



E-Privacy – Privacy in the Electronic Society

Privacy Policy Languages

Günter Karjoth

Spring term 2009

This presentation contains material from:
Marc Langheinrich: "Internet Privacy and P3P." WWW10 Tutorial, May 1, 2001.
Used by permission.

Some Approaches to Improve Privacy

- Laws and Regulations
- Voluntary Guidelines and Codes of Conduct
- Privacy Policies
- Seal Programs
- Privacy Tools

Privacy-enhancing technologies (PETs)

"Privacy Enhancing Technologies (PET) are a coherent system of Information and Communication Technologies measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system."

[Borking and Raab, 2001]

Encryption tools

Prevent others from listening in on your communications

Anonymity tools

Prevent your actions from being linked to you

Transparency tools

Make informed choices about how your information will be used

Trust tools

Know that assurances about information practices are trust worthy

Five-part Privacy Model (*)

1. Notice / Awareness
2. Choice / Consent
3. Access / Participation
4. Integrity / Security
5. Enforcement / Redress

→ no collection limitation

(*) developed around 1995 – 1997 by

U.S. Department of Commerce's National Telecommunications and Information Administration (NCIA)

U.S. Federal Trade Commission

Privacy Policies

- ❑ Policies let consumers know about site's privacy practices.
- ❑ Consumers can then decide whether or not practices are acceptable, when to opt-in or opt-out, and who to do business with.
- ❑ The presence of privacy policies increases consumer trust
- ❑ but policies are often
 - difficult to understand,
 - hard to find,
 - take a long time to read (usually 3-4 pages!), and
 - may change without notice.

Privacy policy components

- Identification of site, scope, contact info
 - Types of information collected
 - Including information about cookies
 - How information is used
 - Conditions under which information might be shared
 - Information about opt-in/opt-out
 - Information about access
 - Information about data retention policies
 - Information about seal programs
- Security assurances
 - Children's privacy

There is lots of information to convey -- but policy should be brief and easy-to-read too!

What is opt-in? What is opt-out?

from: [Lorrie Cranor](#),

Platform for Privacy Preferences Project (P3P)

