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
P3P history

- Idea discussed at November 1995 FTC meeting

- Ad Hoc “Internet Privacy Working Group” convened to discuss the idea in Fall 1996

- W3C began working on P3P in Summer 1997
  - Several working groups chartered with dozens of participants from industry, non-profits, academia, government
  - Numerous public working drafts issued, and feedback resulted in many changes
  - Early ideas about negotiation and agreement ultimately removed
  - Automatic data transfer added and then removed
  - Patent issue stalled progress, but ultimately became non-issue

- P3P issued as official W3C Recommendation on April 16, 2002
  - [http://www.w3.org/TR/P3P/](http://www.w3.org/TR/P3P/)
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
P3P is part of the solution

P3P1.0 helps users understand privacy policies but is not a complete solution

- Seal programs and regulations
  - help ensure that sites comply with their policies

- Anonymity tools
  - reduce the amount of information revealed while browsing

- Encryption tools
  - secure data in transit and storage

- Laws and codes of practice
  - provide a base line level for acceptable policies
The basics

- P3P provides a standard XML format that web sites use to encode their privacy policies.

- Sites also provide XML “policy reference files” to indicate which policy applies to which part of the site.

- Sites can optionally provide a “compact policy” by configuring their servers to issue a special P3P header when cookies are set.

- No special server software required.

- User software to read P3P policies called a “P3P user agent”.
P3P1.0 Spec Defines

- A standard vocabulary for describing set of 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 or sites
- A protocol for transporting P3P policies over HTTP
A simple HTTP transaction

GET /index.html HTTP/1.1
Host: www.att.com

HTTP/1.1 200 OK
Content-Type: text/html

Request web page

Send web page
P3P: Introduction

... with P3P 1.0 added

```
GET /w3c/p3p.xml HTTP/1.1
Host: www.att.com
Request Policy Reference File

Web Server

Send Policy Reference File

Request P3P Policy

GET /index.html HTTP/1.1
Host: www.att.com
. . . Request web page

HTTP/1.1 200 OK
Content-Type: text/html
. . . Send web page
```
Transparency

- P3P clients can check a privacy policy each time it changes.
- P3P clients can check privacy policies on all objects in a web page, including ads and invisible images.

http://www.att.com/accessatt/

http://adforce.imgis.com/?adlink|2|68523|1|146|ADFORCE
**P3P in IE6**

Automatic processing of compact policies only; third-party cookies without compact policies blocked by default.

Privacy icon on status bar indicates that a cookie has been blocked - pop-up appears the first time the privacy icon appears.
Users can click on privacy icon for list of cookies; privacy summaries are available at sites that are P3P-enabled.
Privacy summary report is generated automatically from full P3P policy.
Preview version similar to IE6, focusing, on cookies; cookies without compact policies (both first-party and third-party) are “flagged” rather than blocked by default.

Indicates flagged cookie
Users can view English translation of (part of) compact policy in Cookie Manager.
A policy summary can be generated automatically from full P3P policy.
What’s in a P3P policy?

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

Different users are looking for different things, but many common elements

- What information will be collected about me?
- How will it be used?
- Will it be shared with other companies?
- Will it be used to send me unsolicited marketing?
- How can I opt-out? (but many users not aware this is possible)

Our findings consistent with other studies
Why web sites adopt P3P

- Demonstrate corporate leadership on privacy issues
  - Show customers they respect their privacy
  - Demonstrate to regulators that industry is taking voluntary steps to address consumer privacy concerns

- Distinguish brand as privacy friendly

- Prevent IE6 from blocking their cookies

- Anticipation that consumers will soon come to expect P3P on all web sites

- Individuals who run sites value personal privacy
P3P early adopters

- News and information sites – CNET, About.com, BusinessWeek
- Search engines – Yahoo, Lycos
- Ad networks – DoubleClick, Avenue A
- Telecom companies – AT&T
- Financial institutions – Fidelity
- Computer hardware and software vendors – IBM, Dell, Microsoft, McAfee
- Retail stores – Fortunoff, Ritz Camera
- Government agencies – FTC, Dept. of Commerce, Ontario Information and Privacy Commissioner
- Non-profits - CDT
Legal issues

- P3P specification does not address legal standing of P3P policies or include enforcement mechanisms

- P3P specification requires P3P policies to be consistent with natural-language privacy policies
  - P3P policies and natural-language policies are not required to contain the same level of detail
  - Typically natural-language policies contain more detailed explanations of specific practices

- In some jurisdictions, regulators and courts may treat P3P policies equivalently to natural language privacy policies

