Privacy Preferences

Edgardo Vega
Privacy Preferences

- Introduction to P3P (2002)
- User Interfaces for Privacy Agents (2006)

Lorrie Faith Cranor
Praveen Guduru
Manjula Arjula
INTRODUCTION TO P3P
P3P

Platform for Privacy Preferences

Goals

- Enable the end user to understand what data will be gathered by the site, how the data will be used, and allow the user to have control over that data
- Enable the websites to show their privacy policies in a standard, computer-readable format

Specification

- Standard, computer-readable format for privacy policies
- Protocol to read and process privacy policies automatically
How P3P Works

GET /w3c/p3p.xml HTTP/1.1
Host: www.att.com
Request policy reference file

Send policy reference file

Request P3P policy

Send 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
Major components of a P3P policy

**ENTITY**—contact information for the business, organization, or person who owns the site

**ACCESS**—whether individuals can find out what personal data a site keeps about them in its databases (6 types of access policies are specified)

**DISPUTES**—how to resolve privacy-related disputes with the site (customer-service desk, privacy seals, relevant privacy laws, etc.); also includes REMEDIES subelement

**DATA**—the kinds of data collected (17 data CATEGORY elements and dozens of specific data elements are specified)

**PURPOSE**—how collected data is used and whether individuals can opt-in or opt-out of any of these uses (11 types of purposes and an “other-purpose” are specified, each may take a “required” attribute)

**RECIPIENT**—whether and under what conditions data may be shared and whether there is an opt-in or opt-out (6 types of recipient policies are specified; each may take a “required” attribute)

**RETENTION**—policies for periodic purging of collected data (5 types of retention policies are specified)

**CONSEQUENCE**—human-readable explanation of site’s data practices
Policy File

```xml
<POLICIES xmlns="http://www.w3.org/2002/01/P3Pv1">
  <POLICY discurl="http://p3pbook.com/privacy.html"
     name="policy">
    <ENTITY>
      <DATA-GROUP>
        <DATA>
          ref="#business.contact-info.online.email">privacy@p3pbook.com</DATA>
        </DATA>
        <DATA>
          ref="#business.contact-info.online.uri">http://p3pbook.com/</DATA>
        </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>
```
<POLICIES xmlns="http://www.w3.org/2002/01/p3pv1">
  <POLICY discurl="http://p3pbook.com/privacy.html"
           name="policy">
    <ENTITY />
    <DATA-GROUP>
      <DATA>
        <DATA ref="#business.contact-info.online.email">privacy@p3pbook.com</DATA>
      </DATA>
      <DATA>
        <DATA ref="#business.contact-info.online.uri">http://p3pbook.com/</DATA>
      </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>
User Agents

- Generic term to describe any P3P implementation
  - Web browsers
    - Mozilla
    - IE6
    - Netscape 7
  - Electronic Wallet
  - ISP software
  - Standalone application
  - Search Engines
Implementations

- Compact Policies
  - Cookie filtering decisions only

- P3P Preference Exchange Language (APPEL)
  - Use by an organization to create custom P3P files to distribute to end users

- Privacy Bird and Fox
PRIVACY BIRD
Issues

- Interface for informing users about website privacy policies
- Interface for configuring a user agent to take actions based off the user’s privacy preferences
Privacy Enhancing Technologies (PETs) is part of Fair Information Practices (FIPs)
Challenges

- Privacy policies are difficult
- User preferences are also complex and have nuances
- Users are unfamiliar with the terms
- Users are inexperienced in expressing their preferences
- Users have contradictory expectations
Design

W3C Prototype

Privacy Minder

AT&T/Microsoft P3P Browser Helper Object

AT&T Usability Testing Prototype
Privacy Bird

- A P3P user agent
- Add on for IE 5.01, 5.5, and 6.0
### User Interface

#### Privacy Policy Summary - Yahoo! Inc.

This is a summary of this site's privacy policy. For more details, read the Privacy Fox's detailed translation, or read the site's own, human-readable privacy policy.

<table>
<thead>
<tr>
<th>What data do we collect?</th>
<th>Why do we collect this data?</th>
<th>Can we personally identify you from this data?</th>
<th>Who can see this data?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical contact info.</td>
<td>Telemarketing</td>
<td>Yes</td>
<td>Us</td>
</tr>
<tr>
<td>Website login IDs and other unique identifiers (not government-issued or financial)</td>
<td>Marketing via email or postal mail</td>
<td></td>
<td>Others</td>
</tr>
<tr>
<td>Not Optional: Info about your purchases &amp; payment methods</td>
<td>Web site and system administration</td>
<td></td>
<td>Public</td>
</tr>
<tr>
<td>Not Optional: Info about your computer and Internet connection</td>
<td>Anonymous PSD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Pages you visited on this site and how long you stayed at each page</td>
<td>For pseudonymous profiling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Activities you engaged in at this web site, such as your searches and transactions</td>
<td>To profile you individually</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Demographical info.</td>
<td>For an unspecified other purpose</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Communication between you and the site</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Cookies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Political affiliation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Your medical condition and health interests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Your tastes or interests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Not Optional: Government-issued identifiers such as S.S. numbers</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy Preference 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)
Design Decisions