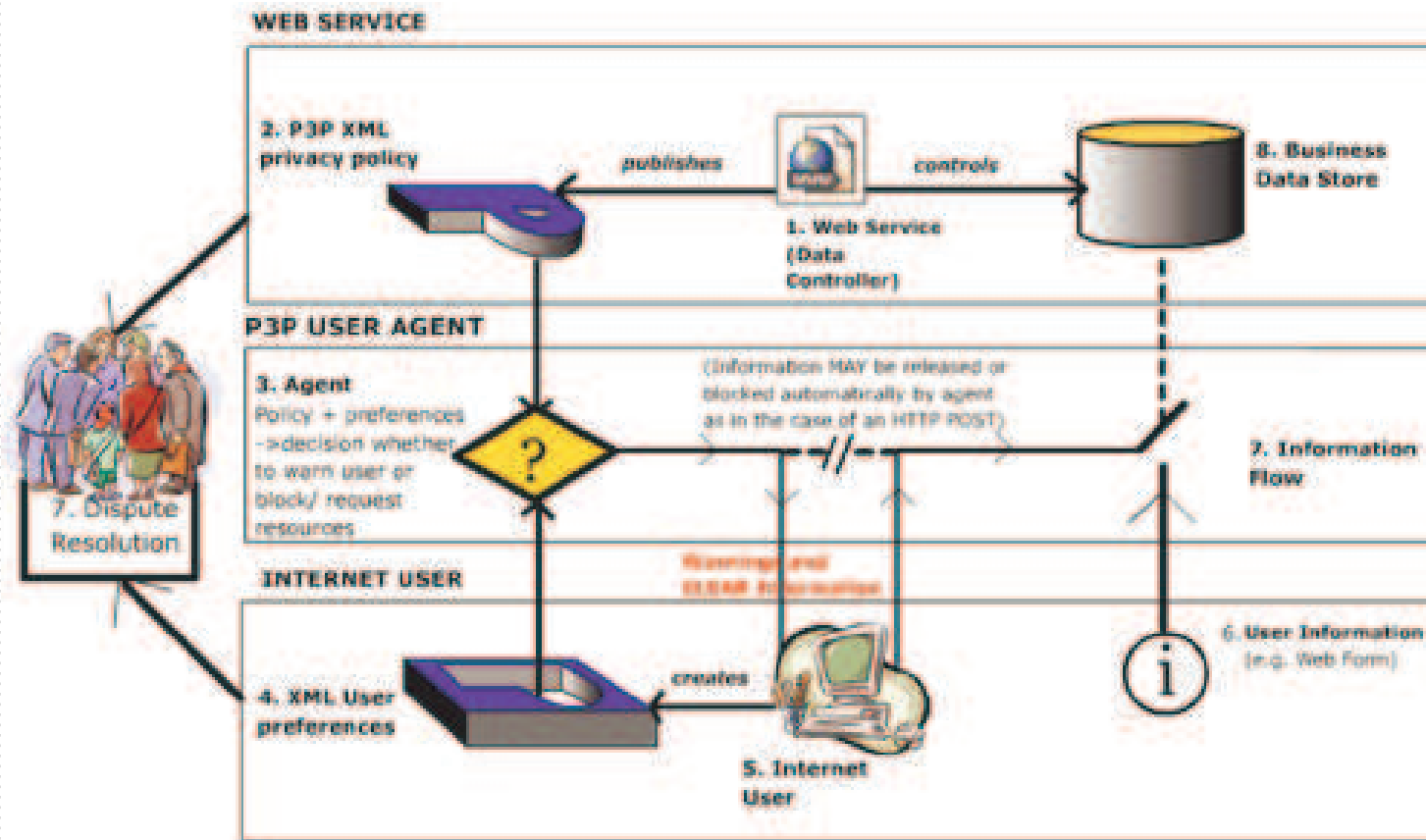
P3P – a tool for notice & consent

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
- developed by the W3C (World-Wide Web Consortium)

What is P3P? Overview Diagram



[from Hogben et al, 2002]

Five-part Privacy Model (*)

1. Notice / Awareness
2. Choice / Consent
3. Access / Participation
4. Integrity / Security
5. Enforcement / Redress

→ no collection limitation

(*) developed around 1995 – 1997 by

U.S. Department of Commerce's National Telecommunications and Information Administration (NCIA)

U.S. Federal Trade Commission

Structure of a P3P Policy

The site's internal privacy policies:

- Where can the detailed policies be found in “human readable form”?
- What is the contact information for the legal entity responsible for the privacy practices of the Web site?
- Can users make changes in how their data is used?
- How are disputes resolved?
- What is the policy for retaining data?

The data being tracked by the site:

- Who is collecting the data?
- What information is being collected?
- For what purposes?
- Which information is being shared with others?
- And who are these data recipients?

Example Privacy Policy

At CatalogExample, we care about your privacy. When you come to our site to look for an item, we will only use this information to improve our site and will not store it in an identifiable way.

CatalogExample is a licensee of the PrivacySealExample Program. ...

Questions regarding this statement should be directed to: CatalogExample 1-248-392-6753

When you browse through our site we collect:

- The basic information about your computer and connection to make sure that we can get you the proper information and for security purposes

- Aggregate information on what pages consumers access or visit to improve our site

We purge the browsing information that we collect regularly.

P3P/XML Encoding

```
<POLICY xmlns="http://www.w3.org/2000/12/P3Pv1"
discuri="http://www.catalog.example.com/Privacy.html">
  <ENTITY>
    <DATA-GROUP><DATA ref="#business.name">CatalogExample</DATA>
      <DATA ref="#business.contact-info.telecom.telephonenumber.intcode">1</DATA>
      <DATA ref="#business.contact-info.telecom.telephonenumber.loccode">248</DATA>
      <DATA ref="#business.contact-info.telecom.telephonenumber.number">3926753</DATA>
    </DATA-GROUP></ENTITY>
  <ACCESS><nonident/></ACCESS>
  <DISPUTES-GROUP> <DISPUTES resolution-type="independent"
    service="http://www.PrivacySeal.example.org"
    short-description="PrivacySeal.exampleorg"
    <REMEDIES><correct/></REMEDIES>
    <IMG src="http://www.PrivacySeal.example.org/Logo.gif"/>
  </DISPUTES></DISPUTES-GROUP>
  <STATEMENT>
    <PURPOSE><admin/><develop/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <RETENTION><stated-purpose/></RETENTION>
    <DATA-GROUP>
      <DATA ref="#dynamic.clickstream"/>
      <DATA ref="#dynamic.http"/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```



P3P Vocabulary

The DISPUTES Element (optional)

- Describes a dispute resolution procedure
 - may be followed for disputes about a service's privacy practices
- Part of a **<DISPUTES-GROUP>**
 - allows several dispute resolution procedures to be listed
- Attributes:
 - resolution-type*
 - customer service
 - independent org.
 - court
 - applicable law
 - service* (URI)
 - short-description
 - verification (URI)
- Sub-Elements
 - <IMAGE>
 - <LONG-DESCRIPTION>
 - <REMEDIES>

* Mandatory Attribute

The REMEDIES Element

- Sub element of DISPUTES element
- Specifies possible remedies in case a policy breach occurs
 - <correct/>, <money/>, <law/>
- Example <DISPUTES-GROUP>

```
<DISPUTES-GROUP>
  <DISPUTES
    resolution-type="independent"
    service="http://www.PrivacySeal.org"
    description="PrivacySeal.org"
    image=http://www.PrivacySeal.org/Logo.gif>
    <REMEDIES><correct/></REMEDIES>
  </DISPUTES>
</DISPUTES-GROUP>
```

The ACCESS Element

- Indicates the ability of individuals to access their data
 - <nonident/>*
 - <all/>
 - <contact-and-other/>
 - <ident-contact/>
 - <other-ident/>
 - <none>

- but the method of access is not specified
 - imposes challenges on how to implement

* Web site does not collect identified data

The STATEMENT Element

- Data practices applied to data elements
 - mostly serves as a grouping mechanism
- Contains the following sub-elements:
 - <CONSEQUENCE>
 - <NON-IDENTIFIABLE>⁺
 - <PURPOSE>^{*}
 - <RECIPIENT>^{*}
 - <RETENTION>^{*}
 - <DATA-GROUP>

* Mandatory Elements

⁺ either no data is collected or data collected [in the statement] will be anonymized

The CONSEQUENCE Element

- Consequences that can be shown to a human user
 - to explain why the suggested practice may be valuable in a particular instance, even if the user would not normally allow the practice
- Example:

```
<CONSEQUENCE>A site with clothes you would  
appreciate</CONSEQUENCE>
```

The PURPOSE Element

- Purposes of data collection, or uses of data
 - `<current/>`
 - `<admin/>`
 - `<develop/>`
 - `<customization/>`
 - `<tailoring/>`
 - `<pseudo-analysis/>`
 - `<pseudo-decision/>`
 - `<individual-analysis/>`
 - `<individual-decision/>`
 - `<contact/>`
 - `<historical/>`
 - `<telemarketing/>`
 - `<other-purpose/>`
- Optional attribute:
 - required
 - always (default)
 - opt-in
 - opt-out
- Example:

```
<PURPOSE>  
  <admin />  
  <develop  
    required="opt-out" />  
</PURPOSE>
```

(*) “completion and support of activity for which data was provided”
but without defining the scope of this activity

The RECIPIENT Element

- Recipients of the collected data
 - <ours>
 - <delivery>
 - <same>
 - <other-recipient>
 - <unrelated>
 - <public>
- Note:
 - <delivery> only used if delivery service does NOT agree to use data only for completion of delivery.
- Optional attribute (all but <ours>):
 - required
 - always (default)
 - opt-in
 - opt-out
- Optional sub-element:
 - <recipient-description>
- Example:

```
<RECIPIENT>  
  <ours />  
  <delivery  
    required="opt-out" />  
</PURPOSE>
```

The RETENTION Element

- Indicates the kind or retention policy that applies to the referenced data
 - <no-retention/>
 - <stated-purpose/>
 - <legal-requirement/>
 - <business-practices/>
 - <indefinitely/>
- Example:

```
<RETENTION><indefinitely/></RETENTION>
```

The DATA Element

- ❑ Describes the data to be transferred or inferred
- ❑ Contained in a DATA-GROUP
- ❑ Attributes:
 - ref*
 - optional
- ❑ Sub-Elements:
 - <CATEGORIES>
- ❑ Example:

```
<DATA-GROUP>  
  <DATA ref="#dynamic.miscdata">  
    <CATEGORIES></preference></political></CATEGORIES>  
  </DATA>  
  <DATA ref="#user.home-info" optional="yes" />  
</DATA-GROUP>
```

* Mandatory Attribute

The CATEGORIES Element

- Provides hints to user agents as to the intended uses of the data
- Physical contact information
- Online contact information
- Unique identifiers
- Purchase information
- Financial information
- Computer information
- Navigation and click-stream data
- Interactive data
- Demographic and socio-economic data
- Content
- State management mechanisms
- Political information
- Health information
- Preference data
- Government-issued identifiers
- other

P3P: Statement Example

<POLICY>

... ..

<STATEMENT>

<PURPOSE>

<individual-decision required="always"/>

<contact required="opt-in"/>

</PURPOSE>

<RECIPIENT><ours/></RECIPIENT>

<RETENTION><business-practices/></RETENTION>

<DATA-GROUP>

<DATA ref="#customer.home-info.postal"/>

<DATA ref="#dynamic.miscdata"/>

<CATEGORIES><demographic/><physical/></CATEGORIES>

</DATA>

</DATA-GROUP>

</STATEMENT>

</POLICY>

Compact Policies (CP)

- ❑ *Optional* performance optimization
- ❑ Summary of (full) P3P policies but only applies to cookies:
 - Allows quick decision whether to accept or reject cookie
 - If not enough information, full policy should be fetched
 - Must declare both data **stored** and **linked to** cookie
 - Only for cookies set in **current response**
- ❑ Part of P3P Header
 - `P3P: policyref="...", CP="NON NID DSP NAV CUR"`
- ❑ Supports 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)

Practical experiences with using P3P

Retention

- Actual maximal time-span is only required in the human-readable text.
- With multiple purposes, data can be retained as long as any of the stated purposes are still active
- variety of retention times for the same data element

Recipients and Purposes

- Fuzzy and mixes notions of business relationship & policy
 - delivery
 - same (no disclosure if receiving entity uses it only once ?)
 - other-recipient
- Purposes
 - Pseudo-analysis, pseudo-decision
 - Contact: “for marketing of services or products” but not
 - via phone (telemarketing)
 - via customized Web content or banner advertisements (tailoring, pseudo/individual-analysis, pseudo/individual-decision)



P3P Data Schemas

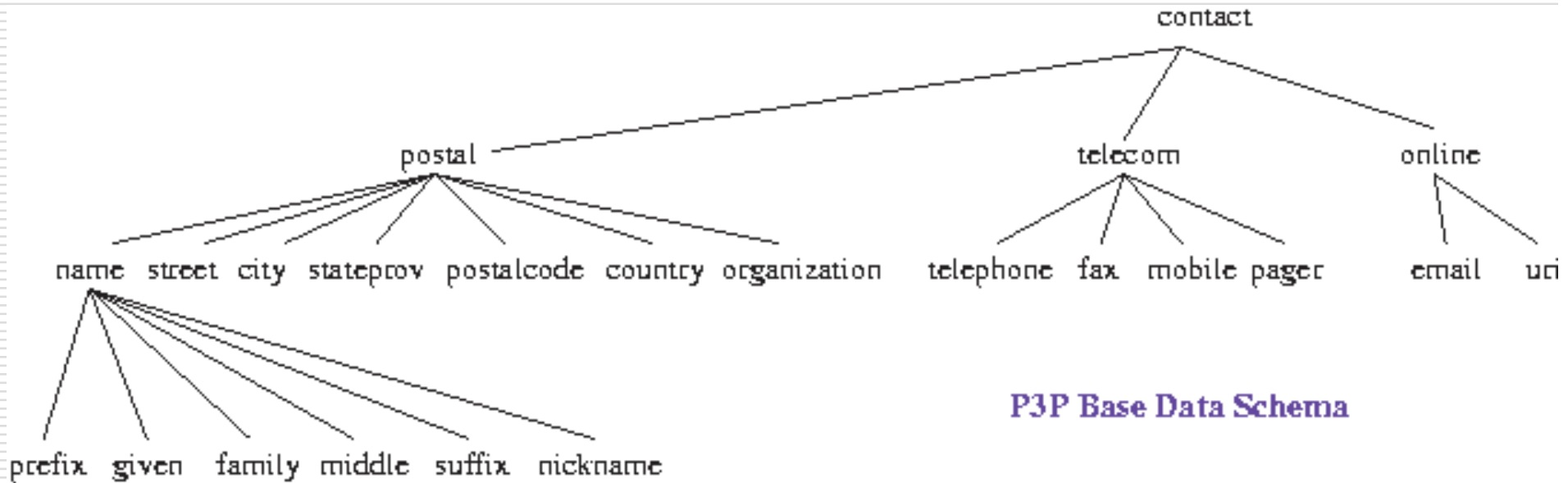
Base Data Schema

- 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
- Dynamic
 - clickstream, http, clientevents, cookies, miscdata, searchtext, interactionrecord

P3P Base Data Structures

- Dates
- Names
- Certificates
- Login Information
- Telephone numbers
- Contact information
- Post mailing address
- Telecommunication numbers
- Online addresses
- URIs & IP addresses
- Access log information
- ...

P3P Base Data Structures



- user data set (112 elements)
 - thirdparty and business
- dynamic data set

dynamic.miscdata

- Used to represent data described only by category (without any other specific data element name)
- Must list applicable categories
- Example:

```
<POLICY ...>  
  . . .  
  <DATA ref = " #dynamic.miscdata" >  
    <CATEGORIES><online/></CATEGORIES>  
  </DATA>  
  . . .  
</POLICY>
```

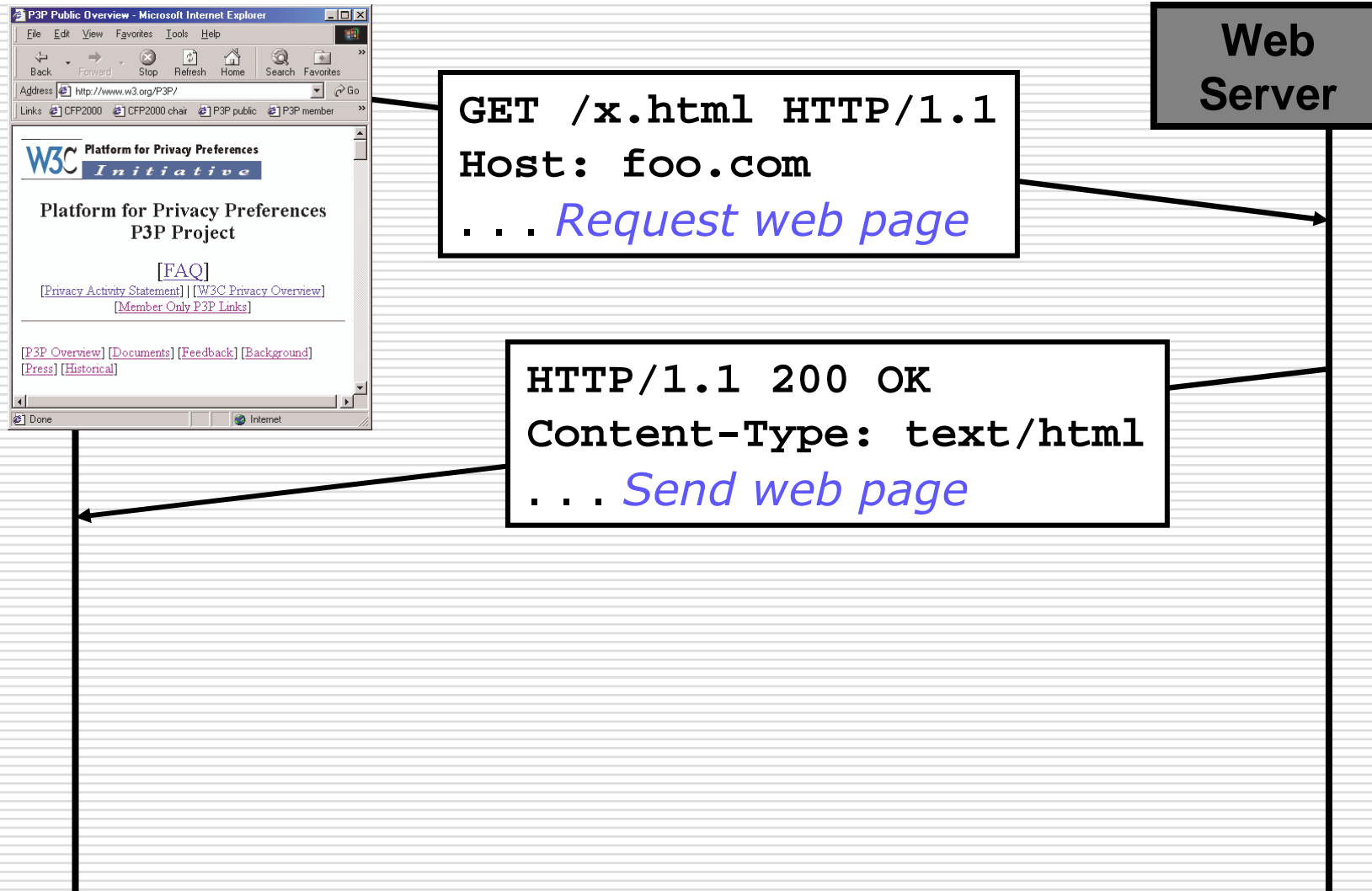
Custom Data Schemas

- Use the `<DATASHEMA>` element
 - Embedded in a policy or in a stand-alone XML file
 - Use `<DATA-DEF>` and `<DATA-TYPE>` elements to define data elements and data types respectively
- **Updates** in referenced XML schema files must either be **backwards-compatible**, or a new name (URI) must be used!

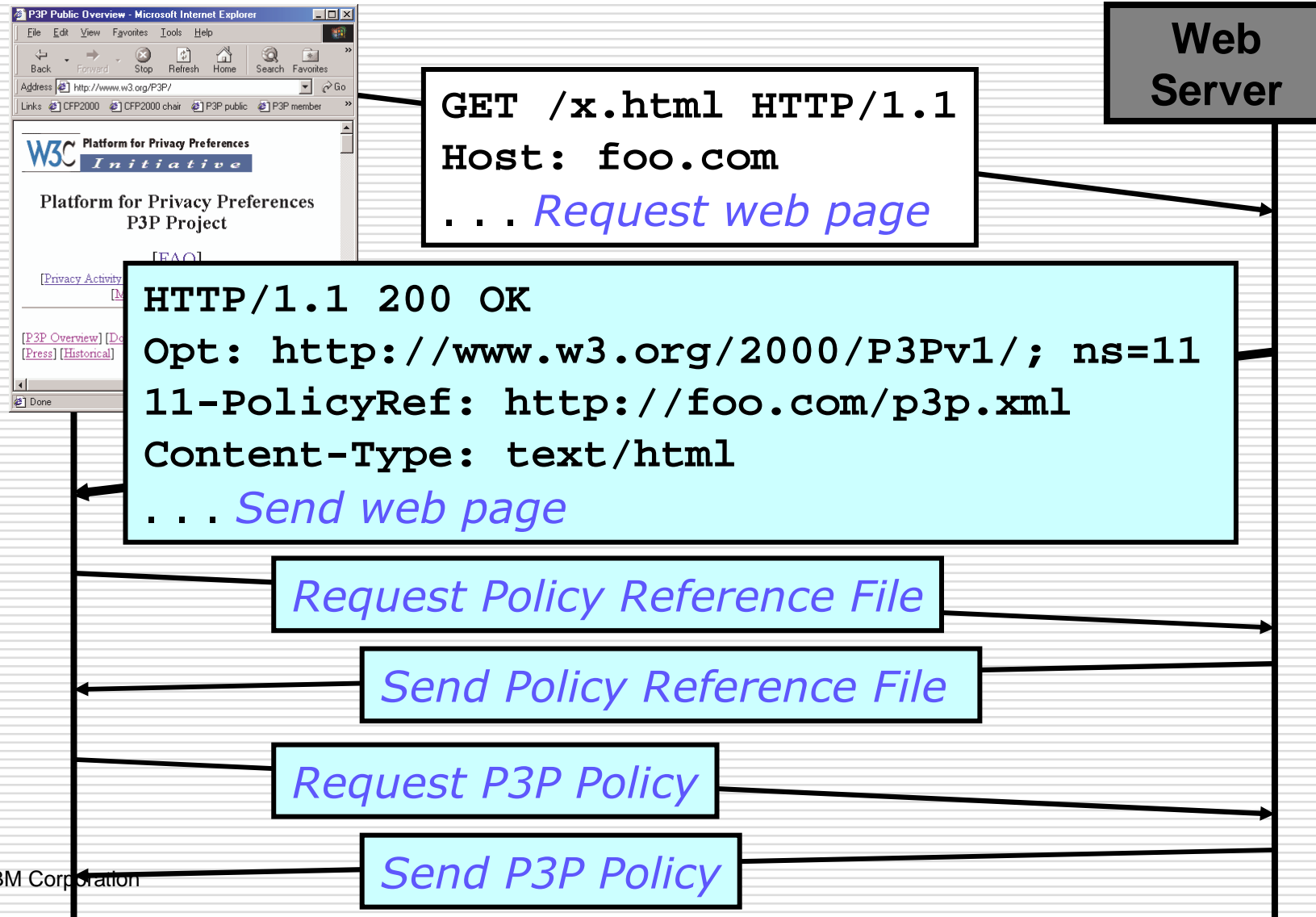
Custom Schema Example

