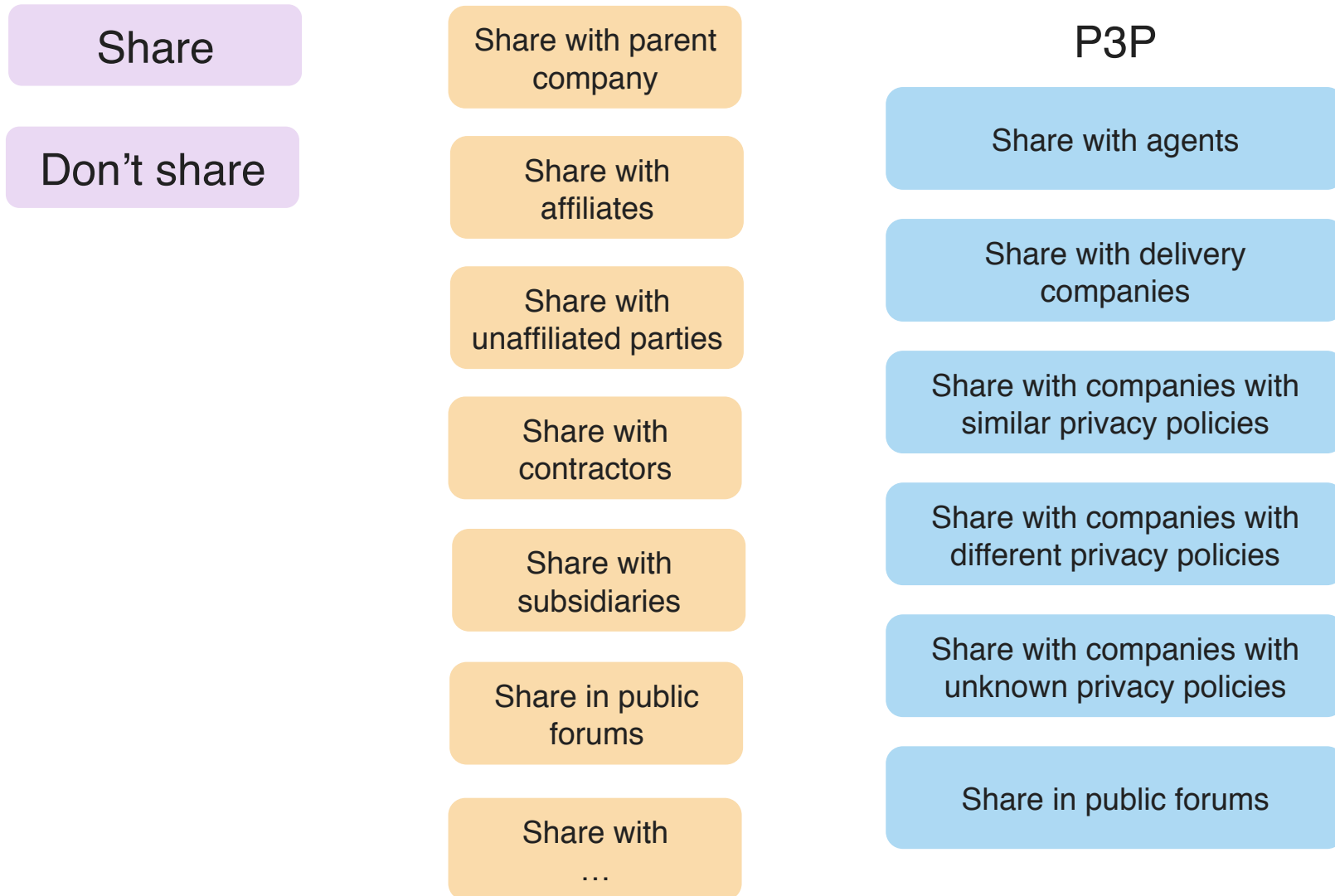
Can't derive more detail from less detail

Characters not well developed
Gratuitous sex and violence



Bad acting?
Boring plot?
Bad script?
Dull characters?
Unbelievable premise?
Unoriginal?
Too much violence?
Not enough violence?

Recipients granularity



eTRUST 1996



Share with agents

Share with delivery companies

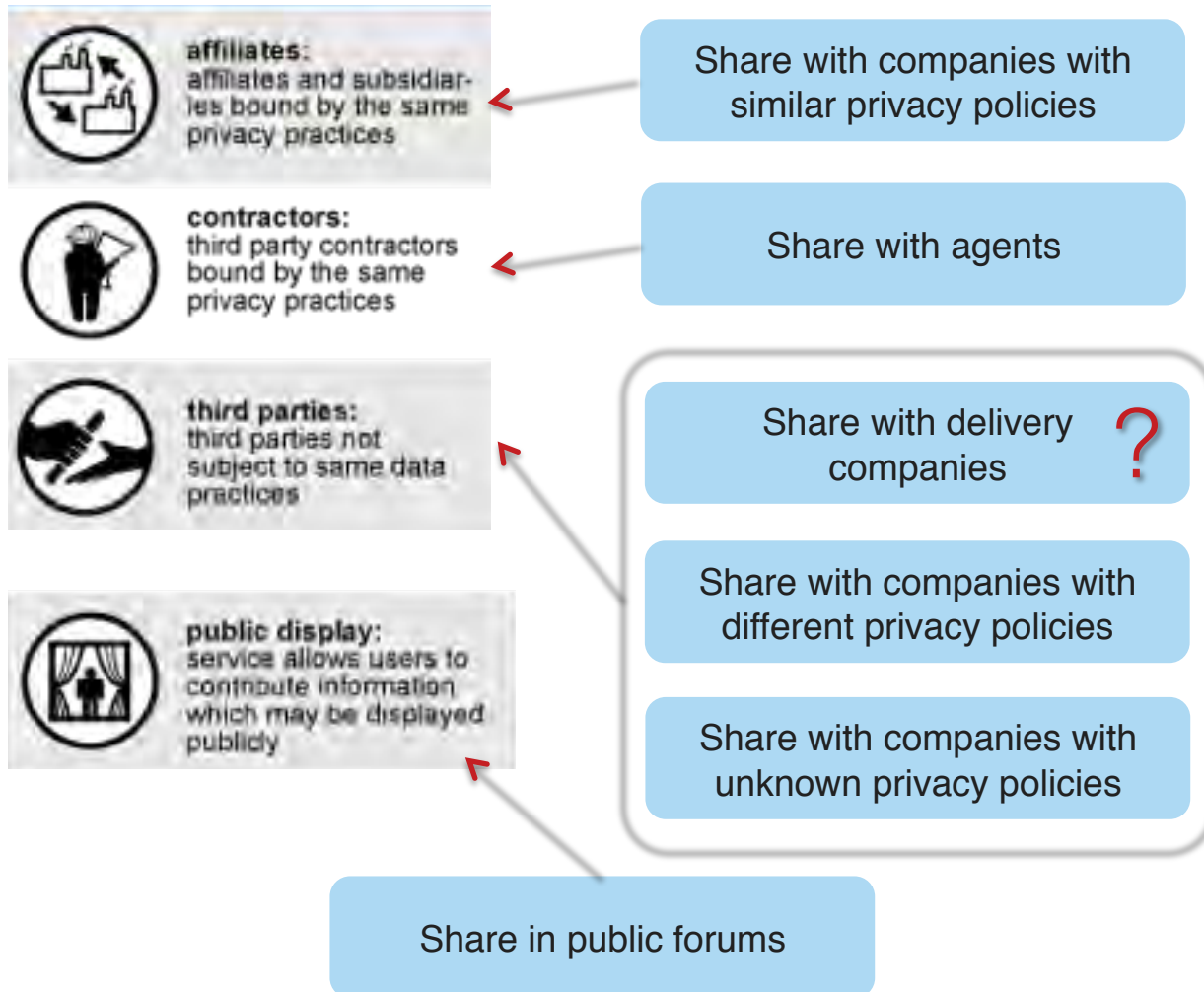
Share with companies with similar privacy policies

Share with companies with different privacy policies

Share with companies with unknown privacy policies

Share in public forums

KnowPrivacy 2009



CMU privacy nutrition label 2009

information sharing

other
companies

public
forums

Share in public forums

Share with companies with
similar privacy policies

Share with companies with
different privacy policies

Share with companies with
unknown privacy policies

Assumed, no
explicit disclosure:

Share with agents

Share with delivery
companies

Mozilla privacy icons 2010



Your data is never bartered or sold.



Your data is never given to advertisers.



Data is given to law enforcement only when legal process is followed.



Your data may be bartered or sold.



Site gives your data to advertisers.



Data may be given to law enforcement even when legal process is not followed.