- The same corporate attorneys and policy makers involved in drafting natural-language privacy policy should be involved in creating P3P policy
<table>
<thead>
<tr>
<th>Privacy policy</th>
<th>P3P policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed to be read by a human</td>
<td>Designed to be read by a computer</td>
</tr>
<tr>
<td>Can contain fuzzy language with “wiggle room”</td>
<td>Mostly multiple choice – sites must place themselves in one “bucket” or another</td>
</tr>
<tr>
<td>Can include as much or as little information as a site wants</td>
<td>Must include disclosures in every required area</td>
</tr>
<tr>
<td>Easy to provide detailed explanations</td>
<td>Limited ability to provide detailed explanations</td>
</tr>
<tr>
<td>Sometimes difficult for users to determine boundaries of what it applies to and when it might change</td>
<td>Precisely scoped</td>
</tr>
<tr>
<td>Web site controls presentation</td>
<td>User agent controls presentation</td>
</tr>
</tbody>
</table>
Impacts

Some companies that P3P-enable think about privacy in new ways and change their practices

- Systematic assessment of privacy practices
- Concrete disclosures – less wiggle room
- Disclosures about areas previously not discussed in privacy policy

Hopefully we will see greater transparency, more informed consumers, and ultimately better privacy policies
P3P Interface design challenges

- P3P 1.0 specification focuses on interoperability, says little about user interface
  - P3P 1.1 spec will provide explanations of P3P vocabulary elements suitable for display to end users

- P3P user agents typically need user interfaces for:
  - informing users about web site privacy policies
  - configuring the agent to take actions on the basis of a user’s privacy preferences
Informing users about privacy is difficult

- Privacy policies are complex
  - Over 36K combinations of P3P “multiple choice” elements

- Users are generally unfamiliar with much of the terminology used by privacy experts

- Users generally do not understand the implications of data practices

- Users are not interested in all of the detail of most privacy policies

- Which details and the level of detail each user is interested in varies
Specifying privacy preferences is difficult

- Privacy policies are complex
- User privacy preferences are often complex and nuanced
- Users tend to have little experience articulating their privacy preferences
- Users are generally unfamiliar with much of the terminology used by privacy experts
Iterative design approach

- Four P3P user agent prototypes developed over 4-year period while P3P specification was under development
  - 1997 - W3C prototype
  - 1999 - Privacy Minder
  - 2000 - AT&T/Microsoft browser helper object
  - 2001 - AT&T usability testing prototype

- AT&T Privacy Bird beta released publicly Feb. 2002
  - August 2002 user study
  - Beta 1.2 released Feb. 2003
Privacy Bird

- Free download of beta from http://privacybird.org/
- “Browser helper object” for IE6
- Reads P3P policies automatically
- Bird icon indicates whether site matches user’s privacy preferences
- Clicking on bird icon gives more information
Bird is privacy indicator

Find web sites that respect your privacy

Many of the web sites you visit may collect your personal information and use it in ways that might surprise you. Privacy Bird® and Privacy Finder are tools that help you find out what web sites will do with your information before you provide it. Privacy Bird is a free tool you can add to your Internet Explorer web browser. Privacy Finder is a free online search engine that will help you identify web sites that respect your privacy.

Download Privacy Bird® now

Privacy Bird reads privacy policies written in the standard format specified by the World Wide Web Consortium’s Platform for Privacy Preferences (P3P).

We invite you to download Privacy Bird software for free. This software will help Internet users stay informed about how information they provide to Web sites could be used. Privacy Bird automatically searches for privacy policies at every website you visit. You can tell the software about your privacy concerns, and it will tell you whether each site’s policies match your personal privacy preferences. The software displays a green bird icon at Web sites that match, and a red bird icon at sites that do not.

Privacy Bird installs quickly and easily into Microsoft Internet Explorer Web browsers (version 5.01/5.5/6.0 on Microsoft Windows platforms). Privacy Bird is the most complete P3P tool currently available. It is the first software to automatically read
Red bird indicates mismatch

Policy Summary

Policy Statement - All users and customers

We use information we collect from you to process your orders, to provide an enhanced and more personalized shopping experience and to inform you and your gift recipients of offers and discounts from 1-800-FLOWERS.COM or other sites and companies that we own.

This site may collect the following types of information about you:

- Messages you send to us or post on this site, such as email, bulletin board postings, or chat room conversations (optional)
- telephone number
- postal address
- click-stream information
- postal address
- gender (optional)
- server stores the transaction history
- user's name
- telephone number
- HTTP protocol information
- email address
- telephone number (optional)
- email address (optional)
- postal address (optional)
- third party’s name
- use of HTTP cookies
Check embedded content too

### Embedded Content

The images and/or other content embedded in this web page are listed below. Some of this content may be covered by a different privacy policy than the rest of the page. Select a URL to view the privacy information related to that content.

