The Platform for Privacy Preferences (P3P)

A user empowerment approach

Marc Langheinrich
APPEL Subgroup Chair
P3P Working Group

ETH Zurich

December 2000 Update
Outline

What is P3P?
- A user empowerment tool
- P3P1.0 a first step - not a full solution

What does P3P provide?
- *Machine-readable privacy policies*
- *Referencing & Exchanging policies*
- *Exchanging Privacy Preferences (APPEL)*

FAQ’s, Wrap-Up
I. What is P3P?

Develop tools that allow people to control the use and dissemination of their personal information
Empowerment Tools

P3P December 2000 Update

I. What is P3P?

- Prevent your actions from being linked to you
  - Crowds (AT&T Labs), Anonymizer, Freedom (zks.net)
- Allow you to develop persistent relationships not linked to each other or you
  - Lucent Personal Web Assistant (Bell Labs)
- Make informed choices about how your information will be used
  - Platform for Privacy Preferences Project - P3P (W3C)
- Know that assurances about information practices are trust worthy
  - TRUSTe, BBBOnline
I. What is P3P?

- **W3C Activity Started Summer 1997**
- **Goals**
  - Web sites offer machine readable policies
  - Browsers automatically compare policies and user preferences
  - Web site & browser negotiate „best deal“
- **P3P 1.0**
  - No negotiation, no choice of policies
  - Goal: Ease of deployment
P3P1.0 Provides

- Machine-readable privacy policies
  - A standard schema for data collected
  - A vocabulary to express purpose, recipients, etc.
  - An XML format for machine-readability
- Referencing & Exchanging policies
  - Reference Files associate P3P policies with Web content (e.g., pages, sites)
  - A protocol for transporting P3P policies over HTTP
Browsing without P3P

II. P3P – Exchanging Policies

Web Server

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
Content-Type: text/html
... Send web page
Browsing with P3P1.0

II. P3P – Exchanging Policies

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
P3P: policyref="http://foo.com/p3p/ref.xml"
Content-Type: text/html
... Send web page

Request Policy Reference File
Send Policy Reference File
Request P3P Policy
Send P3P Policy
The Policy Reference File

II. P3P – Referencing Policies

/w3c/p3p/ref.xml

/w3c/p3p/policy1.xml

/w3c/p3p/policy2.xml

/w3c/p3p/policy3.xml

/index.html
/orders/*.html
/catalog/*

/orders/cgi-bin/*
Set-Cookie: session-id=...

/catalog/kids/*
Reference File Syntax

II. P3P – Referencing Policies

```xml
<META xmlns="http://www.w3.org/2000/11/23/P3Pv1"
    <POLICY-REFERENCES>
    <POLICY-REF web:about="/w3c/p3p/policy1.xml">
        <INCLUDE>/index.html</INCLUDE>
        <INCLUDE>/orders/*.html</INCLUDE>
        <INCLUDE>/catalog/*</INCLUDE>
        <EXCLUDE>/catalog/kids/*</EXCLUDE>
    </POLICY-REF>
    <POLICY-REF web:about="/w3c/p3p/policy2.xml">
        <INCLUDE>/orders/cgi-bin/*</INCLUDE>
        <COOKIES-INCLUDE>session-id .examples.org</COOKIES-INCLUDE>
    </POLICY-REF>
    <POLICY-REF web:about="/w3c/p3p/policy3.xml">
        <INCLUDE>/catalog/kids/*</INCLUDE>
    </POLICY-REF>
</POLICY-REFERENCES>
</META>
```
Reference File Syntax

P3P December 2000 Update

<META xmlns="http://www.w3.org/2000/11/23/P3Pv1"

<POLICY-REFERENCES>

<POLICY-REF web:about="/w3c/p3p/policy1.xml">
  <INCLUDE>/index.html</INCLUDE>
  <INCLUDE>/orders/*.html</INCLUDE>
  <INCLUDE>/catalog/*</INCLUDE>
  <EXCLUDE>/catalog/kids/*</EXCLUDE>
</POLICY-REF>