- Vocabulary Subset
- Bundling Similar Vocabulary Elements
- Removing Jargon
- Using Vocabulary Elements in Combination
- Layered Interfaces
- Default Settings
- Icons and Earcons
Evaluation

- Usefulness and usability of P3P user agents from the perspective of their users
- Controlled laboratory setting as well as how it is used in practice
- Bellotti’s privacy-sensitive design criteria
User Survey

- Yellow bird appeared at most websites
- Strong feelings about the optional sound effects
- Change in online behavior at 88%

- Fewer Form and Opt-Out
- Stopped Visiting Websites
- Compare and Prefer Sites
Laboratory Study

- 12 experienced Microsoft Internet Explorer users who had never used Privacy Bird or the P3P features in IE6
- Given a brief tutorial on Privacy Bird beta 1.2 and the IE6 P3P features
- Answer four questions about a website’s privacy policy.
- Control was to ask user to read an privacy policy at a different website
Questions

1. Whether or not the site might send a visitor unsolicited email
2. Whether or not the site might share a visitor’s email address with another company that might send the visitor unsolicited email
3. Whether or not the site uses cookies
4. Determining what steps a visitor could take to exercise opt-out or unsubscribe options.
## Results (Compare User Agents)

<table>
<thead>
<tr>
<th></th>
<th>Privacy Bird</th>
<th>IE6</th>
<th>Privacy Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average number of correct</td>
<td>3.33 out of 4</td>
<td>2.58 out of 4</td>
<td>3.08 out of 4</td>
</tr>
<tr>
<td>responses to four questions</td>
<td></td>
<td>[3.55 adjusted]</td>
<td></td>
</tr>
<tr>
<td>Average time to answer</td>
<td>259 seconds</td>
<td>408 seconds</td>
<td>285 seconds</td>
</tr>
<tr>
<td>four questions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average time to answer</td>
<td>99 seconds</td>
<td>162 seconds</td>
<td>175 seconds</td>
</tr>
<tr>
<td>question 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average time to answer</td>
<td>61 seconds</td>
<td>81 seconds</td>
<td>28 seconds</td>
</tr>
<tr>
<td>question 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average time to answer</td>
<td>26 seconds</td>
<td>23 seconds</td>
<td>19 seconds</td>
</tr>
<tr>
<td>question 3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average time to answer</td>
<td>73 seconds</td>
<td>142 seconds</td>
<td>64 seconds</td>
</tr>
<tr>
<td>question 4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average rating of ease of</td>
<td>4.17</td>
<td>2.83</td>
<td>2.08</td>
</tr>
<tr>
<td>finding information on five</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>point scale (where five is</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>very easy and 1 is very</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>difficult)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Results (Usefulness)

Table III. Average Ratings of Privacy Bird and IE6 on a Five-Point Scale Where 5 is More Favorable Than 1

<table>
<thead>
<tr>
<th></th>
<th>Privacy Bird</th>
<th>IE6</th>
<th>Paired t-test, two tailed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usefulness</td>
<td>4.17</td>
<td>3.25</td>
<td>$t = 3.53, df = 11, p &lt; .0047$</td>
</tr>
<tr>
<td>Likely to use in the future</td>
<td>4.60</td>
<td>3.50</td>
<td>$t = 2.54, df = 9, p &lt; .032$</td>
</tr>
<tr>
<td>Likely to recommend to a friend</td>
<td>4.58</td>
<td>2.75</td>
<td>$t = 4.53, df = 11, p &lt; .00086$</td>
</tr>
<tr>
<td>Ease of understanding policy summary</td>
<td>4.00</td>
<td>2.67</td>
<td>$t = 5.20, df = 11, p &lt; .00029$</td>
</tr>
<tr>
<td>Ease of finding information</td>
<td>4.17</td>
<td>2.83</td>
<td>$t = 5.20, df = 11, p &lt; .00029$</td>
</tr>
</tbody>
</table>
Results (Other)

- Information Presented by P3P User Agents
- Icons
- Language used in Preference Configuration Interface and Policy Summary
- Privacy Agents as Educational Tools.
Evaluation Criteria

- Trustworthiness
- Appropriate timing
- Perceptibility
- Unobtrusiveness
- Minimal intrusiveness
- Fail safety
- Flexibility
- Low effort
- Meaningfulness
- Learnability
- Low cost
Summary

- Privacy Bird to be both useful and usable.

<table>
<thead>
<tr>
<th>Good</th>
<th>Improve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary format</td>
<td>Policy summary</td>
</tr>
<tr>
<td>Persistent privacy icon</td>
<td>Wording</td>
</tr>
<tr>
<td>Able to determine why warned</td>
<td>Icons</td>
</tr>
<tr>
<td></td>
<td>Obvious expand/collapse</td>
</tr>
</tbody>
</table>
Discussion

- Does simplification run the risk of misleading or confusing users
- What do users want out of privacy policies
- Are privacy preferences independent of the capabilities of a P3P user agent
- Do tools really provide the best way to educated end users
- Why hasn’t P3P adoption taken off