<table>
<thead>
<tr>
<th>URL</th>
<th>Privacy Check</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://adlog.com/adlog/e/-9416t&amp;=641518&amp;t=2006.01.06.19.32">http://adlog.com/adlog/e/-9416t&amp;=641518&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/i/-50238&amp;s=614644&amp;t=2006.01.06.19.32">http://adlog.com/adlog/i/-50238&amp;s=614644&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-5077t&amp;=589960&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-5077t&amp;=589960&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-5979s=622717&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-5979s=622717&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/e/-61081t=501815&amp;t=2006.01.06.19.32">http://adlog.com/adlog/e/-61081t=501815&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/i/-7231s=641321&amp;t=2006.01.06.19.32">http://adlog.com/adlog/i/-7231s=641321&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-7544t=501815&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-7544t=501815&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-90886t=501815&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-90886t=501815&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-9165s=623611&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-9165s=623611&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://adlog.com/adlog/a/-9165t=623682&amp;t=2006.01.06.19.32">http://adlog.com/adlog/a/-9165t=623682&amp;t=2006.01.06.19.32</a>...</td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://ads.com/Ads/common/advertisement.gif">http://ads.com/Ads/common/advertisement.gif</a></td>
<td>Matched</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://c7.sedo.com/jpc/mi.html?n=2338c=14t=8&amp;d=3&amp;w=120&amp;h=90">http://c7.sedo.com/jpc/mi.html?n=2338c=14t=8&amp;d=3&amp;w=120&amp;h=90</a>...</td>
<td>Matched</td>
<td>Frame/IF</td>
</tr>
<tr>
<td><a href="http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul">http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul</a></td>
<td>Unknown</td>
<td>Object</td>
</tr>
<tr>
<td><a href="http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul">http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul</a></td>
<td>Unknown</td>
<td>Object</td>
</tr>
<tr>
<td><a href="http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul">http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul</a></td>
<td>Unknown</td>
<td>Object</td>
</tr>
<tr>
<td><a href="http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul">http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul</a></td>
<td>Unknown</td>
<td>Object</td>
</tr>
<tr>
<td><a href="http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul">http://download.macromedia.com/pub/shockwave/cabs/shockwave.cul</a></td>
<td>Unknown</td>
<td>Object</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/213512/deelogoSMB_Color_88x31.gif">http://i.com/Patterns/1/Ads/213512/deelogoSMB_Color_88x31.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/common/b.gif">http://i.com/Patterns/1/Ads/common/b.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/cnwk.1/Ads/213512/deelogoSMB_Color_88x31.gif">http://i.com/Patterns/1/Ads/cnwk.1/Ads/213512/deelogoSMB_Color_88x31.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/213512/deelogoSMB_Color_88x31.gif">http://i.com/Patterns/1/Ads/213512/deelogoSMB_Color_88x31.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/common/b.gif">http://i.com/Patterns/1/Ads/common/b.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
<tr>
<td><a href="http://i.com/Patterns/1/Ads/common/b.gif">http://i.com/Patterns/1/Ads/common/b.gif</a></td>
<td>Unknown</td>
<td>Image</td>
</tr>
</tbody>
</table>
## Privacy settings

These settings control when a warning icon will be displayed at the top of your browser window. You can click on the warning icon for more information.

### Select Privacy Level:
- Low
- Medium
- High
- Custom
- Imported

### HEALTH OR MEDICAL INFORMATION
- Warn me at websites that use my health or medical information:
  - For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
  - To share with other companies (other than those helping the website provide services to me)

### FINANCIAL OR PURCHASE INFORMATION
- Warn me at websites that use my financial information or information about my purchases:
  - For analysis, marketing, or to make decisions that may affect what content or ads I see, etc.
  - To share with other companies (other than those helping the website provide services to me)

### PERSONALLY IDENTIFIED INFORMATION (name, address, phone number, email address, etc.)
- Warn me at websites that may contact me to interest me in other services or products:
  - Via telephone
  - Via other means (email, postal mail, etc.)
  - And do not allow me to remove myself from marketing/mailing lists
- Warn me at websites that use information that personally identifies me:
  - To determine my habits, interests, or other characteristics
  - To share with other companies (other than those helping the website provide services to me)
  - Warn me at websites that do not allow me to find out what data they have about me

### NON-PERSONALLY IDENTIFIED INFORMATION (demographics, interests, websites visited, etc.)
- Warn me at websites that use my non-personally identified information:
  - To determine my habits, interests, or other characteristics
  - To share with other companies (other than those helping the website provide services to me)
Example: Sending Mother’s Day flowers
FTD.COM - Send flowers and gifts delivered fresh from florists - Microsoft Internet Explorer

Search

FTD's 'Good as Gold' Guarantee — Fresh, beautiful flowers and plants that will last at least 7 days.