<POLICY-REF web:about="/w3c/p3p/policy2.xml">
  <INCLUDE>/orders/cgi-bin/*</INCLUDE>
  <COOKIES-INCLUDE>session-id .examples.org /</COOKIES-INCLUDE>
</POLICY-REF>

<POLICY-REF web:about="/w3c/p3p/policy3.xml">
  <INCLUDE>/catalog/kids/*</INCLUDE>
</POLICY-REF>

</POLICY-REFERENCES>

</META>
Reference File Syntax

II. P3P – Referencing Policies

<META xmlns="http://www.w3.org/2000/11/23/P3Pv1"

<POLICY-REFERENCES>

<POLICY-REF web:about="/w3c/p3p/policy1.xml">
  <INCLUDE>/index.html</INCLUDE>
  <INCLUDE>/orders/*.html</INCLUDE>
  <INCLUDE>/catalog/*</INCLUDE>
  <EXCLUDE>/catalog/kids/*</EXCLUSIVE>
</POLICY-REF>

<POLICY-REF web:about="/w3c/p3p/policy2.xml">
  <INCLUDE>/orders/cgi-bin/*</INCLUDE>
  <COOKIES-INCLUDE>session-id .examples.org</COOKIES-INCLUDE>
</POLICY-REF>

<POLICY-REF web:about="/w3c/p3p/policy3.xml">
  <INCLUDE>/catalog/kids/*</inclusive>
</POLICY-REF>

</POLICY-REFERENCES>

</META>
Reference File Syntax

II. P3P – Referencing Policies

<META xmlns="http://www.w3.org/2000/11/23/P3Pv1"
<POLICY-REFERENCES>
    <POLICY-REF web:about="/w3c/p3p/policy1.xml">
        <INCLUDE>/index.html</INCLUDE>
        <INCLUDE>/orders/*.html</INCLUDE>
        <INCLUDE>/catalog/*</INCLUDE>
        <EXCLUDE>/catalog/kids/*</EXCLUDE>
    </POLICY-REF>
    <POLICY-REF web:about="/w3c/p3p/policy2.xml">
        <INCLUDE>/orders/cgi-bin/*</INCLUDE>
        <COOKIES-INCLUDE>session-id .examples.org</COOKIES-INCLUDE>
    </POLICY-REF>
    <POLICY-REF web:about="/w3c/p3p/policy3.xml">
        <INCLUDE>/catalog/kids/*</INCLUDE>
    </POLICY-REF>
</POLICY-REFERENCES>
</META>
P3P Policies

II. P3P – Expressing Policies

- Machine-readable (XML) version of web site privacy policies
  - Use P3P Vocabulary to express data practices
  - Use P3P Base Data Set to express type of data collected

- Captures common elements of privacy policies but may not express everything
  - sites may provide further explanation in human-readable policies
The P3P Vocabulary

II. P3P – Expressing Policies

- **Who** is collecting data?
- Does the data collector provide **access** to my data?
- What **assurance** is there that this policy will be followed?
- Where is the **human-readable** privacy policy?
- **What** data is collected?
- For what **purpose** will data be used?
- Who are the data **recipients** (anyone beyond the data collector)?
- Hong long will data be **retained**?
A set of common data elements all P3P implementations should know about

Includes “User.” elements such as
- name
- Address
- phone number, etc.

Includes “Dynamic.” elements such as
- indicators that a site collects click-stream
- uses cookies
- collects info of a certain category, etc.
Example Privacy Policy

TheCoolCatalogExample, Inc., of 123 Main Street, Seattle, WA 98103 USA, makes the following statement for the Web page at http://www.TheCoolCatalog.example.com/catalog/.

We have a privacy seal from PrivacySealExample, which provides assurance that we abide by our policy. We do provide access capabilities to any identifiable information we may have from you.

We use cookies and collect your gender, information about your clothing preferences, and (optionally) your home address to customize our entry catalog pages and for our own research and product development. We retain this information indefinitely.