Share with delivery companies

Share with agents

Share in public forums

Share with companies with similar privacy policies

Share with companies with different privacy policies

Share with companies with unknown privacy policies

Pros and cons of detailed vocabulary

Advantages

- Allows maximum expressiveness, allows policy authors to explain nuanced policies
- User agent implementers can select most relevant info to show users
- Users can configure agents to display info they care about

Disadvantages

- Difficult for policy authors to use policy elements correctly
- More difficult for user agent implementers
- When user agents are all different, policy authors are uncertain about how their policy will be displayed

Evaluating the P3P vocabulary

- Consistent with FTC staff's 2010 recommendation not to focus notice and choice on practices such as product fulfillment
 - CURRENT purpose captures primary uses
 - OURS recipient includes agents working on behalf of the company
- Has stood the test of time reasonably well
 - Included location data category
 - Does not allow detailed expression of peer-to-peer data sharing (social networks)
- P3P syntax and some definitions are confusing

Privacy nutrition labels

Can we build a better policy?

- Easy to understand
- Fast to find information
- Easy to compare

ER JOE'S®
SHREDDED
TE SIZE
HEATS

Nutrition Facts
 Serving Size 1 cup (85g)
 Per Container about 10


Amount Per Serving
 130 Calories from Fat 10

% Daily Value*

Total Fat	2%
Saturated Fat	0%
Trans Fat	0%
Cholesterol	0%
Sodium	0%
Total Carbohydrate	3%
Dietary Fiber	30%
Sugars	0%
Protein	0%

INGREDIENTS: Whole Wheat, ... (No preservative treatments)

& Sold Exclusively By
 Trader Joe's,
 Missouri, CA 91018



BARBARA'S BAKERY

Shredded Spoonfuls®
 Multigrain

Nutrition Facts
 Serving Size 3/4 Cup (50g)
 Servings Per Container About 21


Amount Per Serving
 130 Calories
 Calories from Fat 15

% Daily Value*

Total Fat	1 1/2%
Saturated Fat	0%
Trans Fat	0%
Cholesterol	0%
Sodium	2%
Potassium	0%
Total Carbohydrate	24%
Dietary Fiber	15%
Soluble Fiber	1%
Insoluble Fiber	3%
Sugars	1%
Protein	1%

INGREDIENTS: Whole Soft Flour, Yellow Corn Meal, ... (No preservative treatments)

& Sold Exclusively By
 Trader Joe's,
 Missouri, CA 91018



TRADER JOE'S®

Very Berry Clusters CEREAL

Nutrition Facts
 Serving Size 1 cup (55g)
 Servings Per Container about 7

Amount Per Serving
 Calories 100
 Calories from Fat 15

% Daily Value*

Total Fat	1g
Saturated Fat	0.5g
Trans Fat	0g
Cholesterol	0mg
Sodium	140mg
Total Carbohydrate	43g
Dietary Fiber	3g
Sugars	13g
Protein	5g

INGREDIENTS: WHOLE SOFTED OATS, MILDLY SWEETENED SUGAR COMPLEX, ... (No preservative treatments)

CONTAINS WHEAT. MAY CONTAIN TRACES OF TREE NUTS & SOY.

DIST. & SOLD EXCLUSIVELY BY
 TRADER JOE'S, MISSOURI, CA 91018

This product is sold by weight and volume. Some variations in volume may occur due to packing and handling.

Nutrition Facts
 Serving Size 1/4 cup (20g)
 Servings Per Container about 12

Amount Per Serving
 110 Calories
 Calories from Fat 5

% Daily Value*

Total Fat	1.5g
Saturated Fat	0%
Trans Fat	0%
Cholesterol	0mg
Sodium	120mg
Potassium	10mg
Total Carbohydrate	20g
Dietary Fiber	0%
Sugars	0%
Other Carbohydrate	0g
Protein	1g

INGREDIENTS: WHOLE SOFTED OATS, MILDLY SWEETENED SUGAR COMPLEX, ... (No preservative treatments)

CONTAINS WHEAT. MAY CONTAIN TRACES OF TREE NUTS & SOY.

DIST. & SOLD EXCLUSIVELY BY
 TRADER JOE'S, MISSOURI, CA 91018

This product is sold by weight and volume. Some variations in volume may occur due to packing and handling.

Shredded Oats®
 Original

Nutrition Facts
 Serving Size 1/4 Cup (25g)
 Servings Per Container About 12

Amount Per Serving
 100 Calories
 Calories from Fat 25

% Daily Value*


Total Fat	2.5g
Saturated Fat	0.5g
Trans Fat	0%
Cholesterol	0mg
Sodium	150mg
Potassium	100mg
Total Carbohydrate	43g
Dietary Fiber	3g
Soluble Fiber	2g
Insoluble Fiber	3g
Sugars	1g
Protein	1g

INGREDIENTS: Whole Soft Flour, Whole Wheat Flour, ... (No preservative treatments)

CONTAINS WHEAT AND SOY. Made on equipment that also processes milk, almonds and hazelnuts.

DIST. & Sold Exclusively By
 Trader Joe's, Missouri, CA 91018

Sold Exclusively By
 Trader Joe's,
 Missouri, CA 91018



TRADER JOE'S®

Organic HIGH FIBER O'S

Nutrition Facts
 Serving Size 1/4 cup (55g)
 Servings per Container 8

Amount per Serving
 Calories 100
 Calories from Fat 10

% Daily Value*


Total Fat	1g
Saturated Fat	0g
Trans Fat	0%
Cholesterol	0mg
Sodium	115mg
Total Carbohydrate	44g
Dietary Fiber	9g
Soluble Fiber	less than 1g
Insoluble Fiber	8g
Sugars	9g
Protein	6g

INGREDIENTS: Organic Whole Grain Wheat Flour, Organic Whole Grain Organic (Preserved) Oats, ... (No preservative treatments)

CONTAINS WHEAT AND SOY. Made on equipment that also processes milk, almonds and hazelnuts.

DIST. & Sold Exclusively By
 Trader Joe's, Missouri, CA 91018

Sold Exclusively By
 Trader Joe's,
 Missouri, CA 91018



Nutrition Facts
 Serving Size 1/4 cup (55g)
 Servings per Container 8

Amount per Serving
 Calories 100
 Calories from Fat 10

% Daily Value*


Total Fat	1g
Saturated Fat	0g
Trans Fat	0%
Cholesterol	0mg
Sodium	115mg
Total Carbohydrate	44g
Dietary Fiber	9g
Soluble Fiber	less than 1g
Insoluble Fiber	8g
Sugars	9g
Protein	6g

INGREDIENTS: Organic Whole Grain Wheat Flour, Organic Whole Grain Organic (Preserved) Oats, ... (No preservative treatments)

CONTAINS WHEAT AND SOY. Made on equipment that also processes milk, almonds and hazelnuts.

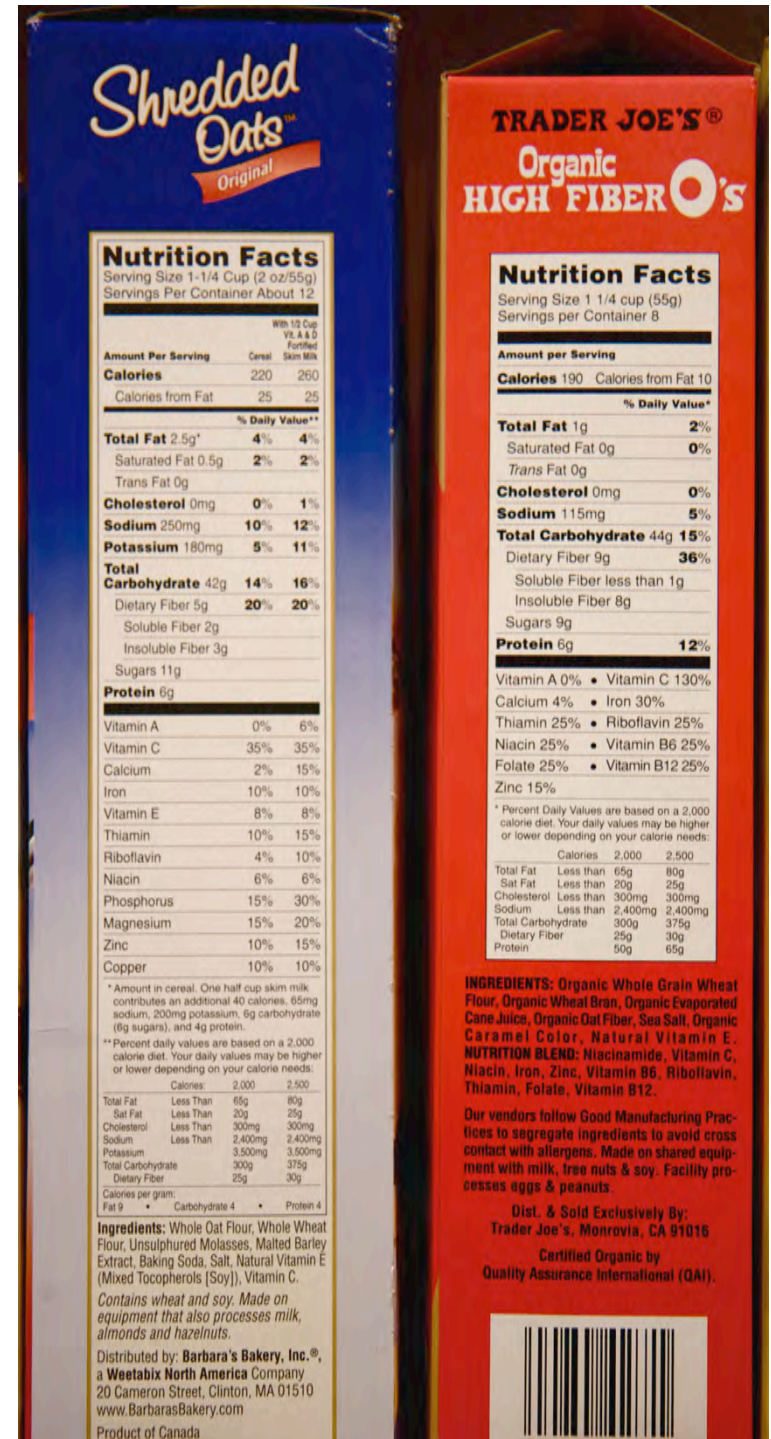
DIST. & Sold Exclusively By
 Trader Joe's, Missouri, CA 91018