Order Now $34.99

Order Now $29.99

Mixed Tulips Starting at $29.99

Customer Service ?

Shopping Cart

My Account

International Deliveries | Find a Florist | Reminder Service | Our Guarantee | Browse Our Store

Sign up for Savings!

Email:

Holidays

Valentine's Day

Occasions

Anniversary

Birthday

Congratulations

Friendship

Get Well

Gifts for Business

I'm Sorry

Love & Romance

New Baby

Sympathy & Funeral

Thank You

Thinking of You

Wedding

Shop By Price

Under $25

Flowers

Plants

Roses

Gourmet Gifts

More Gift Ideas

Deliver It Today

Order Now

More like this

Go
PHILLIP'S 1-800-FLORALS
1-800-356-7257

1800Florals SEARCH
Choose A Product
Choose An Occasion
All Price Ranges
Select one or more options and go!


PICKS OF THE WEEK

FTD® Star Gazer™ Bouquet
#9081X $29.95

Multicolor Roses Bowl #5637
$39.95

Pastel Basket Planter #1112T
$49.95
Privacy Finder

- Prototype developed at AT&T Labs, improved and deployed by CUPS
- Uses Google or Yahoo! search API
- Checks for P3P, evaluates against user’s preferences
- Composes search result page with privacy annotations and links to “Privacy Report”
- http://privacyfinder.org/
This site may collect the following types of information about you:

- search terms
- HTTP protocol information
- click-stream information
- use of HTTP cookies
  - Information about your tastes or interests
  - Cookies and mechanisms that perform similar functions
  - Which pages you visited on this web site and how long you stayed at each page
  - Websites login IDs and other identifiers (excluding government IDs and financial account numbers)
  - Information about the computer you are using, such as its hardware, software, or Internet address
  - Email address or other online contact information
  - Name, address, phone number, or other contact information
- third party’s name
- home contact information (optional)
- server stores the transaction history
- user’s name (optional)

The ways your information may be used:

- To aid in historical preservation as governed by a law or policy described in this privacy policy
- To contact you through means other than telephone (for example, email or postal mail) to market services or products -- unless you opt-out
- To make decisions that directly affect you using information about you, for example to recommend products or services based on your previous purchases -- unless you opt-out
- To customize the site for your current visit only
- To do research and analysis in which your information may be linked to an ID code but not to your personal identity
- To contact you by telephone to market services or products -- unless you opt-out
- For research and development, but without connecting any information to you
- To perform web site and system administration
- To provide the service you requested

With whom this site may share your information:

- Other companies whose privacy policies are unknown to this site -- unless you opt-out
- Companies that have privacy policies similar to this site's -- unless you opt-out
- Delivery companies that help this site fulfill your requests and who may also use your information in other ways

Access to your information

Done
UGG Australia 'Classic Tall' Boot
and shearing lining top a lightweight EVA outsole for a style that will keep you stylishly warm and cozy. Pull-on style. Approx. boot shaft height: 12 1/2"; 16" calf circumference. Wide calf. By UGG Australia; Imported. Women's Shoes. Color(s): lilac. Brand: UGG Australia. store.nordstrom.com/product/product.asp?stideid=2887641&cm_vend=yahoo&cm_cat=data... - Privacy Policy - Similar Pages

$69.90

Ugg Classic Sheepskin Boots - Tall for Women
Ugg Classic Sheepskin Boots - Tall for Women. Stylish Ugg boots are bound to be the hottest item this winter. Baby soft pastels are fashionably unique. Suede upper... feedpoint.net/redir.jsp?engine=YP&Pclid=32128&mid=1115398&url=8ovxfr8q6s8u2m7l... - Privacy Policy - Similar Pages

$64.95

Women's Classic Tall Boots by Ugg (Baby Pink Sheepskin)
Step into winter with the Classic Ugg Boot. This boot offers total comfort, warmth and functionality, and the tall version gives a cozy, comfortable feeling against bare legs. Features a molded rubber lugged outsole for traction and slip resistance... feedpoint.net/redir.jsp?engine=YP&Pclid=17228&mid=11123221&url=8vvyi2eg89bMtcnx... - Privacy Policy - Similar Pages