We also maintain server logs that include information about visits to the http://www.CoolCatalog.example.com/catalog/ page, and the types of browsers our visitors use. We use this information in order to administrate and improve our web site. We retain this information indefinitely.
II. P3P – Expressing Policies

P3P/XML Encoding

<POLICY xmlns="http://www.w3.org/2000/11/23/P3Pv1">

<ENTITY> ... [machine-readable entity description] ... </ENTITY>

<DISPUTES-GROUP>

<DISPUTES service="http://www.PrivacySeal.example.org"
    resolution-type="independent"
    description="PrivacySeal, a third-party seal provider">

<IMG src="http://www.PrivacySeal.org/Logo.gif"/>

</DISPUTES>

</DISPUTES-GROUP>

<ACCESS><contact-and-other/></ACCESS>

<STATEMENT>

<CONSEQUENCE>

Will will tailor this site to better suit your needs

</CONSEQUENCE>

<RECIPIENT><ours/></RECIPIENT>

<RETENTION><indefinitely/></RETENTION>

<PURPOSE><custom/><develop/></PURPOSE>

<DATA-GROUP>

<Data name="#dynamic.cookies"><CATEGORIES><state/></CATEGORIES></Data>

<Data name="#user.gender"/>

<Data name="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></Data>

<Data name="#user.home." optional="yes"/>

</DATA-GROUP>

</STATEMENT>

<STATEMENT>

<RECIPIENT><ours/></RECIPIENT>

<PURPOSE><admin/></PURPOSE>

<RETENTION><indefinitely/></RETENTION>

<DATA-GROUP>

<Data name="#dynamic.clickstream.server"/>

<Data name="#dynamic.http.useragent"/>

</DATA-GROUP>

</STATEMENT>

</POLICY>
P3P/XML Encoding

II. P3P – Expressing Policies

<ENTITY> ... [machine-readable entity description] ... </ENTITY>

<DISPUTES-GROUP>
  <DISPUTES service="http://www.PrivacySeal.example.org"
    resolution-type="independent"
    description="PrivacySeal, a third-party seal provider">
    <IMG src="http://www.PrivacySeal.org/Logo.gif"/>
  </DISPUTES>
</DISPUTES-GROUP>

<ACCESS><contact-and-other/></ACCESS>

<STATEMENT>
  <CONSEQUENCE>
    Will will tailor this site to better suit your needs
  </CONSEQUENCE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><indefinitely/></RETENTION>
  <PURPOSE><custom/><develop/></PURPOSE>
  <DATA-GROUP>
    <DATA name="#dynamic.cookies"><CATEGORIES><state/></CATEGORIES></DATA>
    <DATA name="#user.gender"/>
    <DATA name="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></DATA>
    <DATA name="#user.home." optional="yes"/>
  </DATA-GROUP>
</STATEMENT>

<STATEMENT>
  <RECIPIENT><ours/></RECIPIENT>
  <PURPOSE><admin/></PURPOSE>
  <RETENTION><indefinitely/></RETENTION>
  <DATA-GROUP>
    <DATA name="#dynamic.clickstream.server"/>
    <DATA name="#dynamic.http.useragent"/>
  </DATA-GROUP>
</STATEMENT>
</POLICY>
<POLICY xmlns="http://www.w3.org/2000/11/23/P3Pv1">
  
  <ENTITY> ... [machine-readable entity description] ... </ENTITY>

  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.example.org"
      resolution-type="independent"
      description="PrivacySeal, a third-party seal provider">
      <IMG src="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES>
  </DISPUTES-GROUP>

  <ACCESS><contact-and-other/></ACCESS>

  <STATEMENT>
    <CONSEQUENCE>
      Will will tailor this site to better suit your needs
    </CONSEQUENCE>

    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>

    <DATA-GROUP>
      <DATA name="#dynamic.cookies"><CATEGORIES><state/></CATEGORIES></DATA>
      <DATA name="#user.gender"/>
      <DATA name="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></DATA>
      <DATA name="#user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>