Sold Exclusively By
 Trader Joe's,
 Missouri, CA 91018



Towards a privacy “nutrition label”

- Standardized format
 - People learn where to find answers
 - Facilitates policy comparisons
- Standardized language
 - People learn terminology
- Brief
 - People find info quickly
- Linked to extended view
 - Get more details if needed



Nutrition Facts

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

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

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

	Calorie	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300 mg	300mg
Sodium	Less than	2,400 mg	2,400 mg
Total Carbohydrate		300g	370g
Dietary Fiber		25g	30g

LOW

Fat
7.7g per serving

LOW

Saturates
2.0g per serving

HIGH

Sugars
42.2g per serving

MED

Salt
2.0g per serving

WARNING:
CHOKING HAZARD
This toy is a small ball.
Not for children under 3 yrs.

ENERGYGUIDE

Compare the Energy Use of this Refrigerator with Others before You Buy.

This Model Uses **775 kWh/year**

Energy Use (kWh/year) range of all similar models

Uses Least Energy
742

Uses Most Energy
818

kWh/year (kilowatt hours per year) is a measure of energy use. The utility company will bill you based on this. This model uses 775 kWh a year. The label also shows the range of all similar models.

Refrigerators using more energy cost more to operate. This model's estimated yearly operating cost is:

\$68

Based on a 1992 U.S. Department of Energy survey of 100 U.S. cities. Your actual operating cost will vary depending on your utility rates and your use of the product.

Drug Facts

Active Ingredient (in each tablet)	Purpose
Chlorpheniramine maleate 4 mg	Antihistamine

Uses temporarily relieves these symptoms that may occur in children with respiratory allergies: ■ sneezing ■ runny nose ■ itchy, watery eyes ■ itchy throat

Warnings
Ask a doctor before use if you have
 ■ glaucoma ■ a breathing problem, such as emphysema or chronic bronchitis
 ■ trouble urinating due to an enlarged prostate gland
Ask a doctor or pharmacist before use if you are taking tranquilizers or sedatives.

When using this product
 ■ you may get drowsy ■ avoid alcoholic drinks
 ■ alcohol, sedatives, and tranquilizers may increase drowsiness
 ■ be careful when driving a motor vehicle or operating machinery
 ■ excitability may occur, especially in children.

If pregnant or breast-feeding, ask a health professional before use. Keep out of reach of children. In case of overdose, get medical help or contact a Poison Control Center right away.

WATER RATING

4

For more information and to compare appliances, visit us at www.waterrating.gov.au

Energy

Washing machine

Manufacturer Model	Energy consumption kWh/cycle
More efficient	
A	
B	
C	
D	
E	
F	
G	
Less efficient	
Energy consumption kWh/cycle	1.75
Based on standard test results for 60°C cotton cycle	

Challenges

- People are not familiar with privacy terminology
- Context matters
 - Need to know *which data are used for what purposes*
- Privacy policies are complex
- People don't understand privacy implications

Iterative design process

- Focus groups
- Lab studies
- Online studies
- Measuring
 - Reading-comprehension - accuracy
 - Time to find information
 - Ease of policy comparison
 - Subjective opinions, ease, fun, trust
- <http://cups.cs.cmu.edu/privacyLabel>



Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder. A "Nutrition Label" for Privacy. SOUPS 2009.

ACME Privacy Policy

[Contact Site](#)

Information **not** used

Information may be used

May be used, **only if you request this**

May be used, **unless you opt-out**

Expand the column for more information

Some information may be used - **expand for details**

opt-in opt-out

WHO may use your information

Companies who help us

Other companies

People who read your public postings

click for more...

click for more...

HOW your information may be used

Hide Unused Information ✓

Provide service and maintain site

Research & Development

Profiling

Analysis

- not linked to you
- linked to you

Decisions affecting you

- not linked to you
- linked to you

Marketing

- Postal, email, etc.
- Telemarketing

Other

click for more...

1. Access log and cookies

Our Web server collects access logs and cookies. A cookie is a small data file that we transfer to your computer's hard drive through your web browser when you visit our sites. Cookies enable our systems to recognize your computer, so that we can provide you with personalized information and features. We also use cookies to track user traffic patterns. **Retention Time: Indefinitely**

Types of Information Collected

2. Ordering Books and Conferences

We collect information in order to process your purchase. If you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme conferences. We send conference brochures to past conference attendees. **Retention Time: Indefinitely**

Types of Information Collected

Name, address, phone number, etc.

User Information

Name

Home Contact Information

Business Contact Information

Email address, online contact info

Web Browsing Information

R.W. Reeder, P.G. Kelley, A.M. McDonald, and L.F. Cranor. A User Study of the Expandable Grid Applied to P3P Policy Visualization. Workshop on Privacy in the Electronic Society WPES 2008. <http://lorrie.cranor.org/pubs/wpes24reeder.pdf>

Design evolution

ACME Privacy Policy

Information we use
 Information we use
 May be used, only if you request this
 May be used, unless you opt out
 Exclude the option to more information
 Exclude the option to more information
 Exclude the option to more information
 Exclude the option to more information

WHO may use your information

Companies who help us
 Other companies
 People who read your posts
 Other companies

HOW your information may be used

Provide services and maintain site
 Profiling
 Marketing
 Other

Push Us Your Information

Push Us Your Information
 Push Us Your Information
 Push Us Your Information
 Push Us Your Information

1. Access log and cookies

Our Web server collects access log and cookies. A cookie is a small data file that we transfer to your computer's hard drive through your web browser when you visit our site. Cookies enhance our ability to recognize your computer, so that we can provide you with personalized responses and features. [Read our cookie policy.](#)

2. Ordering Books and Conferences

We collect information in order to process your purchase. If you register for an Acme conference, or sign up for a conference email list, we will send you email announcements and updates about Acme gatherings. We send conference notices to past conference attendees. [Read our Terms & Conditions.](#)

Types of Information Collected

Name, address, phone number, etc.
 User information
 Name
 Home Contact Information
 Business Contact Information
 Email address, online contact info
 Web Browsing Information
 Cookies (optional)
 User Information
 Third Party Information

Nutrition Facts

Serving Size 1 cup (240g)
 Calories 250

Total Fat	5g	10%
Saturated Fat	3g	6%
Total Crap	1g	2%
Cholesterol	20mg	40%
Sodium	450mg	90%
Total Crap	1g	2%
Sodium	450mg	90%
Sugar	5g	10%
Protein	5g	10%
Vitamin C	25%	50%
Calcium	25%	50%
Iron	25%	50%

Percent Daily Values are based on a diet of 2,000 calories a day. Daily Values may vary slightly from those listed on the product label.

Privacy Facts

What does ACME Corporation do with Your Personal Information?

WHAT Information do they collect?
 Information about your computer and the way you use our website.
 Information about your preferences and how you interact with our website.
 Information about your contact information and how you interact with our website.
 Information about your purchase history and how you interact with our website.
 Information about your browsing history and how you interact with our website.

HOW do they use your information?
 To provide you with personalized content and offers.
 To analyze your usage patterns and improve our website.
 To contact you about our products and services.
 To provide you with targeted advertising.
 To provide you with personalized recommendations.

WHY do they need this information?
 To provide you with personalized content and offers.
 To analyze your usage patterns and improve our website.
 To contact you about our products and services.
 To provide you with targeted advertising.
 To provide you with personalized recommendations.

