Privacy Negotiations with P3P

W3C Privacy Workshop
17.10.2006, Ispra
Sören Preibusch
Overcoming current drawbacks

- static privacy policy
  - one size fits all
  - take it or leave it
  - ex ante

- negotiated privacy contracts
  - individually agreed
  - compensation
  - ad hoc
Existing Privacy Languages

- Privacy Preference Languages
  - APPEL, XPref

- Data Handling Descriptions
  - P3P

- Organizational Guidelines / Rules
  - EPAL
Privacy Negotiations

- Two parties:
  - service provider
  - service user / requestor

- P3P describes data handling at the user/provider interface

- Preference languages support the negotiations
- Rules enforce the negotiated contract
Privacy Negotiations at a glance

– Service Provider and Customers individually negotiate the data handling practices
  • the customer gets a compensation for disclosure, e.g. rebate
  • each possible tuple (data, rebate) is a different contract

– Privacy Dimensions span the Data Space
  • for each dimension, different revelation levels exist
  • revelation thresholds indicate a minimum revelation level
Negotiation design

− Unit of analysis:
  • P3P statement

− Negotiable attributes:
  • Privacy dimensions of a statement

− Integrative negotiations:
  • Offers are alternative statements
Privacy Dimensions in P3P

– P3P top level Privacy Dimensions
  • Recipient
  • Purpose
  • Retention
  • Data

– Non-negotiable P3P elements
  • Consequence
  • meta-information
Extending P3P

– Extending the Policy Reference File (PRF)
  • only compatible browsers find negotiable policies

– Extending P3P Policies
  • multiple alternative statements

– Semantic equivalence
  • between one negotiable policy and multiple standard policies
  • backward compatibility
The new P3P elements

- Two elements added as extensions
  - NEGOTIATION-GROUP-DEF
  - NEGOTIATION-GROUP

- Comparable to the existing tandem
  - STATEMENT-GROUP-DEF
  - STATEMENT-GROUP

- Seamless extension
Negotiable P3P Policy

– NEGOTIATION-GROUP-DEF
  • defines an abstract pool of alternative usage scenarios
    - e.g.: “newsletter format”
  • different statements correspond to different usage alternatives

– NEGOTIATION-GROUP
  • indicates pool membership of a given statement
  • the statement specifies the details of the usage alternative
Example of a negotiable P3P Policy

- **P3P Policy**
  - `NEGOTIATION-GROUP-DEF id="newsletter"`
  - negotiable privacy policy

- **P3P Statement**
  - `NEGOTIATION-GROUP id="newsletter_generic" groupid="newsletter"`
  - negotiation alternatives

- **P3P Statement**
  - `NEGOTIATION-GROUP id="newsletter_personalized" groupid="newsletter"`
Example of a negotiable P3P Policy

```xml
<POLICY> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP-DEF id="newsletter" standard="newsletter_personalized"
    fallback="newsletter_generic" selected="newsletter_personalized" />
<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_generic" groupid="newsletter"
    serviceuri="/services/newsletter/unpersonalized" benefits="You get a standard newsletter and no personal data is collected." />
<DATA-GROUP> <DATA ref="#user.home-info.online.email"/>
</DATA-GROUP>
</STATEMENT>

<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_personalized" groupid="newsletter"
    serviceuri="/services/newsletter/personalized" benefits="You get a personalized newsletter, promoting only the products you are interested in." />
<DATA-GROUP>
    <DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata">
    <CATEGORIES><preference/></CATEGORIES>
</DATA></DATA-GROUP>
</STATEMENT>
</STATEMENT>
</STATEMENT> </EXTENSION /> </STATEMENT>
</EXTENSION> </STATEMENT>
</STATEMENT>
</POLICY>
```
Example of a negotiable P3P Policy

```xml
<POLICY> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP-DEF id="newsletter" standard="newsletter_personalized"
  fallback="newsletter_generic" selected="newsletter_personalized" />
</EXTENSION>

<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_generic" groupid="newsletter"
  serviceuri="/services/newsletter/unpersonalized" benefits="You get a standard
  newsletter and no personal data is collected." />
</EXTENSION>

<DATA-GROUP> <DATA ref="#user.home-info.online.email"/>
</DATA-GROUP>
</STATEMENT>

<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_personalized" groupid="newsletter"
  serviceuri="/services/newsletter/personalized" benefits="You get a personalized
  newsletter, promoting only the products you are interested in." />
</EXTENSION>

<DATA-GROUP>
  <DATA ref="#user.home-info.online.email"/>
  <DATA ref="#dynamic.miscdata" CATEGORIES><preference/></CATEGORIES>
</DATA-GROUP>
</STATEMENT>
</POLICY>
```
Example of a negotiable P3P Policy

```xml
<POLICY> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP-DEF id="newsletter" standard="newsletter_personalized"
  fallback="newsletter_generic" selected="newsletter_personalized" />
<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_generic" groupid="newsletter"
  serviceuri="/services/newsletter/unpersonalized" benefits="You get a standard newsletter and no personal data is collected." />
<DATA-GROUP> <DATA ref="#user.home-info.online.email"/>
</DATA-GROUP>
</STATEMENT>

<STATEMENT> <EXTENSION optional="no">
<PRINT:NEGOTIATION-GROUP id="newsletter_personalized" groupid="newsletter"
  serviceuri="/services/newsletter/personalized" benefits="You get a personalized newsletter, promoting only the products you are interested in." />
<DATA-GROUP>
  <DATA ref="#user.home-info.online.email"/>
  <DATA ref="#dynamic.miscdata">
  <CATEGORIES><preference/></CATEGORIES>
  </DATA>
</DATA-GROUP>
</STATEMENT>
</EXTENSION>
</POLICY>
```
Design Principles

– lightweight extension

– no policy-exchange protocol but acknowledgement by URI-retrieval

– full backward compatibility

– negotiations can be realized in “safe zone”
Presenting all alternatives at once

- P3P principle: “choice and control”
- informed consent based on all alternatives
- facilitate negotiation support systems
- secret policies may be overt by repeated transactions
- economic considerations
Another application: substitutive data types
Another application: substitutive data types

office address

home address

CZS
C
0

0  C  CZS
Another application: substitutive data types

Diagram showing a grid with axes labeled 'office address' and 'home address'. The grid contains points labeled 'R1', 'R2', 'C', and '0'.
Another application: substitutive data types

- R₁: Identity concerned
- R₂: Marginally concerned
- R₁: Profile averse
Status and Future Work

– XML schema definitions available
  • for extended Policy Reference File and P3P Policies
  • XSLT for backward transformation
  • example files

– sound economic background

– software support
  • browser integration
  • authoring tools and deployment tools

– experiments on user behaviour
Thank you!

– Sören Preibusch

German Institute for Economic Research (DIW Berlin)
Königin-Luise-Str. 5
14195 Berlin, Germany
spreibusch@diw.de