  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/></PURPOSE>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="#dynamic.clickstream.server"/>
      <DATA name="#dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>

</POLICY>
P3P/XML Encoding

II. P3P – Expressing Policies

<POLICY xmlns="http://www.w3.org/2000/11/23/P3Pv1">
  <ENTITY> ... [machine-readable entity description] ... </ENTITY>
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.example.org"
      resolution-type="independent"
      description="PrivacySeal, a third-party seal provider">
      <IMG src="http://www.PrivacySeal.org/Logo.gif"/>
    </DISPUTES>
  </DISPUTES-GROUP>
  <ACCESS><contact-and-other/></ACCESS>

  <STATEMENT>
    <CONSEQUENCE>
      Will will tailor this site to better suit your needs
    </CONSEQUENCE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><indefinitely/></RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>
    <DATA-GROUP>
      <DATA name="#dynamic.cookies"><CATEGORIES><state/></CATEGORIES></DATA>
      <DATA name="#user.gender"/>
      <DATA name="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></DATA>
      <DATA name="#user.home." optional="yes"/>
    </DATA-GROUP>
  </STATEMENT>

  <STATEMENT>
    <RECIPIENT><ours/></RECIPIENT>
    <PURPOSE><admin/></PURPOSE>
    <RETENTION><indefinitely/></RETENTION>
    <DATA-GROUP>
      <DATA name="#dynamic.clickstream.server"/>
      <DATA name="#dynamic.http.useragent"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
II. P3P – Expressing Policies

<POLICY xmlns="http://www.w3.org/2000/11/23/P3Pv1">
<ENTITY> ... [machine-readable entity description] ... </ENTITY>
<DISPUTES-GROUP>
  <DISPUTES service="http://www.PrivacySeal.example.org"
    resolution-type="independent"
    description="PrivacySeal, a third-party seal provider">
    <IMG src="http://www.PrivacySeal.org/Logo.gif"/>
  </DISPUTES></DISPUTES-GROUP>
<ACCESS><contact-and-other/></ACCESS>
<STATEMENT>
  <CONSEQUENCE>
    Will will tailor this site to better suit your needs
  </CONSEQUENCE>
  <RECIPIENT><ours/></RECIPIENT>
  <RETENTION><indefinitely/></RETENTION>
  <PURPOSE><custom/><develop/></PURPOSE>
  <DATA-GROUP>
    <DATA name="#dynamic.cookies"><CATEGORIES><state/></CATEGORIES></DATA>
    <DATA name="#user.gender"/>
    <DATA name="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></DATA>
    <DATA name="#user.home." optional="yes"/>
  </DATA-GROUP>
</STATEMENT>
<STATEMENT>
  <RECIPIENT><ours/></RECIPIENT>
  <PURPOSE><admin/></PURPOSE>
  <RETENTION><indefinitely/></RETENTION>
  <DATA-GROUP>
    <DATA name="#dynamic.clickstream.server"/>
    <DATA name="#dynamic.http.useragent"/>
  </DATA-GROUP>
</STATEMENT>
</POLICY>
Displaying a Privacy Policy

II. P3P – Expressing Policies

Example of Privacybank.com describing the Starbucks Privacy Policy (non-P3P)
User Privacy Preferences

P3P 1.0 agents may (optionally) take action based on user preferences
- Users should not have to trust privacy defaults set by software vendors
- User agents that can read APPEL (A P3P Preference Exchange Language) files can offer users a number of canned choices developed by trusted organizations
- Preference editors allow users to adapt existing preferences to suit own tastes, or create new preferences from scratch
II. P3P – Expressing Preferences

- **Rules** with 3 standard behaviors
  - request, limited-request, block
  - Optional prompt messages

- **Matching Semantics**
  - Logical connectives
    - and, or; exact match, negation, ...
  - Support matching of P3P policies
Example Preferences

II. P3P – Expressing Preferences

1. Requests for **personal information** which will be given out to **3rd parties** should be **blocked**.

2. The user **does not mind** revealing click-stream and user agent information to sites that collect no other information. However, she insists that the service provides some form of **assurance**.

