DIW Berlin

German Institute
for Economic Research

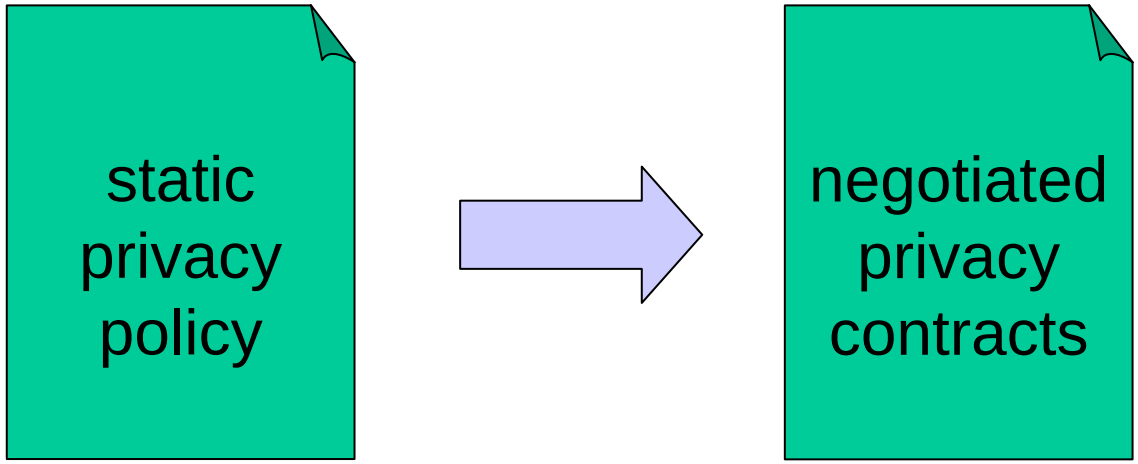
www.diw.de

Privacy Negotiations with P3P

W3C Privacy Workshop
17.10.2006, Ispra

Sören Preibusch

Overcoming current drawbacks



one size fits all

take it or leave it

ex ante

individually agreed

compensation

ad hoc

Existing Privacy Languages

- Privacy Preference Languages
  - APPEL, XPref

  User
- Data Handling Descriptions
  - P3P

  User / Provider
- Organizational Guidelines / Rules
  - EPAL

  Provider

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

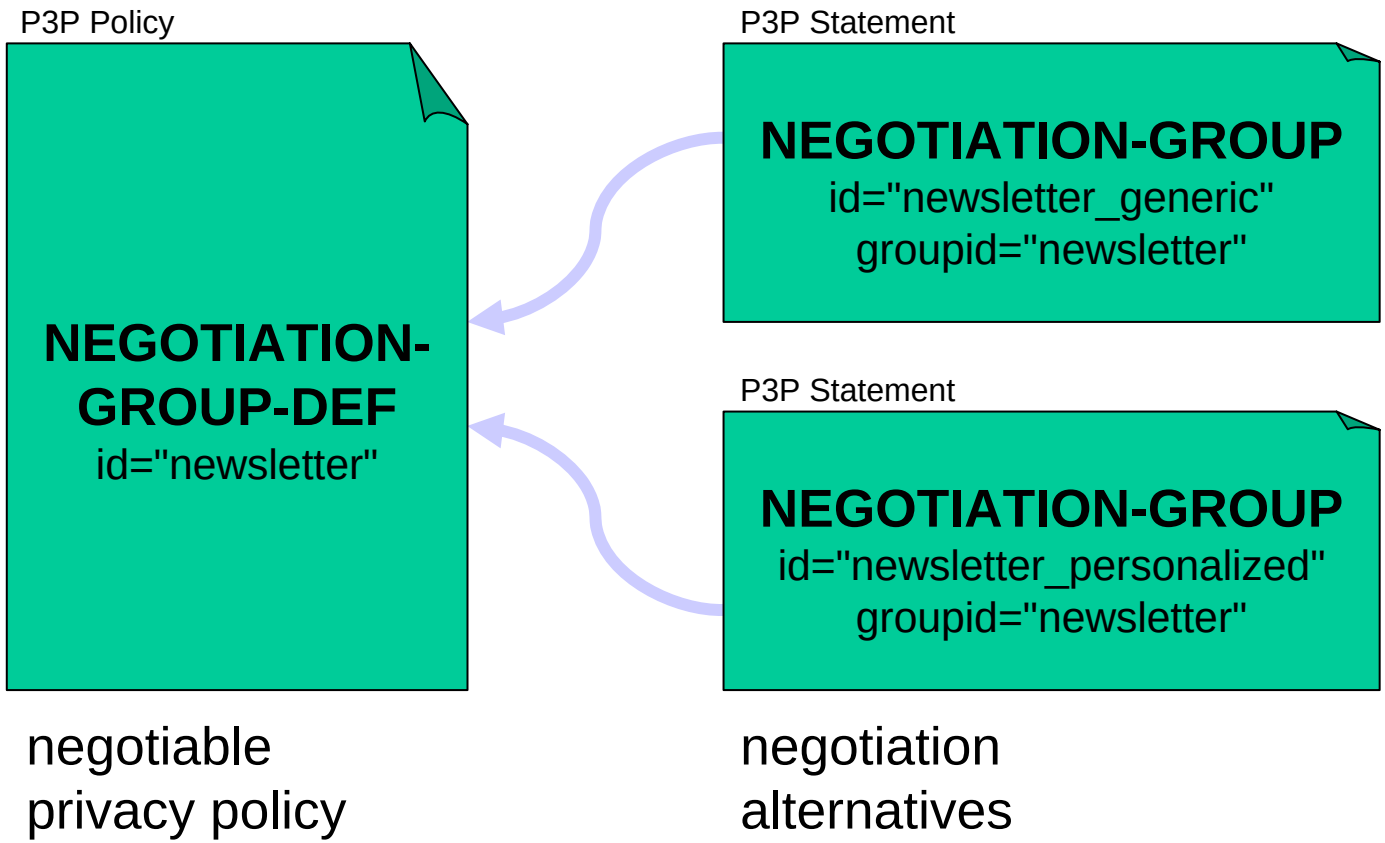
- Two elements added as extensions
  - NEGOTIATION-GROUP-DEF
  - NEGOTIATION-GROUP
- Comparable to the existing tandem
  - STATEMENT-GROUP-DEF
  - STATEMENT-GROUP
- Seamless extension