```
<POLICY>
  [...]
  <!-- Custom data elements defined by this policy. -->
  <DATASHEMA>
    <DATA-DEF name="example" short-description="Example Data">
      <LONG-DESCRIPTION>Custom data elements by example.com</LONG-DESCRIPTION>
      <CATEGORIES><uniqueid/></CATEGORIES>
    </DATA-DEF>
    <DATA-DEF name="example.registration"
      short-description="Registration information">
      <CATEGORIES><uniqueid/></CATEGORIES>
    </DATA-DEF>
    <DATA-DEF name="example.registration.userid" short-description="User ID">
      <LONG-DESCRIPTION>User ID created by registering
        at our site.</LONG-DESCRIPTION>
      <CATEGORIES><uniqueid/></CATEGORIES>
    </DATA-DEF>
    <DATA-DEF name="example.registration.password" short-description="Password">
      <LONG-DESCRIPTION>Password created by the user
        when registering at our site.</LONG-DESCRIPTION>
      <CATEGORIES><uniqueid/></CATEGORIES>
    </DATA-DEF>
  </DATASHEMA>
  [...]
</POLICY>
```

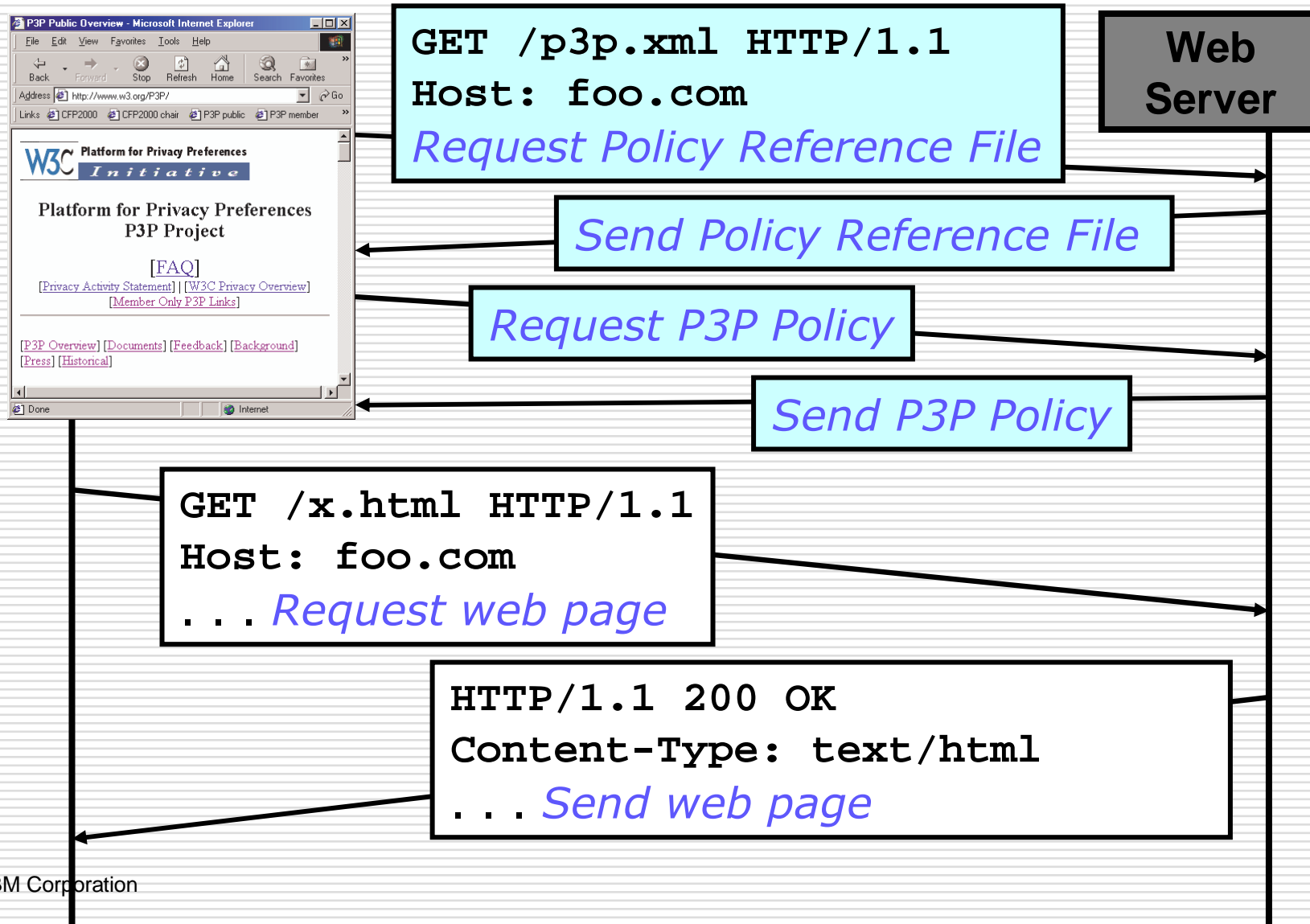
A simple HTTP Transaction



P3P1.0 over HTTP



Or using /p3p.xml File



P3P Prototypes

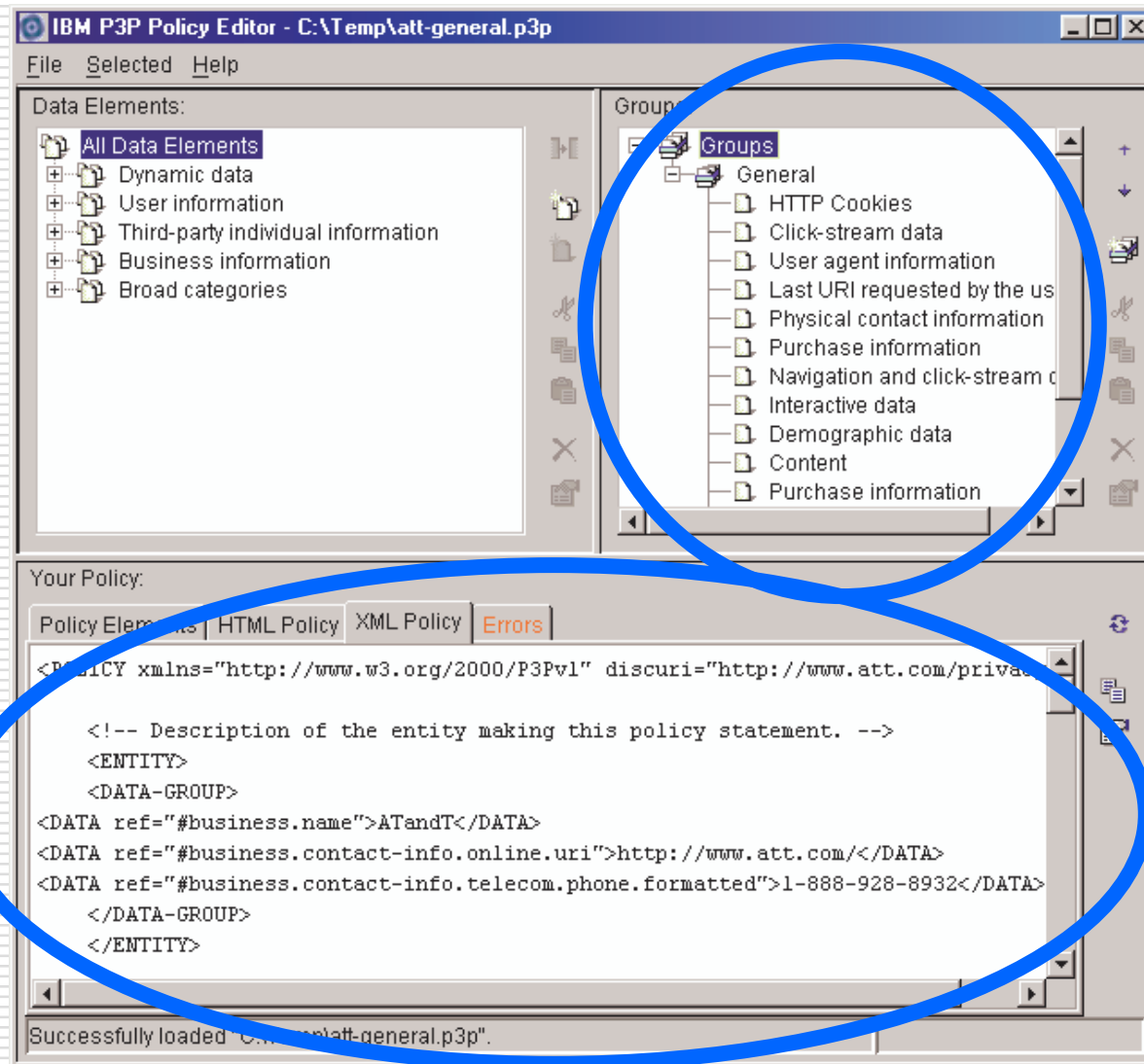
1. P3P User Agents/Proxies
 - [Netscape 7.0](#)
 - [JRC P3P Proxy](#)
 - [AT&T Privacy Bird](#)
 - [Internet Explorer 6.0](#)
2. Server-side P3P Support
 - [IBM Tivoli Privacy Manager for e-business](#)
3. Policy Generators/Editors/Checkers
 - [P3PBuilder](#)
 - [P3P Validator](#)
 - [P3P Policy Editor](#)

AT&T Privacy Bird®

- “Browser helper object” for IE 5.01/5.5/6.0
- Reads P3P policies at all P3P-enabled sites automatically
- Puts bird icon at top of browser window that changes to indicate whether site matches user’s privacy preferences (green – yellow – red)
- Clicking on bird icon gives more information
- Current version is information only – no cookie blocking
- Free download of beta from privacybird.com/; C++ source code distributed under open source license