3. All **other requests** for data transfer should result in a **prompt-message** (indicating a conflict with her privacy preferences).
Example Ruleset

II. P3P – Expressing Preferences

P3P December 2000 Update

<APPEL:APPEL xmlns:APPEL="http://www.w3.org/TR/APPEL"
<APPEL:RULESET crtdby="W3C" crtdon="13-Nov-1999 09:12:32 GMT">
  <APPEL:RULE behavior="block"
    description="Service collects identifiable data for 3rd parties">
    <POLICY><STATEMENT>
      <DATA-GROUP quantifier="or-exact"><DATA name="User.*"/></DATA-GROUP>
      <RECIPIENT quantifier="or">
        <same/><other-recipient/><delivery/><public/><unrelated/>
      </RECIPIENT>
    </STATEMENT></POLICY>
  </APPEL:RULE>

  <APPEL:RULE behavior="request"
    description="Service only collects clickstream data">
    <POLICY><STATEMENT>
      <DATA-GROUP quantifier="or-exact">
        <DATA name="#dynamic.http.useragent"/>
        <DATA name="#dynamic.clickstream.server"/>
      </DATA-GROUP>
    </STATEMENT>
    <DISPUTES-GROUP><DISPUTES service="*"></STATEMENT></DISPUTES-GROUP>
  </POLICY>
</APPEL:RULE>

  <APPEL:RULE behavior="request" prompt="yes"
    description="Suspicious Policy. Beware!">
    <APPEL:OTHERWISE/>
  </APPEL:RULE>

</APPEL:RULESET></APPEL:APPEL>
Example Ruleset

II. P3P – Expressing Preferences

<APPEL:RULE behavior="block"
    description="Service collects identifiable data for 3rd parties">
    <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact">
            <DATA name="User.*"/>
        </DATA-GROUP>
        <RECIPIENT quantifier="or">
            <same/>
            <other-recipient/>
            <delivery/>
            <public/>
            <unrelated/>
        </RECIPIENT>
    </STATEMENT></POLICY>
</APPEL:RULE>

<APPEL:RULE behavior="request"
    description="Service only collects clickstream data">
    <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact">
            <DATA name="#dynamic.http.useragent"/>
            <DATA name="#dynamic.clickstream.server"/>
        </DATA-GROUP>
    </STATEMENT>
    <DISPUTES-GROUP><DISPUTES service="*"></DISPUTES-GROUP>
    </POLICY>
</APPEL:RULE>

<APPEL:RULE behavior="request" prompt="yes"
    description="Suspicious Policy. Beware!">
    <APPEL:OTHERWISE/>
</APPEL:RULE>

</APPEL:RULESET></APPEL:APPEL>
Example Ruleset

II. P3P – Expressing Preferences

<APPEL:APPEL xmlns:APPEL="http://www.w3.org/TR/APPEL">
  <APPEL:RULESET crtdby="W3C" crtdon="13-Nov-1999 09:12:32 GMT">
    <APPEL:RULE behavior="block"
        description="Service collects identifiable data for 3rd parties">
      <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact">
          <DATA name="User.*"/></DATA-GROUP>
        <RECIPIENT quantifier="or">
          <same/><other-recipient/><delivery/><public/><unrelated/>
        </RECIPIENT>
      </STATEMENT></POLICY>
    </APPEL:RULE>

    <APPEL:RULE behavior="request"
        description="Service only collects clickstream data">
      <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact">
          <DATA name="#dynamic.http.useragent"/>
          <DATA name="#dynamic.clickstream.server"/></DATA-GROUP>
      </STATEMENT>
      <DISPUTES-GROUP><DISPUTES service="*"/></DISPUTES-GROUP>
    </POLICY>
  </APPEL:RULE>

    <APPEL:RULE behavior="request" prompt="yes"
        description="Suspicious Policy. Beware!">
      <OTHERWISE/>
    </APPEL:RULE>
  </APPEL:RULESET></APPEL:APPEL>
Example Ruleset