CONTACT US Call 1-800-555-5555 or visit us online at [www.acme.com](#)

eBay Privacy Policy

What we collect

Personal information
 Contact information
 Demographic information
 Financial information
 Health information
 Preferences
 Purchasing information
 Social security number & gov ID
 Your activity on this site
 Your location

How we use your information

Provide services and maintain site
 Research and product development
 Marketing
 Telemarketing
 Profiling and targeted advertising
 Profiling and targeted advertising
 Other companies
 Public forums

Who shares your information with

Provide services and maintain site
 Research and product development
 Marketing
 Telemarketing
 Profiling and targeted advertising
 Profiling and targeted advertising
 Other companies
 Public forums

Understanding this privacy report

! Data is collected and used in this way. | Your data will not be used in this way unless you opt-in. | You can opt out of this data use.

The Acme Policy

how we use your information

provide services & maintain site
 research & development
 marketing
 telemarketing
 profiling
 other companies
 public forums

types of information

contact information
 cookies
 demographic information
 financial information
 health information
 preferences
 purchasing information
 social security number & gov ID
 your activity on this site
 your location

who we share your information with

provide services & maintain site
 research & development
 marketing
 telemarketing
 profiling
 other companies
 public forums

Understanding this privacy policy

! we will use your information in this way. | we will not collect or use your information in this way. | we will not 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 1-800-555-5555 [www.acme.com](#)

Acme

information we collect

ways we use your information

provide service and maintain site
 marketing
 telemarketing
 profiling
 other companies
 public forums

information sharing

provide service and maintain site
 marketing
 telemarketing
 profiling
 other companies
 public forums

Access to your information

This site gives you access to your contact data and some of its other data identified with you.

How to resolve privacy-related disputes with this site

Please email our customer service department

Acme.com
 5000 Forbes Avenue
 Pittsburgh, PA 15213 United States
 Phone: 800-555-5555
 help@acme.com

we will collect and use your information in this way

opt out

by default, we will collect and use your information in this way unless you tell us not to by opting out

we will not collect and use your information in this way

by default, we will not collect and use your information in this way unless you allow us to by opting in

Removes wiggle room and complicated terminology by using four standard symbols

Acme

information we collect

ways we use your information

information sharing

	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out		opt out	opt in
cookies		opt out	opt out			
demographic information		opt out	opt out			
financial information						
health information		opt out	opt out			

Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out		opt out	opt in
cookies		opt out	opt out			
demographic information		opt out	opt out			
financial information						
health information		opt out	opt out			
preferences		opt out	opt out			opt in
purchasing information		opt out	opt out			opt in
social security number & govt ID						
your activity on this site		opt out	opt out			
your location						

Bell Group

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt in			opt out	
cookies						
demographic information		opt in			opt out	
financial information						
health information						
preferences		opt in			opt out	
purchasing information		opt in			opt out	
social security number & govt ID						
your activity on this site		opt in			opt out	
your location						

Allows for quick high-level visual feedback by looking at the overall intensity of the page

Acme

information we collect

	ways we use your information	
	provide service and maintain site	marketing
contact information		opt out
cookies		opt out
demographic information		opt out
financial information		
health information		opt out
preferences		opt out
purchasing information		opt out
social security number & gov't ID		
your activity on this site		opt out
your location		

Bell Group

information we collect

	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt in			opt out	
cookies						
demographic information		opt in			opt out	
financial information						
health information						
preferences						
purchasing information						
social security number & gov't ID						
your activity on this site						
your location						

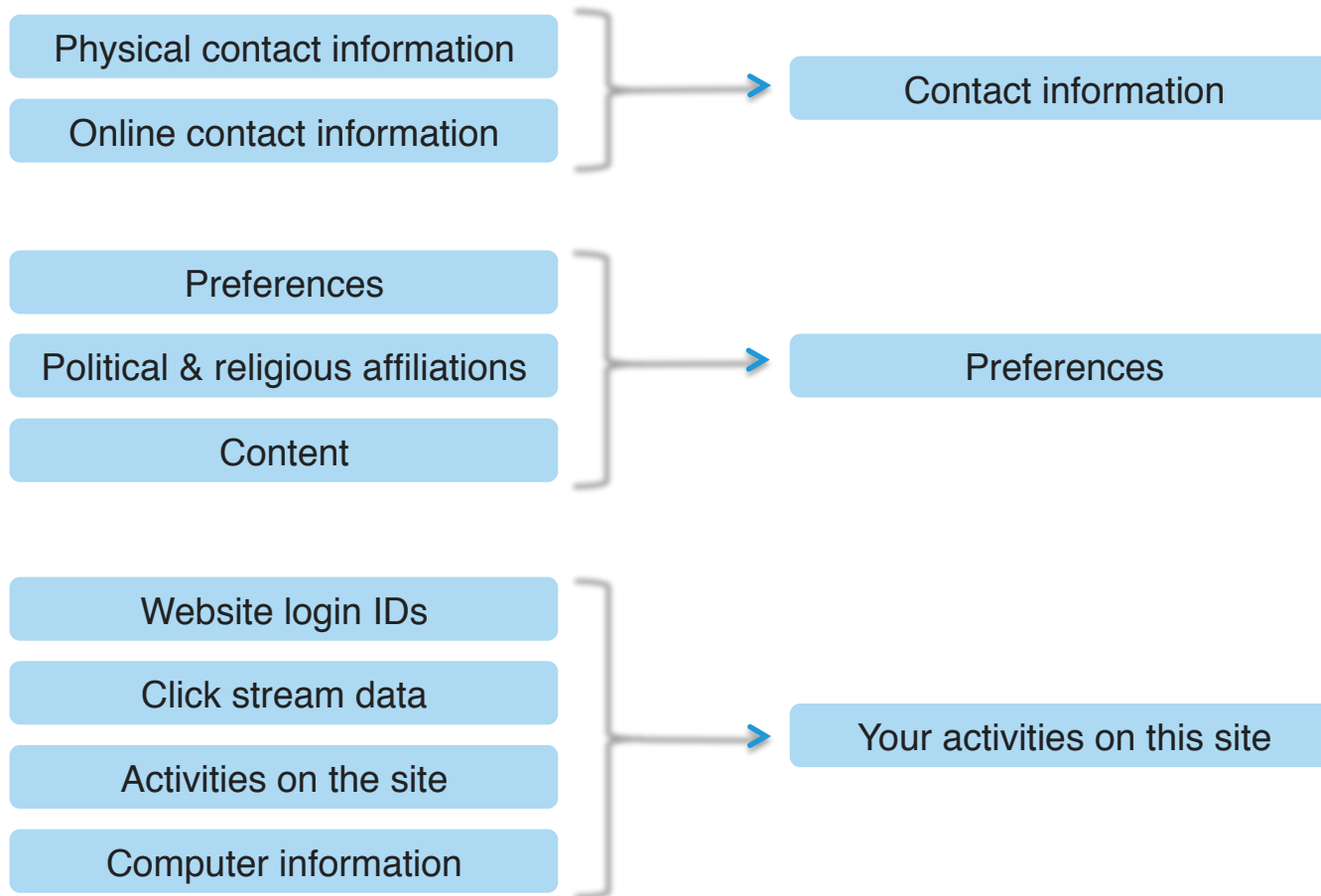
Allows for information to be found in the same place every time