$83.99

UGG Classic Tall Boot
Pull-on style. Suede upper. Flexible rubber sole. Imported. Shearling origin: New Zealand. Chestnut (20), orchid (68); also in sand (17), black (01), blue (40), lilac (55) or pink (66). Full sizes only 5-10M. ... www.offeredby.net/silver/rdm.cm?trkrid=20562510369240 - Privacy Policy - Similar Pages

$130.00

Women's Classic Tall Ugg's Boot
Sand (shown) Cornflower Orchid Sizes Women's Whole Sizes 5-9 (half sizes order down) Some colors and sizes are unavailable Women's Classic Tall Ugg's Boot Apparel & Shoes, Shoes, Women's Shoes, Women's Boots, Women's Fashion Boots ... clickserve.dartsearch.net/link/click?tid=403000000003622169 - Privacy Policy - Similar Pages

$139.95

Black Ugg Classic Tall Boots
Black Tall Classic Ugg Australia boots on our site are IN STOCK NOW... yes right now... so if you order a pair we will ship them to you asap. And yes they are authentic UGG Australia Boots. Special Special Special... For the rest of the month Australiadirect... store.yahoo.com/australiadirect/uggcatalog.html - Privacy Policy - Similar Pages

$140.00

UGG Classic Tall Boot - Sand
UGG's original, authentic boot for ultimate comfort, warmth, and functionality. Taller height is cozy and comfortable against bare legs. 100% premium wool fleece wicks moisture away. Naturally thermostatic, sheepskin maintains body temperature in warm or... www.discountedboots.com/site/604790/product/58155 - Similar Pages

$129.99
Evaluating Privacy Finder

Have enough sites adopted P3P for Privacy Finder to be useful?


Will the prominent display of privacy information cause consumers to take privacy into account when making online purchasing decisions?

P3P adoption study

- Compiled two lists of search terms:
  - Typical: 20,000 terms sampled from week of AOL user 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

- Checked for P3P policies on 30,000 domains most clicked on by AOL search engine users
Frequency of P3P-enabled hits

- P3P-enabled top-20 search results
  - Typical search terms: 10%
  - E-commerce search terms: 21%

- Searches that return at least one P3P-enabled results
  - In top 10 results: 68%
  - In top 20 results: 83%

- AOL users will find sites with “good” privacy policies in first 2 pages of results about 1/3 of the time

- We’ve also collected data about types of privacy practices, types of sites that have adopted P3P, and errors in P3P policies
Results: Most popular P3P policies

**Typical Terms**
- http://privacy.yahoo.com/
- http://about.com/
- http://privacy.msn.com/
- http://disney.go.com/
- http://images.rootsweb.com/
- http://adserver.ign.com/
- http://www.bizrate.com/
- http://www.superpages.com/
- http://www.shopping.com/

**Ecommerce Terms**
- http://privacy.yahoo.com/
- http://about.com/
- http://www.bizrate.com/
- http://www0.shopping.com/
- http://www.shopping.com/
- http://www.pricegrabber.com/
- http://www.cpsc.gov/
- http://www.overstock.com/
- http://www.cooking.com/
- http://www.altrec.com/
Does Privacy Finder influence purchases?

Online shopping studies
- Pay participants to make online purchases with their own credit cards
- Some use Privacy Finder and some use generic search engine
- Experiment with privacy sensitivity of purchase and price sensitivity
- Lab studies
  - Study of college students purchasing power strips and condoms, no price incentive (reimburse cost)
  - Study of Pittsburgh residents purchasing batteries and sex toys, with price incentive (keep the change)
  - Larger study testing additional conditions planned

Privacy Finder field study planned
Lab study design

16 participants in each condition
- Condition 1: No information
- Condition 2: Irrelevant information
- Condition 3: Privacy information

Products
- Non-privacy Sensitive - batteries
- Privacy sensitive - sex toy

Participants paid fixed amount and told to “keep the change”
Privacy information condition

Privacy premium: $0.69 4.8%

Duracell AA Batteries 8-pack
Duracell Coppertop Alkaline AA Batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players.
www.ccvssoftware.com/c/product.html?record@56119

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovy.com/product/DURMN15RT12Z  Privacy Policy

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK
Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Copppertop-Alkaline-Lithium-Bat...  Privacy Policy

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1S008B...  Privacy Policy

Privacy premium: $14.45 (w/shipping)

Privacy premium: $14.60 (w/shipping)

Privacy premium: $14.80 (w/shipping)

Privacy premium: $15.14 (w/shipping)
Duracell Alkaline Battery, AA, 8/PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvssoftware.com/c/product.html?record@56119

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs
discountofficeitems.zoovy.com/product/DURMN15RT12Z

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Bat...