II. P3P – Expressing Preferences

<APPEL:APPEL xmlns:APPEL="http://www.w3.org/TR/APPEL">
  <APPEL:RULESET crtdby="W3C" crtdon="13-Nov-1999 09:12:32 GMT">
    <APPEL:RULE behavior="block"
      description="Service collects identifiable data for 3rd parties">
      <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact"><DATA name="User.*"/></DATA-GROUP>
        <RECIPIENT quantifier="or">
          <same/><other-recipient/><delivery/><public/><unrelated/>
        </RECIPIENT>
      </STATEMENT></POLICY>
    </APPEL:RULE>

    <APPEL:RULE behavior="request"
      description="Service only collects clickstream data">
      <POLICY><STATEMENT>
        <DATA-GROUP quantifier="or-exact">
          <DATA name="#dynamic.http.useragent"/>
          <DATA name="#dynamic.clickstream.server"/>
        </DATA-GROUP>
      </STATEMENT>
    </APPEL:RULE>

    <DISPUTES-GROUP><DISPUTES service="*"></DISPUTES-GROUP>
  </POLICY>
</APPEL:RULESET></APPEL:APPEL>
P3P1.0 Provides (Recap)

- Machine-readable privacy policies
  - A standard schema for data collected
  - A vocabulary to express purpose, recipients, etc.
  - An XML format for machine-readability

- Referencing & Exchanging policies
  - Reference Files associate P3P policies with Web content (e.g., pages, sites)
  - A protocol for transporting P3P policies over HTTP
P3P - Frequently Asked Questions
III. P3P FAQ – Data leakage?

Spilling the Beans?

P3P December 2000 Update

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
P3P: policyref="http://foo.com/p3p/ref.xml"
Content-Type: text/html
... Send web page

Request Policy Reference File
Send Policy Reference File

Request P3P Policy
Send P3P Policy
Methods against leakage

- The „Safe Zone“
  - Should be used for all P3P related communication
  - P3P clients should suppress transmission of unnecessary data (e.g., Referer, Cookies, etc.)
  - P3P server should not require such data for fetching P3P files

- Well-known Policy Reference File
  - Encourages sites to use \( /w3c/p3p.xml \)
  - Can be fetched with minimal disclosure before accessing individual pages
III. P3P FAQ – Data leakage?

p3p.xml

Web Server

GET /x.html HTTP/1.1

... Request web page

HTTP/1.1 200 OK
P3P: policyref="…"
Content-Type: text/html

... Send web page
III. P3P FAQ – Data leakage?

GET /p3p.xml HTTP/1.1
... Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
P3P: policyref="..."
Content-Type: text/html
... Send web page
p3p.xml

GET /p3p.xml HTTP/1.1
... Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
P3P: policyref="…"
Content-Type: text/html
... Send web page

Safe Zone Communication
GET /p3p.xml HTTP/1.1
... Request Policy Reference File

Send Policy Reference File

Request P3P Policy

Send P3P Policy

GET /x.html HTTP/1.1
... Request web page

HTTP/1.1 200 OK
P3P: policyref="..."
Content-Type: text/html
... Send web page
What’s missing in P3P1.0?

P3P December 2000 Update

III. P3P FAQ – What’s missing?

- Allow web sites to offer a choice of policies
  - P3P 1.0 supports only one policy per resource

- Allow for “negotiation” and explicit agreements to be reached between user agent and web site
  - P3P 1.0 features “take-or-leave” functionality

- Allow for non-repudiation of agreements, signatures from third-party seal providers, etc.
  - P3P 1.0 comes in plain text, no possibility to prove that certain communication took place

- Facilitate automated data transfer
  - P3P 1.0 requires external mechanisms (e.g., form-fill) to transfer data
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
Can I Trust a P3P Policy?

III. P3P FAQ – Trusting a policy?

- No Worse Off than We are Today
  - Web site publishes privacy policy
  - Visitor has to take at face value

- Seal Programs Ensure Compliance
  - Provide dispute resolution
  - Contract provides legal binding

- Market Forces: Trust Pays!
  - Doubleclick Example
How Long Does it Take?