IBM P3P Policy Editor



Sites can list the types of data they collect

And view the corresponding P3P policy

Project Timeline

- Jul 10, 1997 – W3C P3P kickoff meeting
- 1997-1999 – Many working drafts published
- Oct 28, 1999 – W3C patent analysis published
<http://www.w3.org/TR/P3P-analysis>
- Jun 21, 2000 – P3P “Interop” event, New York
- Dec 15, 2000 – P3P becomes „W3C Candidate Recommendation“
- Required for „Proposed Recommendation“
 - implementations (2 user agents, 2 tools)
 - at least 10 P3P-enabled Web sites
- Mar 22, 2001 – Microsoft introduces IE 6.0 with support for the use of P3P to handle preferences for cookies
- Jan 28, 2002 – P3P becomes „W3C Proposed Recommendation“
- [Apr 16, 2002 - W3C Standard](#)
- Jan 4, 2005 – Public Working Draft of P3P v1.1
- Oct 2007 – work suspended

Open Issues

- primary and secondary data use
- disclosures necessary for compliance with EU Directive
- mismatch between users' and companies' needs
- relationship between P3P statements and human-readable policies

In cases where the P3P vocabulary is not precise enough to describe a Web site's practices, sites should use the vocabulary terms that most closely match their practices and provide further explanation in the CONSEQUENCE field and/or their human-readable policy. However, policies MUST NOT make false or misleading statements.

- policies may be changed/removed
- tracking of privacy violations

Summary: P3P

- P3P defines a [standardized, machine-readable format](#) for privacy policies, along with a [protocol](#) for finding them;
- needs ...
 - no special software on server side
 - P3P-aware client software, tools
 - industry support;
- addresses a relatively narrow conception of privacy, limited to the principles of notice & choice, but does not provide mechanisms for
 - imposing limits on collection & use of data,
 - access enforcement.

Web Sites using P3P: ca. 450 (+430) as of May 2004