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500BB...
No information condition

Duracell Alkaline Battery, AA, 8/ PK
Duracell Coppertop Alkaline AA Batteries Long-life alkaline batteries provide the best, longest power source.
Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players
www.ccvsoftware.com/c/product.html?record@56119

$14.45 (w/shipping)

Duracell AA8 DURACELL - Alkaline Batteries Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs...
discountofficeitems.zoovy.com/product/DURMN15RT12Z

$14.60 (w/shipping)

Duracell Alkaline Battery Value Packs
Duracell AA8 DURACELL Alkaline Battery Value Packs DURACELL AA ALKALINE BATTERY - 8 PACK
Cardboard card for peg hook 8 pack Specifications Weight 0.45 lbs Length 4.5 inches Width 3.75 inches Height 1 inches Manufactures Web site www.duracell...
www.instawares.com/Coppertop-Alkaline-Lithium-Bat...

$14.80 (w/shipping)

Duracell Coppertop Alkaline AA Batteries
Long-life alkaline batteries provide the best, longest power source. Recommended for use in smoke alarms, flashlights, lanterns, calculators, pagers, cameras, recorders, radios, CD players, medical equipment, toys and electronic games. Dependable after seven years of storage.
www.officequarters.com/product.php/item/DUR-MN1500BB...

$15.14 (w/shipping)
Results

% Purchases by Level of Privacy

- No Information
- Handicap
- Privacy

Level of Privacy

None Low Med. High None Low Med. High

Results

Batteries

Sex Toy
Conclusions

- Accessible privacy information affects consumer behavior
- Consumers willing to pay for better privacy
- Privacy Finder helps users make privacy informed decisions
Deploying P3P on Web Sites
P3P deployment overview

1. Create a privacy policy
2. Analyze the use of cookies and third-party content on your site
3. Determine whether you want to have one P3P policy for your entire site or different P3P policies for different parts of your site
4. Create a P3P policy (or policies) for your site
5. Create a policy reference file for your site
6. Configure your server for P3P
7. Test your site to make sure it is properly P3P enabled
One policy or many?

- P3P allows policies to be specified for individual URLs or cookies
- One policy for entire web site (all URLs and cookies) is easiest to manage
- Multiple policies can allow more specific declarations about particular parts of the site
- Multiple policies may be needed if different parts of the site have different owners or responsible parties (universities, CDNs, etc.)
Third-party content

- Third-party content should be P3P-enabled by the third-party

- If third-party content sets cookies, IE6 will block them by default unless they have P3P compact policy

- Your first-party cookies may become third-party cookies if your site is framed by another site, a page is sent via email, etc.
Cookies and P3P

- P3P policies must declare all the data *stored* in a cookie as well as any data *linked* via the cookie.

- P3P policies must declare all uses of stored and linked cookie data.

- Sites should not declare cookie-specific policies unless they are sure they know where their cookies are going!
  - Watch out for domain-level cookies.
  - Most sites will declare broad policy that covers both URLs and cookies.
Generating a P3P policy

- Edit by hand
  - Cut and paste from an example

- Use a P3P policy generator
  - Recommended: IBM P3P policy editor
    http://www.alphaworks.ibm.com/tech/p3peditor

- Generate compact policy and policy reference file the same way (by hand or with policy editor)

- Get a book
  - *Web Privacy with P3P*
    by Lorrie Faith Cranor
  http://p3pbook.com/
Sites can list the types of data they collect.

And view the corresponding P3P policy.
Locating the policy reference file

- Place policy reference file in “well known location”
  /w3c/p3p.xml
  - Most sites will do this

- Use special P3P HTTP header
  - Recommended only for sites with unusual circumstances, such as those with many P3P policies

- Embed link tags in HTML files
  - Recommended only for sites that exist as a directory on somebody else’s server (for example, a personal home page)
Compact policies

- HTTP header with short summary of full P3P policy for cookies (not for URLs)
- Not required
- Must be used in addition to full policy
- Must commit to following policy for lifetime of cookies
- May over simplify site’s policy
- IE6 relies heavily on compact policies for cookie filtering – especially an issue for third-party cookies
Server configuration

- Only needed for compact policies and/or sites that use P3P HTTP header
- Need to configure server to insert extra headers
- Procedure depends on server – see *P3P Deployment Guide* appendix
  
  http://www.w3.org/TR/p3pdeployment or Appendix B of *Web Privacy with P3P*
Don’t forget to test!

