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

Lorrie Faith Cranor
February 2011
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
Lots of talk about standardizing privacy notices
Advertising option icon
## KnowPrivacy

http://knowprivacy.org

UC Berkeley student project, June 2009

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

**Icon Key**

- yes
- unclear
- no
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.
Privacy Icons

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

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.
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.
### OUT

- Cookies (the tracking kind)
- FIPPS light
- Self-Regulation
- Boucher-Stearns Bill
- Boarded Privacy Notices
- No Practices Are Acceptable
- Privacy by Forcing
- Only online data protected
- Global skepticism of US privacy commitment
- "None of your business - what data we have"

### IN

- Cupcakes 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 sibling process
- Recognition of FTC as ethical global Data Protection Authority group
- Access

*January 2011*
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 TuschaYa Sloneker Communications
Production by Pacific Digital Interactivs
“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

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

— Christine Varney, former FTC Commissioner

“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

“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”

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
Seamless Information Exchange

Will you send me your address?

Only if you won’t use it to market to me

Web site

service

Browser

user agent

information practices

privacy preferences

P3 circa 1997
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

```xml
<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
Privacy Summary for:

Microsoft Corporation

To read this Web site's complete privacy policy, click here.

Privacy Certificate:

Register a dispute

Site statement 1

What kind of information does this Web site collect?

Information that allows an individual to be contacted or located in the physical world, such as a telephone number or a postal address.

Information that allows an individual to be contacted or located on the Internet such as an e-mail address. Often, this information is independent of the physical world.
Move the slider to select a privacy setting for the Internet zone.

**Medium**
- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

To override cookie handling for individual Web sites, click the Edit button.
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/](http://privacyfinder.org/)
PrivacyFinder

Win prizes and help our research
Login here if you already signed up

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

Search Engine: Google, Yahoo!
Preference Level: Medium

Dress, Casual & Athletic Shoes | Zappos.com
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
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
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
Sells mens' and womens' shoes, sandals, boots, and sneakers.
http://www.shoebuy.com/ - Cached - Privacy Policy - Similar Pages

Footwear Shopping in the Yahoo! Directory
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, Sketchers, 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

**POLICY**
- POLICY attributes
- TEST
- ENTITY
- ACCESS
- DISPUTES-GROUP
- additional STATEMENT elements

**DISPUTES-GROUP**
- DISPUTES
- REMEDIES
- additional DISPUTES elements

**STATEMENT**
- CONSEQUENCE
- NON-IDENTIFIABLE
- PURPOSE
- RECIPIENT
- RETENTION
- DATA-GROUP

- = mandatory element
- = optional element (not all optional elements are shown)
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

Share
- Share with parent company
- Share with affiliates
- Share with unaffiliated parties
- Share with contractors
- Share with subsidiaries
- Share in public forums
- Share with ...

Don’t share

P3P
- 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
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

- Share with companies with similar privacy policies
- Share with agents
- Share with delivery companies
- Share with companies with different privacy policies
- Share with companies with unknown privacy policies
- Share in public forums
CMU privacy nutrition label 2009

Information sharing:
- Share with other companies
- Share in public forums

Assumed, no explicit disclosure:
- Share with agents
- Share with delivery companies

Share with companies with:
- Similar privacy policies
- Different privacy policies
- Unknown privacy policies
Mozilla privacy icons 2010

1. Your data is never bartered or sold.
2. Your data is never given to advertisers.
3. Data is given to law enforcement only when legal process is followed.
4. Your data may be bartered or sold.
5. Site gives your data to advertisers.
6. 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
<table>
<thead>
<tr>
<th>Brand</th>
<th>Product</th>
<th>Nutrition Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td>BARBARA'S</td>
<td>Shredded Oats</td>
<td>Nutritional information (as per the image)</td>
</tr>
<tr>
<td>SHREDDED</td>
<td>OAT'S</td>
<td>Nutritional information (as per the image)</td>
</tr>
<tr>
<td>SPOONFULS</td>
<td></td>
<td>Nutritional information (as per the image)</td>
</tr>
<tr>
<td>TRADER JOE'S</td>
<td>Very Berry Clusters</td>
<td>Nutritional information (as per the image)</td>