Creating simple nutrition label from complex P3P

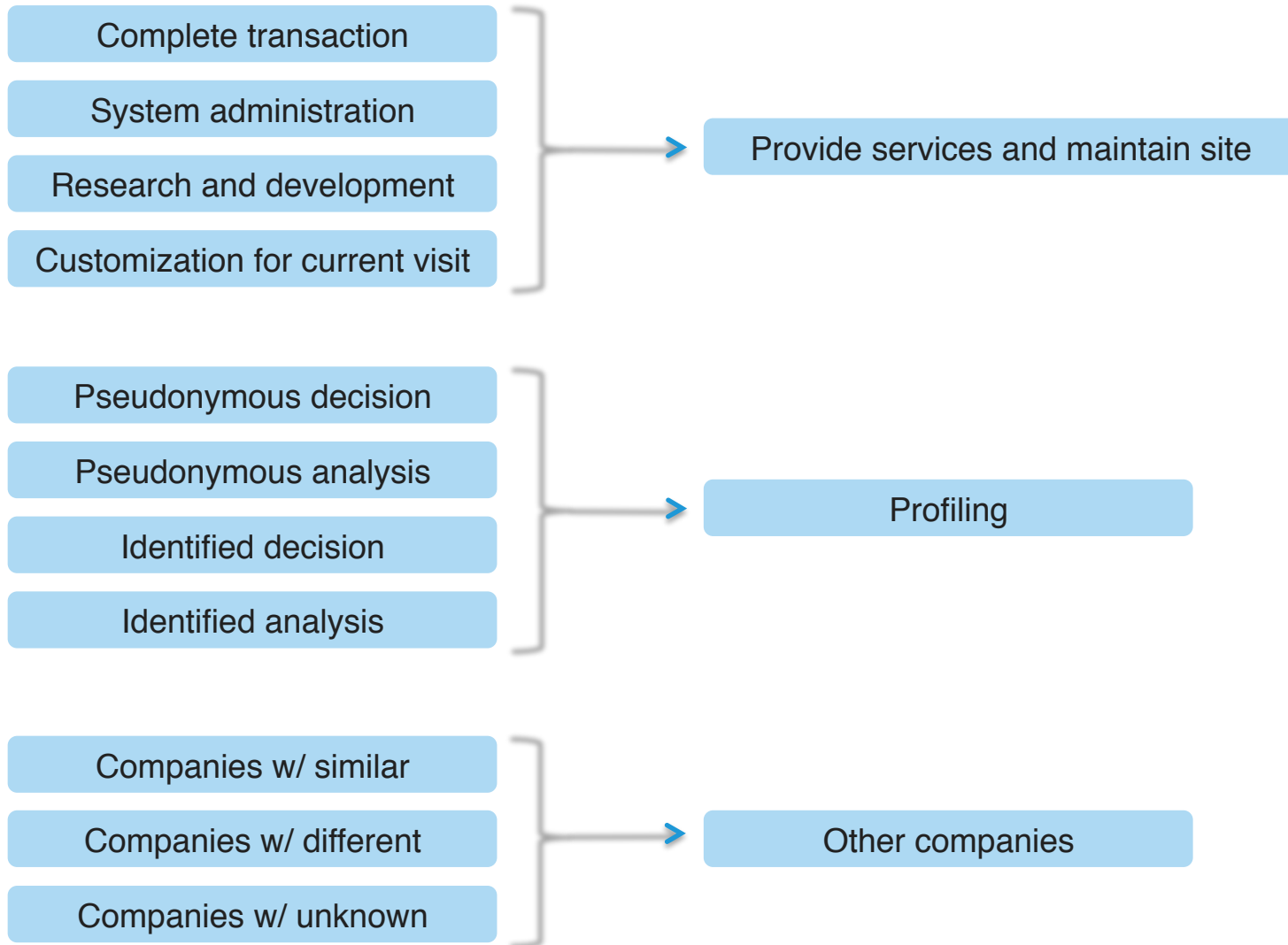
- Merge all statements
- Reduce the number of data categories (rows)
- Reduce the number of purposes and recipients (columns)



Reducing the rows



Reducing the columns



Online study

- 763 participants
- Conducted through Amazon's Mechanical Turk
- Between subjects design
 - Standardized label
 - Standardized short label
 - Standardized short text
 - Full text
 - Layered text
- Measured time, accuracy, and enjoyability on information finding and comparison tasks

P.G. Kelley, L.J. Cesca, J. Bresee, and L.F. Cranor. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. CHI2010.

Standardized label

Short label

Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Acme

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
preferences		opt out	opt out			
purchasing information		opt out	opt out			
your activity on this site		opt out	opt out			

Information not collected or used by this site: social security number & government ID, financial, health, location.

Access to your information
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Short Standardized Text

Acme

Acme will collect your contact information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will share this information with other companies unless you opt out. They will share this information on public forums if you opt in.

Acme will collect your activity on this site, demographic information, your health information, and cookie information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will not share this information.

Acme will collect your preferences and your purchase information. They will use this information for providing you service and maintaining the site and profiling. They will also use this information for marketing and telemarketing unless you opt out. They will share this information on public forums if you opt in.

Information not collected or used by this site:
financial, SSN or government ID, and location.

Access to your information

This site gives you access to your contact data and some of its other data identified with you

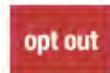
How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213 United States
Phone: 800-555-5555
help@acme.com

Legend & Definitions



we **will** collect and use your information in this way



by default, we **will** collect and use your information in this way unless you tell us not to by opting out



we **will not** collect and use your information in this way



by default, we **will not** collect and use your information in this way unless you allow us to by opting in

Definitions

contact information

Contact information may include name, address, phone number, email address, or other online or physical contact information.

cookies

Cookies or mechanisms that perform similar functions. A cookie is a small text file that a website can place on your computer's hard drive to collect information about your activities on the site or to allow the site to remember information about you and your activities.

demographic information

Demographic information may include social and economic categories that apply to you, such as your gender, age, income, or where you are from.

financial information

Financial information may include your accounts, balances, and transactions.

provide service and maintain site

Collecting information to provide the service you requested, to customize the site for your current visit, to perform web site and system maintenance, or to enhance, evaluate, or otherwise review the site, but without connecting any information to you.

public forums

A public area, such as a bulletin board, chat room, or directory.

purchasing information

Information about your purchases may include the payment methods you used.

social security number & govt ID

Includes government-issued identifiers such as your social security number.

telemarketing

Contacting you by telephone to market services or products

Full Policy Text

Amazon.com Privacy Notice

Last updated: October 1, 2008. To see what has changed, [click here](#).

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

- [What Personal Information About Customers Does Amazon.com Gather?](#)
- [What About Cookies?](#)
- [Does Amazon.com Share the Information It Receives?](#)
- [How Secure Is Information About Me?](#)
- [What About Third-Party Advertisers and Links to Other Websites?](#)
- [Which Information Can I Access?](#)
- [What Choices Do I Have?](#)
- [Are Children Allowed to Use Amazon.com?](#)
- [Does Amazon.com Participate in the Safe Harbor Program?](#)
- [Conditions of Use, Notices, and Revisions](#)
- [Examples of Information Collected](#)

What Personal Information About Customers Does Amazon.com Gather?

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

- **Information You Give Us:** We receive and store any information you enter on our Web site or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com or advertisements and other content served by or on behalf of Amazon.com on other Web sites. [Click here](#) to see examples of the information we receive.
- **E-mail Communications:** To help us make e-mails more useful and interesting, we

a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used to transfer add-ons, such as Flash cookies, by changing the add-on settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to sign in.

Does Amazon.com Share the Information It Receives?
Information about our customers is an important part of our business, and we are not in the business of selling it to others. We share customer information only as described below and with subsidiaries Amazon.com, Inc. controls that either are subject to this Privacy Notice or follow practices at least as protective as those described in this Privacy Notice.

Affiliated Businesses We Do Not Control: We work closely with affiliated businesses. In some cases, such as Marketplace sellers, these businesses operate stores at Amazon.com or sell offerings to you at Amazon.com. In other cases, we operate stores, provide services, or sell products jointly with these businesses. [Click here](#) for some examples of co-branded and joint offerings. You can tell whether a third party is involved in your transactions, and we share customer information related to those transactions with that third party.

Third-Party Service Providers: We employ other companies and individuals to perform functions on our behalf. Examples include fulfilling orders, delivering packages, sending postal mail and e-mail, removing repetitive information from customer lists, analyzing data, providing marketing assistance, providing search results and links (including paid listings and links), processing credit card payments, and providing customer service. They have access to personal information needed to perform their functions, but may not use it for other purposes.

Promotional Offers: Sometimes we send offers to selected groups of Amazon.com customers on behalf of other businesses. When we do this, we do not give that business your name and address. If you do not want to receive such offers, please adjust your [Customer Communication Preferences](#).

Business Transfers: As we continue to develop our business, we might sell or buy stores, subsidiaries, or business units. In such transactions, customer information generally is one of the transferred business assets but remains subject to the promises made in any pre-existing Privacy Notice. (Of course, the customer consents otherwise.) Also, in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Protection of Amazon.com and Others: We release account and other personal information when we believe release is appropriate to comply with the law, enforce or apply our [Conditions of Use](#) and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

With Your Consent: Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?
We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.
We reveal only the last five digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

What About Third-Party Advertisers and Links to Other Websites?
Our site includes third-party advertising and links to other Web sites. We do not provide any personally identifiable customer information to these advertisers or third-party Web sites. [Click here](#) for more information about our Advertising Policies and Specifications.

These third-party Web sites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our Web site directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize

substantially all of its assets are acquired, customer information will of course be one of the transferred assets.

Protection of Amazon.com and Others: We release account and other personal information when we believe release is appropriate to comply with the law, enforce or apply our [Conditions of Use](#) and other agreements; or protect the rights, property, or safety of Amazon.com, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. Obviously, however, this does not include selling, renting, sharing, or otherwise disclosing personally identifiable information from customers for commercial purposes in violation of the commitments set forth in this Privacy Notice.

With Your Consent: Other than as set out above, you will receive notice when information about you might go to third parties, and you will have an opportunity to choose not to share the information.

How Secure Is Information About Me?
We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input.
We reveal only the last five digits of your credit card numbers when confirming an order. Of course, we transmit the entire credit card number to the appropriate credit card company during order processing.
It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer. [Click here](#) for more information on how to sign off.