- Make sure you use the P3P validator to check for syntax errors and make sure files are in the right place
  
  http://www.w3.org/P3P/validator/

  - But validator can’t tell whether your policy is accurate

- Use P3P user agents to view your policy and read their policy summaries carefully

- Test multiple pages on your site
XML syntax basics

Element opening tag

< BIG-ELEMENT >
  <element name="value" />
</ BIG-ELEMENT >

Attribute

Comment

<!-- This is a comment -->

Element that contains character data

< ELEMENT > Sometimes data goes between opening and closing tags </ ELEMENT >

Element that doesn't contain other elements (ending slash)

Element closing tag (beginning slash)
 Assertions in a P3P policy

■ General assertions
  • Location of human-readable policies and opt-out mechanisms – `discuri`, `opturi` attributes of `<POLICY>`
  • Indication that policy is for testing only – `<TEST>` (optional)
  • Web site contact information – `<ENTITY>`
  • Access information – `<ACCESS>`
  • Information about dispute resolution – `<DISPUTES>` (optional)

■ Data-Specific Assertions
  • Consequence of providing data – `<CONSEQUENCE>` (optional)
  • Indication that no identifiable data is collected – `<NON–IDENTIFIABLE>` (optional)
  • How data will be used – `<PURPOSE>`
  • With whom data may be shared – `<RECIPIENT>`
  • Whether opt-in and/or opt-out is available – required attribute of `<PURPOSE>` and `<RECIPIENT>`
  • Data retention policy – `<RETENTION>`
  • What kind of data is collected – `<DATA>`
Structure of a P3P policy

- POLICY
  - POLICY attributes
  - TEST
  - ENTITY
  - ACCESS
  - DISPUTES-GROUP
  - STATEMENT
    - 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)
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>
```
The **POLICY** element

- Contains a complete P3P policy
- Takes mandatory `discuri` attribute
  - Indicates location of human-readable privacy policy
- Takes `opturi` attribute (mandatory for sites with opt-in or opt-out)
  - Indicates location of opt-in/opt-out policy
- Takes mandatory `name` attribute
- Sub-Elements
  - `<EXTENSION>`, `<TEST>`, `<EXPIRY>`, `<DATASHEMA>`, `<ENTITY>`, `<ACCESS>`, `<DISPUTES-GROUP>`, `<STATEMENT>`, `<EXTENSION>`

**Example**

```
<POLICY name="general-p3p-policy" discuri="http://www.example.com/privacy.html" opturi="http://www.example.com/opt-out.html">
```

**Diagram**

```
POLICY
  | POLICY attributes
  | TEST
  | ENTITY
  | ACCESS
  | DISPUTES-GROUP
  | STATEMENT
  | additional STATEMENT elements
```
The STATEMENT element

- Data practices applied to data elements
  - mostly serves as a grouping mechanism
- Contains the following sub-elements
  - `<CONSEQUENCE>` (optional)
  - `<NON-IDENTIFIABLE>` (optional)
  - `<PURPOSE>`
  - `<RECIPIENT>`
  - `<RETENTION>`
  - `<DATA-GROUP>`
## Customization purposes

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Does this involve creating a profile of the user?</th>
<th>How is the user identified?</th>
<th>Does this result in a decision that directly affects the user?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research and development</td>
<td>No</td>
<td>user is not identified</td>
<td>No</td>
</tr>
<tr>
<td>One-time tailoring</td>
<td>No</td>
<td>user may not be identified at all, or may be identified with a pseudonym or with personally-identifiable information</td>
<td>Yes</td>
</tr>
<tr>
<td>Pseudonymous analysis</td>
<td>Yes</td>
<td>pseudonym</td>
<td>No</td>
</tr>
<tr>
<td>Pseudonymous decision</td>
<td>Yes</td>
<td>pseudonym</td>
<td>Yes</td>
</tr>
<tr>
<td>Individual analysis</td>
<td>Yes</td>
<td>personally-identifiable information</td>
<td>No</td>
</tr>
<tr>
<td>Individual decision</td>
<td>Yes</td>
<td>personally-identifiable information</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Base Data Schema

- **User data** – *user*
  - *name, bdate, cert, gender, employer, department, jobtitle, home-info, business-info*

- **Third party data** – *thirdparty*
  - Same as *user*

- **Business data** – *business*
  - *name, department, cert, contact-info*

- **Dynamically generated** - *Dynamic*
  - *clickstream, http, clientevents, cookies, miscdata, searchtext, interactionrecord*
**dynamic.miscoedta**

- Used to represent data described only by category (without any other specific data element name)

- Must list applicable categories

- Example