Surfing with P3P takes longer
- Find policy
- Download policy
- Evaluate policy

Speed-ups
- Caching (EXPIRY element)
- Providing policies for embedded content (EMBEDDED-INCLUDE element)
- Compact policies
Compact P3P Policies

- Summarized P3P policy for cookies only
  - ACCESS, DISPUTES, REMEDIES, NON-IDENTIFIABLE, PURPOSE, RECIPIENT, RETENTION, CATEGORY
  - Optional for both clients and servers

- Specified in the HTTP response
  - Describes cookies set in response
  - Allows synchronous evaluation

- Example

  HTTP/1.1 200 OK
  P3P: Policyref="...", CP="NON CUSo OUR PREV NAV UNI"
  Set-Cookie: session-id=320-2931; domain=.example.com path=/
  Content-Type: text/html
  ...

  ...
How Does it Look?

A Number of Prototypes available

- Microsoft/AT&T P3P Browser Helper Object
- Idcide Privacy Companion
- YOUpowered Orby Privacy Plus
- ...

III. P3P FAQ – Client Prototypes
III. P3P FAQ – Client Prototypes

A privacy check has been performed to compare your personal privacy settings and the corresponding privacy rules to the privacy policy of the web site you are currently visiting.

View policy: [http://www.att.com](http://www.att.com)

There are no warnings.

Legend: ☑ Privacy OK  🚸 Privacy policy unknown  🚭 Privacy violation
A privacy check has been performed to compare your personal privacy settings and the corresponding privacy rules to the privacy policy of the web site you are currently visiting.

View policy: http://www.ttuhscl.edu

This site does not allow you to find out what data they have about you.

Legend: Privacy OK Privacy policy unknown Privacy violation

A privacy check has been performed to compare your personal privacy settings and the corresponding privacy rules to the privacy policy of the web site you are currently visiting.

View policy: http://www.microsoft.com

This site may collect data that does identify you for profiling.

Legend: Privacy OK Privacy policy unknown Privacy violation
A privacy check has been performed to compare your personal privacy settings and the corresponding privacy rules to the privacy policy of the website you are currently visiting.

View policy: http://www.ttuhscl.edu

This site does not allow you to find out what data they have about you.

Legend:  Privacy OK  Privacy policy unknown  Privacy violation

A privacy check has been performed to compare your personal privacy settings and the corresponding privacy rules to the privacy policy of the website you are currently visiting.

View policy: http://www.microsoft.com

There are no warnings.

Legend:  Privacy OK  Privacy policy unknown  Privacy violation
How do I P3P-enable a Site?

- Formulate privacy policy
- Translate privacy policy into P3P format
  - Using a policy generator tool
- Place P3P policy on web site
  - One policy for entire site or multiple policies for different parts of the site
- Associate policy with web resources:
  - Place P3P policy reference file at well-known location (p3p.xml) on server;
  - Configure server to insert P3P header with link to P3P policy; or
  - Insert link to P3P policy in HTML content
IBM P3P Policy Editor

- Allows web sites to create privacy policies in P3P and human-readable format
- Drag and drop interface
- Available from IBM AlphaWorks site: http://www.alphaworks.ibm.com/tech/p3peditor
Sites can list the types of data they collect and view the corresponding P3P policy.
Properties windows allows sites to specify detailed information about how each type of data is used.
The Take Home Message

December 2000 Update
P3P 1.0

- Is ...
  - a user empowerment tool
  - is not a solution in itself

- Provides ...
  - XML encoding, vocabulary & base data set to express privacy practices
  - Reference files and exchange protocol for publishing privacy practices
  - Optional preference exchange language (APPEL)

- Allows ...
  - Easy deployment
  - Wide range of client applications
Resources and Feedback

P3P December 2000 Update

For further info on P3P see
http://www.w3.org/P3P/

Send comments to
www-p3p-public-comments@w3.org