What About Third-Party Advertisers and Links to Other Websites?
Our site includes third-party advertising and links to other Web sites. We do not provide any personally identifiable customer information to these advertisers or third-party Web sites. [Click here](#) for more information about our Advertising Policies and Specifications.

These third-party Web sites and advertisers, or Internet advertising companies working on their behalf, sometimes use technology to send (or "serve") the advertisements that appear on our Web site directly to your browser. They automatically receive your IP address when this happens. They may also use cookies, JavaScript, web beacons (also known as action tags or single-pixel gifs), and other technologies to measure the effectiveness of their ads and to personalize advertising content. We do not have access to or control over cookies or other services that they may use, and the information practices of these advertisers and third-party Web sites are not covered by this Privacy Notice. Please contact them directly for more information about their privacy practices. In addition, the [Federal Trade Commission](#) offers useful information about Internet advertising companies (also called "ad networks" or "network advertisers"), including information about how to opt-out of their information collection.

Amazon.com also displays personalized third-party advertising based on personal information about customers, such as purchases on Amazon.com, visits to Amazon Associate Web sites, or use of payment services like Checkout by Amazon on other Web sites. [Click here](#) for more information about the personal information that we gather.

Although Amazon.com does not provide any personal information to advertisers, advertisers (including ad-serving companies) may assume that users who interact with or click on a personalized advertisement meet their criteria to personalize the ad (for example, users in the northwestern United States who bought or browsed for personal music). If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your [Advertising Preferences](#).

Which Information Can I Access?
Amazon.com gives you access to a broad range of information about your account and your interactions with Amazon.com for the limited purpose of viewing and, in certain cases, updating that information. [Click here](#) to see some examples, the list of which will change as our Web site evolves.

What Choices Do I Have?
As discussed above, you can always choose not to provide information even though it might be needed to make a purchase or to take advantage of such Amazon.com features as [Your Profile](#), [Web Lists](#), [Reviews](#), and [Amazon Prime](#).
You can add or update certain information on pages such as those referred to in the ["Which Information Can I Access?"](#) section. When you update information, we usually keep a copy of the prior version for our records.
If you do not want to receive e-mail or other mail from us, please adjust your [Customer Communication Preferences](#). If you do not want to receive [Conditions of Use](#) and other legal notices from us, such as this Privacy Notice, those notices will still govern your use of Amazon.com, and it is your responsibility

employ to you, please adjust your [Advertising Preferences](#).
The large portion of the toolbar on most browsers will tell you how to prevent your browser from accepting new cookies, how to have the browser notify you when you receive a new cookie, or how to disable cookies altogether. Additionally, you can disable or delete similar data used by browser add-ons, such as Flash cookies, by changing the add-on settings or visiting the Web site of its manufacturer. However, because cookies allow you to take advantage of some of Amazon.com's essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to sign in.

Are Children Allowed to Use Amazon.com?
Amazon.com does not sell products for purchase by children. We sell children's products for purchase by adults. If you are under 18, you may use Amazon.com only with the involvement of a parent or guardian.

Does Amazon.com Participate in the Safe Harbor Program?
Amazon.com is a participant in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. We have certified that we adhere to the Safe Harbor Privacy Principles agreed upon by the U.S. and the E.U. For more information about the Safe Harbor and to view our certification, visit the [U.S. Department of Commerce's Safe Harbor](#) Web site. If you would like to contact Amazon.com directly about the Safe Harbor program, please send an e-mail to safeharbor@amazon.com.

Conditions of Use, Notices, and Revisions
If you choose to visit Amazon.com, your visit and any dispute over privacy is subject to this Notice and our [Conditions of Use](#), including limitations on damages, resolution of disputes, and application of the law of the state of Washington. If you have any concern about privacy at Amazon.com, please [contact us](#) with a thorough description, and we will try to resolve it. Our business changes constantly, and our Privacy Notice and the [Conditions of Use](#) will change also. We may e-mail periodic reminders of our notices and updates, and you are instructed as to, but you should check our Web site frequently to see recent changes. Unless stated otherwise, our current Privacy Notice applies to all information that we have about you and your account. We stand behind the promises we make, however, and will never materially change our policies and practices to make them less protective of customer information collected in the past without the consent of affected customers.

Related Practices and Information
• [Conditions of Use](#)
• [Disability Support](#)
• [Community Sites](#)
• [Web Discontent](#)
• [Top Product Categories](#)
• [Your Profile and Community Guidelines](#)

Examples of Information Collected
Information You Give Us
You provide most such information when you search, buy, list, post, participate in a contest or questionnaire, or communicate with customer service. For example, you provide information when you search for a product; place an order through Amazon.com or one of our third-party sellers; provide information in [Your Account](#) (and you might have more than one if you have used more than one e-mail address when shopping with us); or [Track Profile](#); communicate with us by phone, e-mail, or otherwise; complete a questionnaire or a contest entry form; complete [Web Lists](#) or other gift registries; provide information when opening a corporate account; participate in [Question Boards](#) or other community features; provide [Rate Feedback](#); specify a [Social Occasion Reminder](#); share information with [Amazon Friends](#); and employ other Personal Notification Services, such as Available to Order Notifications.



As a result of these actions, you might supply us with such information as your name, address, and phone numbers; credit card information; people to whom purchases have been shipped, including addresses and phone number; people (with addresses and phone number) listed in [L1C1L1](#) settings; e-mail addresses of [Amazon Friends](#) and other people; content of reviews and e-mails to us; personal description and photograph in [Your Profile](#); and financial information, including Social Security and driver's license numbers.

Automatic Information
Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login e-mail address; password; computer and connection information such as browser type, version, and

Layered Policy

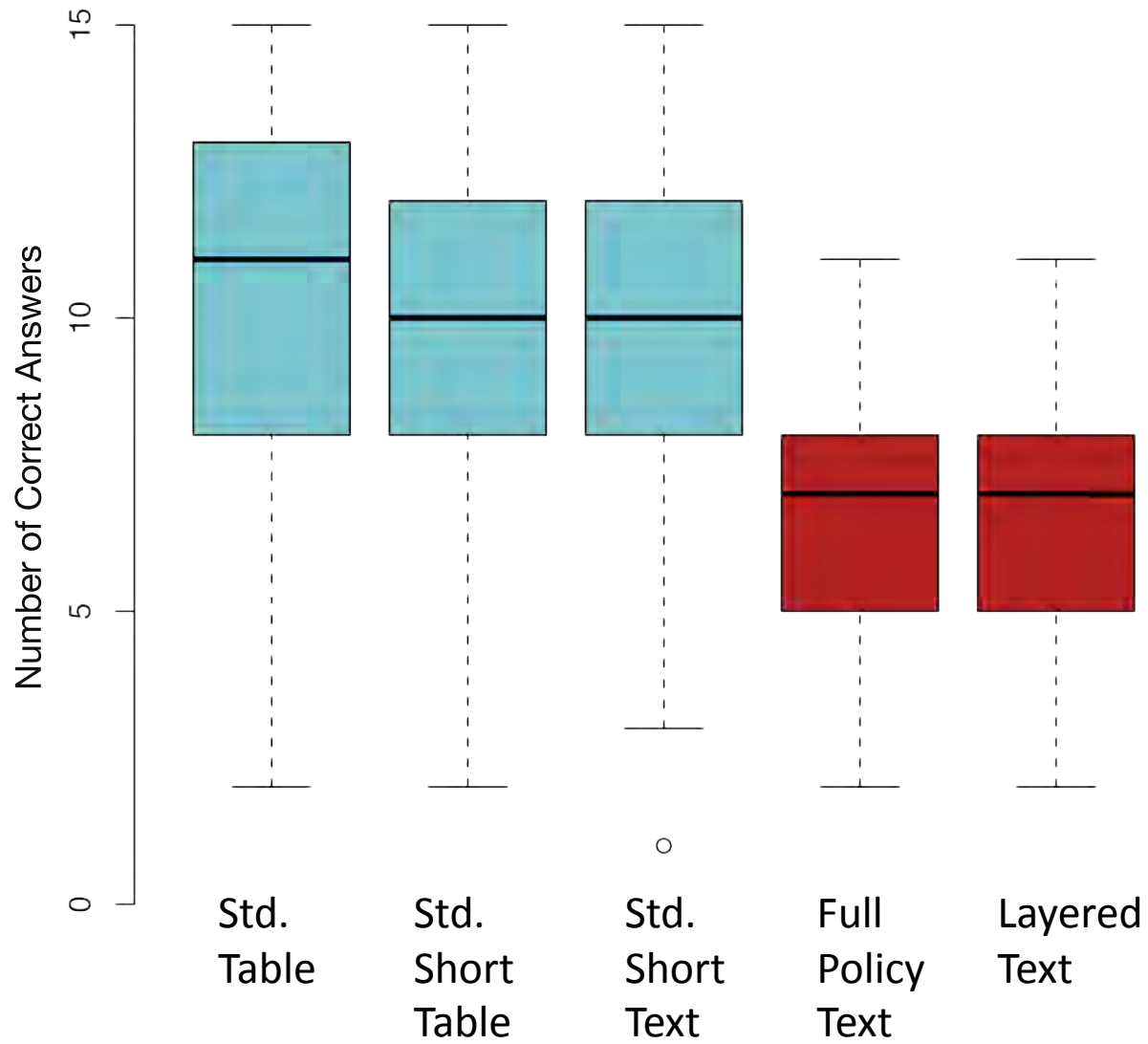
Acme Privacy Notice Highlights

(last updated May 2008)