  ```xml
  <DATA ref = "#dynamic.miscoedta" >
    <CATEGORIES>
      <online/>
    </CATEGORIES>
  </DATA>
  ```
Custom data schemas

- You can define your own data elements
- Not required – you can always use categories
- May be useful to make specific disclosures, interface with back-end databases, etc.
- Use the <DATASCHEMA> element
  - Embedded in a policy file or in a stand-alone XML file
Extension mechanism

- `<EXTENSION>` describes extension to P3P syntax

- `optional` attribute indicates whether the extension is mandatory or optional (default is `optional="yes"`)  
  - Optional extensions may be safely ignored by user agents that don’t understand them

- Only useful if user agents or other P3P tools know what to do with them

- Example (IBM `GROUP-INF` extension used to add `name` attribute to `STATEMENT` elements)

```
<STATEMENT>
  <EXTENSION optional="yes">
    <GROUP-INF xmlns="http://www.software.ibm.com/P3P/editor/extension-1.0.html"
      name="Site management"/>
  </EXTENSION>
  ...
</STATEMENT>
```
Compact policy syntax

Part of P3P Header

- **P3P**: CP="NON NID DSP NAV CUR"

Represents subset of P3P vocabulary

- ACCESS (NOI ALL CAO IDC OTI NON)
- CATEGORIES (PHY ONL UNI PUR ... OTC)
- DISPUTES (DSP)
- NON-IDENTIFIABLE (NID)
- PURPOSE (CUR ADM DEV CUS ... OTP) aio
- RECIPIENT (OUR DEL SAM UNR PUB OTR) aio
- REMEDIES (COR MON LAW)
- RETENTION (NOR STP LEG BUS IND)
- TEST (TST)
Policy reference files (PRF)

- Allows web sites to indicate which policy applies to each resource (URL or cookie)
  - Every resource (HTML page, image, sound, form action URL, etc.) can have its own policy

- User agents can cache PRFs (as long as permitted by `EXPIRY`) so they don’t have to fetch a new PRF every time a user clicks
PRF elements

- `<EXPIRY>`
  - Determines how long PRF is valid – default is 24 hours

- `<POLICY-REF>`
  - Provides URL of policy in `about` attribute

- `<INCLUDE>`, `<EXCLUDE>`
  - URL prefixes (local) to which policy applies/doesn’t apply

- `<COOKIE-INCLUDE>`, `<COOKIE-EXCLUDE>`
  - Associates / disassociates cookies with policy – if you want a policy to apply to a cookie, you must use `<COOKIE-INCLUDE>`!

- `<METHOD>`
  - HTTP methods to which policy applies

- `<HINT>`
  - Provides URLs of PRFs for third-party content
PRF example

```xml
<META xmlns="http://www.w3.org/2002/01/P3Pv1" xml:lang="en">
  <POLICY-REFERENCES>
    <EXPIRY max-age="172800"/>
    <POLICY-REF about="http://www.example.com/privacy.xml#policy1">
      <INCLUDE/>
      <INCLUDE>/news/*</INCLUDE>
      <EXCLUDE>/news/top/*</EXCLUDE>
    </POLICY-REF>
    <POLICY-REF about="http://www.example.net/pp.xml#policy2">
      <INCLUDE>/news/top/*</INCLUDE>
    </POLICY-REF>
    <POLICY-REF about="/P3P/policies.xml#policy3">
      <INCLUDE>/photos/*</INCLUDE>
      <INCLUDE>/ads/*</INCLUDE>
      <COOKIE-INCLUDE/>
    </POLICY-REF>
    <HINT scope="http://www.example.org"
          path="/mypolicy/p3.xml"/>
  </POLICY-REFERENCES>
</META>
```
Policy updates

- Changing your P3P policy is difficult, but possible
- New policy applies only to new data (old policy applies to old data unless you have informed consent to apply new policy)
- Technically you can indicate exact moment when old policy will cease to apply and new policy will apply
- But, generally it’s easiest to have a policy phase-in period where your practices are consistent with both policies
- Default policy life time is 24 hours, so phase-in period would be just one day for most sites
Interested in finding a better solution to the password problem?

5-899/08-534/08-734
Usable Privacy and Security

Spring 2008: Mondays and Wednesdays, 1:30-2:50 pm

http://cups.cs.cmu.edu/courses/ups.html