www.w3.org/P3P/compliant_sites

Platform for Privacy Preferences Project (P3P)

- Developed by the World Wide Web Consortium (W3C)
 - Final P3P1.0 Recommendation issued 16 April 2002
- Allows web sites to communicate about their privacy policies in a standard computer-readable format
 - Does not require web sites to change their server software
- Enables the development of tools (built into browsers or separate applications) that
 - Summarize privacy policies
 - Compare privacy policies with user preferences
- P3P helps users understand privacy policies
 - P3P increases transparency, but it does not set baseline standards or enforce policies
- P3P user agent software available (as of July 2002)
 - Microsoft Internet Explorer 6
 - Netscape Navigator 7
 - AT&T Privacy Bird
<http://privacybird.com/>
- For more information
 - <http://www.w3.org/P3P/>
 - <http://p3ptoolbox.org/>
 - *Web Privacy with P3P*
by Lorrie Faith Cranor
<http://p3pbook.com/>

References

- "The Platform for Privacy Preferences 1.1 (P3P1.1) Specification." W3C Working Draft, 4-January-2005. <http://www.w3.org/TR/2005/WD-P3P11-20050104/>.
- H. Hochheiser: "The Platform for Privacy Preferences as a Social Protocol: An Examination Within the U.S. Policy Context". ACM Trans. on Internet Technology 2(4) 276-306, Nov. 2002.
- M. Langheinrich: "Internet Privacy and P3P." Tutorial at WWW10 2001. Foils. www.vs.inf.ethz.ch/publ/slides/p3p-www10-0508-export.pdf
- G. Hogben, T. Jackson, and M. Wilikens: "A fully compliant research implementation of the P3P standard for privacy protection: experiences and recommendations." ESORICS 2002, Lecture Notes in Computer Science #2502, Springer. Foils at p3p.jrc.it/presentations/EsoricsPresentation.ppt
- [L.F. Cranor](#): **Web Privacy with P3P**. 2002, O'Reilly
- T. Yu, N. Li, and A.I. Antón: "[A Formal Semantics for P3P](#)". ACM Workshop on Secure Web Services (SWS), October 2004.