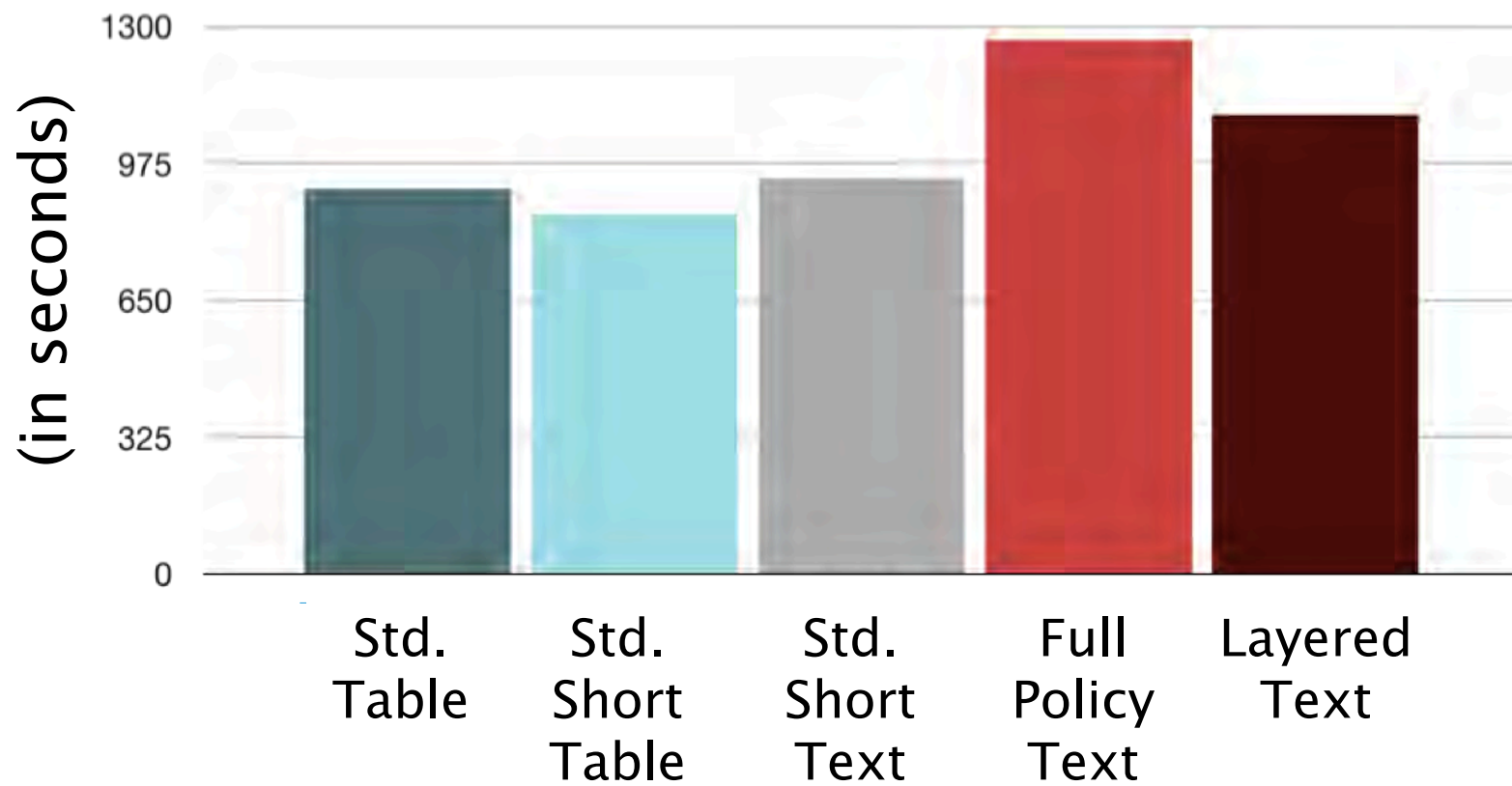


Scope	
This notice provides highlights of the full Acme Online Privacy Statement . This notice and the full privacy statement apply to those Acme Web sites and services that display or link to this notice.	
Personal Information	Your Choices
<ul style="list-style-type: none">•When you register for certain Acme services, we will ask you to provide personal information.•The information we collect may be combined with information obtained from other Acme services and other companies.•We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.	<ul style="list-style-type: none">•You can stop the delivery of promotional e-mail from a Acme site or service by following the instructions in the e-mail you receive.•To make proactive choices about how we communicate with you by e-mail, telephone, and postal mail, follow the instructions listed in the Communication Preferences of the full privacy statement.•To opt-out of the display of personalized advertisements, go to the Display of Advertising section of the full privacy statement.•To view and edit your personal information, go to the access section of the full privacy statement.
Uses of Information	Important Information
<ul style="list-style-type: none">•We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.•We use your information to inform you of other products or services offered by Acme and its affiliates, and to send you relevant survey invitations related to Acme services.•We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.	<ul style="list-style-type: none">•The full Acme Online Privacy Statement contains links to supplementary information about specific Acme sites or services.•The sign in credentials (e-mail address and password) used to sign in to most Acme sites and services are part of the Acme Networks.•For more information on how to help protect your personal computer, your personal information and your family online, visit our online safety resources.•Acme is a member of the TRUSTe privacy seal program.
How to Contact Us	
For more information about our privacy practices, go to the full Acme Online Privacy Statement . Or write us using our Web form . If you have a technical or general support question, please visit http://support.Acme.com to learn more about Acme Support offerings.	
© 2009 Acme Corporation. All rights reserved.	

Overall Accuracy by Format



Timing Results



Enjoyability - Comparisons

(1-7 Likert Scale, 7 is best)



Full policy text torture

- “torture to read and understand”
- likened them to “Japanese Stereo Instructions”

Standardized format better

“This layout for privacy policies is MUCH more consumer friendly. I hope this becomes the industry standard”

Benefits of standardized approach

- Structured information presentation
- Clear labeling of information that is not used or collected
- Standardized terminology to minimize length and increase the clarity of the text
- Definitions of standardized terms


Minor differences between standardized formats

- Standardized table
 - Presents holistic view
- Short table
 - Takes up less space
 - Sometimes makes comparison tasks and tasks about data not collected more difficult
- Text
 - Doesn't scale well for complex policies
 - People more likely to miss text in the middle of paragraphs

- Integrated into <http://privacyfinder.org/>
- Automatically generated from P3P
- Ongoing work to refine label and make it interactive

PrivacyFinder Policy Details for: <http://www.microsoft.com/>

http://www.privacyfinder.org/policy_details?url=http%3A%2F%2F Google

 Search!

Microsoft Corporation

[What do these symbols mean?](#)
[How to contact this site](#)
[Frequently Asked Questions](#)

information we collect	ways we use your information				information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums
contact information		opt out	opt out			
cookies						
demographic information		opt out	opt out			
financial information						
health information						
preferences		opt out	opt out			
purchasing information		opt out	opt out			
social security number & gov't ID						
your activity on this site		opt out	opt out			
your location						

Microsoft Corporation
1 Microsoft Way

[How to resolve privacy-related disputes with this site](#)

[Retention practices for this site](#)
Your data may be retained indefinitely.

Adoption and enforcement

P3P Adoption Studies

- Compiled two lists of search terms:
 - Typical: 20,000 terms randomly sampled from one week of AOL user search queries
 - Ecommerce: 940 terms screen scraped from Froogle front page
- Submitted search terms to Google, Yahoo!, and AOL search engines and collected top 20 results for each term
- Checked each result for P3P policy and evaluated policies against 5 “rulesets” and P3P validator
- Saved 1,232,955 annotated search results in database
- Separately checked for P3P policies on 30,000 domains most clicked on by AOL search engine users

L. Cranor, S. Egelman, S. Sheng, A. McDonald, and A. Chowdhury. [P3P Deployment on Websites](#). *Electronic Commerce Research and Applications*, 2008.