</tr>
<tr>
<td></td>
<td>CEREAL</td>
<td>Nutritional information (as per the image)</td>
</tr>
</tbody>
</table>

Note: The nutritional information provided is a representation of what is typically found on the back of cereal boxes. Actual values may vary.
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

<table>
<thead>
<tr>
<th>Serving Size 1 cup (228g)</th>
<th>Serving Per Container 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Amount Per Serving</strong></td>
<td></td>
</tr>
<tr>
<td>Calories 250</td>
<td>Calories from Fat 110</td>
</tr>
<tr>
<td>% Daily Value*</td>
<td></td>
</tr>
<tr>
<td>Total Fat 12g</td>
<td>18%</td>
</tr>
<tr>
<td>Saturated Fat 3g</td>
<td>15%</td>
</tr>
<tr>
<td>Cholesterol 30mg</td>
<td>10%</td>
</tr>
<tr>
<td>Sodium 470mg</td>
<td>20%</td>
</tr>
<tr>
<td>Total Carbohydrate 31g</td>
<td>10%</td>
</tr>
<tr>
<td>Dietary Fiber 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Sugars 5g</td>
<td></td>
</tr>
<tr>
<td>Protein 5g</td>
<td></td>
</tr>
</tbody>
</table>

**Vitamin A** 4%  
**Vitamin C** 2%  
**Calcium** 20%  
**Iron** 4%

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

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

### Drug Facts

<table>
<thead>
<tr>
<th>Active ingredient (in each tablet)</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chlorpheniramine maleate 4 mg</td>
<td>Antihistamine</td>
</tr>
</tbody>
</table>

**Uses** temporarily relieves these symptoms due to hay fever or other upper respiratory allergies:

- Swelling
- Running nose
- Itchy, watery eyes
- Itchy throat

**Warnings**

- Ask a doctor before use if you have:
  - Glaucoma
  - Disabling problem such as asthma or chronic bronchitis
  - Trouble urinating due to an enlarged prostate gland
- Ask a doctor or pharmacist before use if you are taking other medicines or are under these conditions:
  - Alcohol, sedatives, or tranquilizers may increase drowsiness
  - Be careful when driving a motor vehicle or operating machinery
  - Muscle weakness 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.

### Energy Guide

**Manufacturer Model**

**More efficient**

- Energy consumption kWh/cycle
  - 1.75 kWh/cycle

**Washing machine** A

### ENERGYGUIDE

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

**This Model Uses** 775 kWh/year

**Uses Least Energy** 742 kWh/year

**Uses Most Energy** 924 kWh/year

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

**$68**
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

Design evolution
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.
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

Physical contact information
Online contact information

Contact information

Preferences
Political & religious affiliations
Content

Preferences

Website login IDs
Click stream data
Activities on the site
Computer information

Your activities on this site
Reducing the columns

- Complete transaction
- System administration
- Research and development
- Customization for current visit

→ Provide services and maintain site

- Pseudonymous decision
- Pseudonymous analysis
- Identified decision
- Identified analysis

→ Profiling

- Companies w/ similar
- Companies w/ different
- Companies w/ unknown

→ Other companies
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

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

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.
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 Revocations
- 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 a possible more useful and interesting, we

Published on Amazon.com
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

- 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.

Your Choices

- 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

- 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.

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

Number of Correct Answers

Std. Table  Std. Short Table  Std. Short Text  Full Policy Text  Layered Text
Timing Results

(in seconds)

<table>
<thead>
<tr>
<th></th>
<th>Std. Table</th>
<th>Std. Short Table</th>
<th>Std. Short Text</th>
<th>Full Policy Text</th>
<th>Layered Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar Graph</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The graph shows a comparison of timing results for different text formats.
Enjoyability - Comparisons

(1-7 Likert Scale, 7 is best)

<table>
<thead>
<tr>
<th></th>
<th>Std. Table</th>
<th>Std. Short Table</th>
<th>Std. Short Text</th>
<th>Full Policy Text</th>
<th>Layered Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enjoyability</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>5</td>
</tr>
</tbody>
</table>
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
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

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

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
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

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

A simple compact policy that fulfills this criteria follows:

P3P: C2="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

“AMZN”
invalid and missing 5 categories of tokens

“DSP LAW”
missing 5 categories of tokens
(previously “HONK”)
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.
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 it’s 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