Results

- 10% of results from typical search terms have P3P
- 21% of results from ecommerce search terms have P3P
- More popular sites are more likely to have P3P
- 68% of searches had at least one P3P site in top 10 results
- 29% of top 20 search results returned by AOL search engine for typical search terms had at least 1 P3P site that matches medium privacy preferences
- Frequent errors in P3P policies

P3P compact policy error study

- Collected 33,000+ CPs
- Scripts to check for syntax and semantic errors
- Checked frequency of errors in entire data set plus several interesting subsets
- Checked for corresponding P3P full policies
- Tracked down source of most frequent errors
- Compared some CPs with full P3P policies and human-readable policies

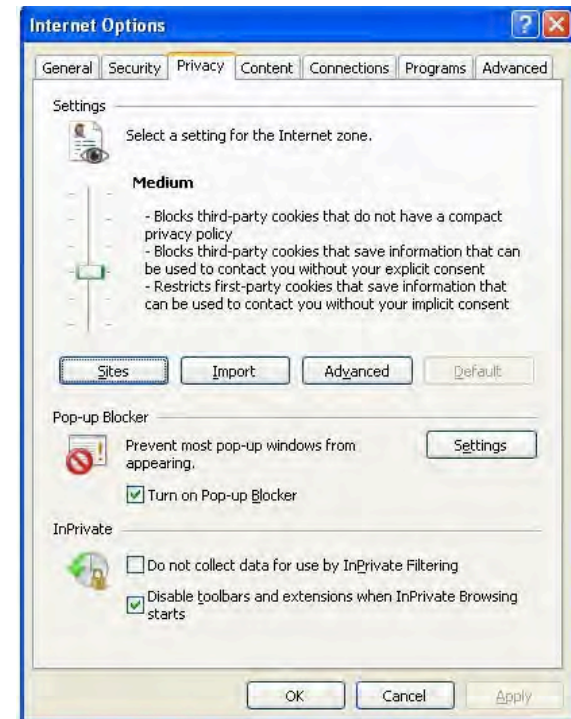
P. Leon, L. Cranor, A. McDonald, and R. McGuire. Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens. WPES 2010. http://www.cylab.cmu.edu/research/techreports/2010/tr_cylab10014.html

P3P compact policies

- String of 3-character and 4-character tokens
- Minimum of 5 required elements
 - Categories: What information is collected?
 - Purpose: How is it used?
 - Recipient: Who has access to it?
 - Retention: How long is it stored?
 - Access: What information can the user access?

Internet Explorer privacy agent

- Default privacy setting
 - Rejects third-party cookies without a CP
 - Rejects unsatisfactory third-party cookies
 - Restricts unsatisfactory first-party cookies
- Does not check for semantic or syntax errors in CPs
 - Unsatisfactory policy gets blocked
 - Policy containing only made-up strings or missing required categories does not get blocked



Crawled web to collect CPs

- 32K+ from Privacy Finder cache
- 3,417 from TRUSTe seal holders
- 100 Quantcast most-visited sites
- 75 network advertisers with their opt-out on BEEF TACO



qu^αntcast



Results

- 34% of 33,139 analyzed CPs had errors (11,176)
 - 12% had invalid tokens (3,839)
 - 19% had missing tokens (6,402)
 - 14% had conflicting tokens errors (4,708)
- Errors found even in most popular, TRUSTe certified, and network advertising sites
- It is likely that more errors exist that we didn't detect automatically
- Many CPs have been crafted to avoid IE cookie filtering
- Large number of web sites using the same erroneous CPs
 - 2,756 sites use the CP suggested by Microsoft
 - 4,360 sites use the CP suggested by O'Reilly blog

PRB: Session Variables Are Lost If You Use FRAMESET in Internet Explorer 6.0

This article was previously published under Q323752

On this Page

- ↓ [SYMPTOMS](#)
- ↓ [CAUSE](#)
- ↓ [RESOLUTION](#)
- ↓ [STATUS](#)
- ↓ [MORE INFORMATION](#)
- ↓ [REFERENCES](#)

Article ID : 323752
Last Review : April 29, 2003
Revision : 1.0

RESOLUTION

You can add a P3P compact policy header to your child content, and you can declare that no malicious actions are performed with the data of the user. If Internet Explorer detects a satisfactory policy, then Internet Explorer permits the cookie to be set.

Visit the following MSDN Web site for a complete list of satisfactory and unsatisfactory policy codes:

Privacy in Internet Explorer 6

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnpriv/html/ie6privacyfeature.asp>

A simple compact policy that fulfills this criteria follows:

```
P3P: CP="CAO PSA OUR"
```

This code sample shows that your site provides you access to your own contact information (CAO), that any analyzed data is only "pseudo-analyzed", which means that the data is connected to your online persona and not to your physical identity (PSA), and that your data is not supplied to any outside agencies for those agencies to use (OUR).

Errors at popular sites

- 21 out of 48 top visited sites using CPs have errors
- 134 out of 391 TRUSTe certified sites' CPs had errors
- 1 out 11 network advertisers with CPs had errors

amazon.com

“AMZN”

invalid and missing 5 categories of tokens

facebook

“DSP LAW”

missing 5 categories of tokens
(previously “HONK”)

Let's talk P3P

By Fran Maler

President

TRUSTe

Last Friday researchers at Carnegie Mellon University published a research report entitled, "Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens". The researchers found invalid P3P compact policies (CP) for approximately 1/3rd of the 33,000 websites they evaluated and found that in 98% of these cases the invalid CPs resulted in cookies remaining unblocked by the Internet Explorer web browser under its default cookie settings. The report alleges that in a number of these cases the CP errors are intentional and amount to cookie blocking work-around by the offending sites. The report identified 134 TRUSTe-certified websites with invalid CPs.

Let's look at the bigger picture

TRUSTe certifies over 3,000 websites and less than 12 percent even use P3P compact policies. Moreover, among that 12 percent the researchers found that only 1/3rd had erroneous CPs. This 1/3rd error rate among TRUSTe-certified, P3P-using

TRUSTe Response

This 1/3rd error rate among TRUSTe-certified, P3P-using sites is virtually identical to what the researchers found in the field at large.

If we find that any ... sites we certify have P3P policies that do not align with their standard web privacy policy, we will assist our clients to ensure that consistency is maintained.

P3P irrelevance resulting from barriers to implementation and disregard by consumers encouraged non-compliance.

The New York Times

Business ■ Innovation ■ Technology ■ Society

September 17, 2010, 2:39 PM

A Loophole Big Enough for a Cookie to Fit Through

By RIVA RICHMOND

If you rely on Microsoft's Internet Explorer's privacy settings to control cookies on your computer, you may want to rethink that strategy.

Large numbers of Web sites, including giants like Facebook, appear to be using a loophole that circumvents I.E.'s ability to block cookies, according to researchers at CyLab at the Carnegie Mellon University School of Engineering.

February 2011 update

- Rechecked 48 top-100 websites with CPs
 - 10 dropped their CPs
 - 3 previously invalid CPs now valid
 - 1 previously invalid improved but contains typo
 - 11 invalid policies remain unchanged
- Amazon now has a valid CP but has a note about why they don't like P3P in place of a full P3P policy
- Facebook's new CP:

P3P:CP="Facebook does not have a P3P policy. Learn why here:
<http://fb.me/p3p>"

Ineffective self-regulation

- CPs cannot be relied on for accurate information about web site privacy policies
- If IE checked for errors, CPs would be more effective in protecting user privacy
- Companies do not have sufficient incentives to provide accurate machine-readable privacy policies
- Unless regulators take action, users will be unable to rely on P3P compact policies

Conclusions and recommendations

Standardization

- Current privacy policies are failing consumers
- Empirical studies show standardized policies are easier and faster to use and facilitate policy comparison

Machine-readable policies

- Even the best policies take time to read and compare
- Machine-readable policies facilitate automated tools that further reduce user burden
- All standardized policy efforts should include machine-readable component

Layers

- Different users are interested in different levels of detail
- Layered policies allow for both simple and detailed views

Standard policy types

- Privacy policies are complex and there are huge numbers of policy variations
- Simplify by mapping detailed policies to a small number of standard “policy types” (Type 1, type 2, type 3, etc.) with corresponding icons
- Consumers could look for their preferred types
- Companies would have incentives to improve policy to comply with types preferred by consumers

P3P vocabulary

- P3P vocabulary should be used as a starting point for future privacy efforts
 - Find specific examples of what it can't express
 - Improve syntax
- Despite its problems, P3P vocabulary is actually pretty good
 - “Ahead of its time”

Incentives and enforcement

“Industry disclosure schemes often founder without strong government/public pressure. Otherwise, companies are simply too busy to adopt them, and customers don’t factor the information disclosed into their buying habits.”

– Esther Dyson, 1997

- There is little reason to believe that other privacy notice/choice standards will be adopted without strong incentives
- Enforcement is essential for the success of future self-regulatory mechanisms



**Carnegie
Mellon
University**

CyLab 

isr institute for
SOFTWARE
RESEARCH

**ENGINEERING &
PUBLIC POLICY**