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



Example of a negotiable P3P Policy

<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></DATA-GROUP>
</STATEMENT> </POLICY>

Example of a negotiable P3P Policy

<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></DATA-GROUP>
</STATEMENT> </POLICY>

Example of a negotiable P3P Policy

<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></DATA-GROUP>
</STATEMENT> </POLICY>

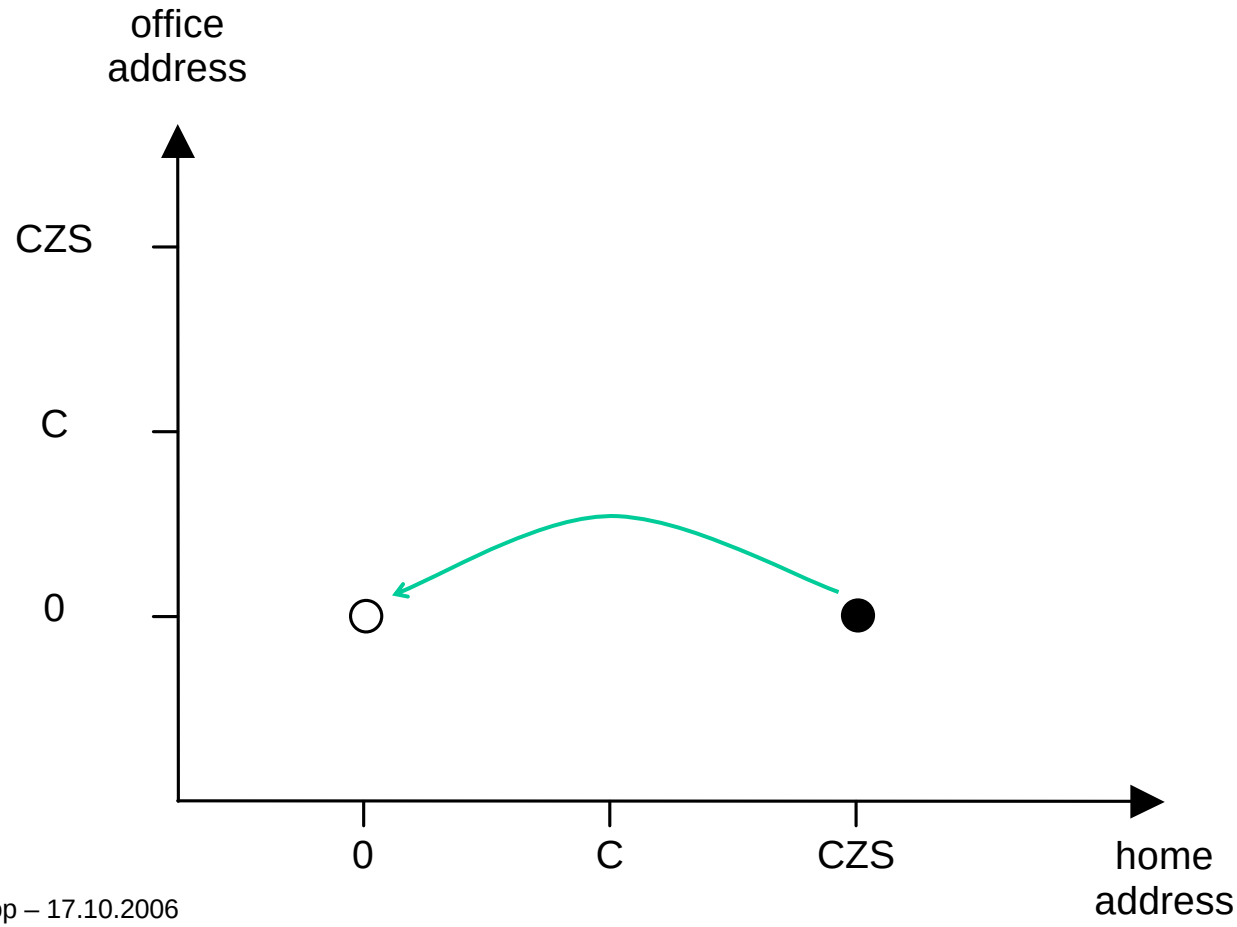
Design Principles

- lightweight extension
- no policy-exchange protocol
  but acknowledgement by URI-retrieval
- full backward compatibility
- negotiations can be realized in “safe zone”

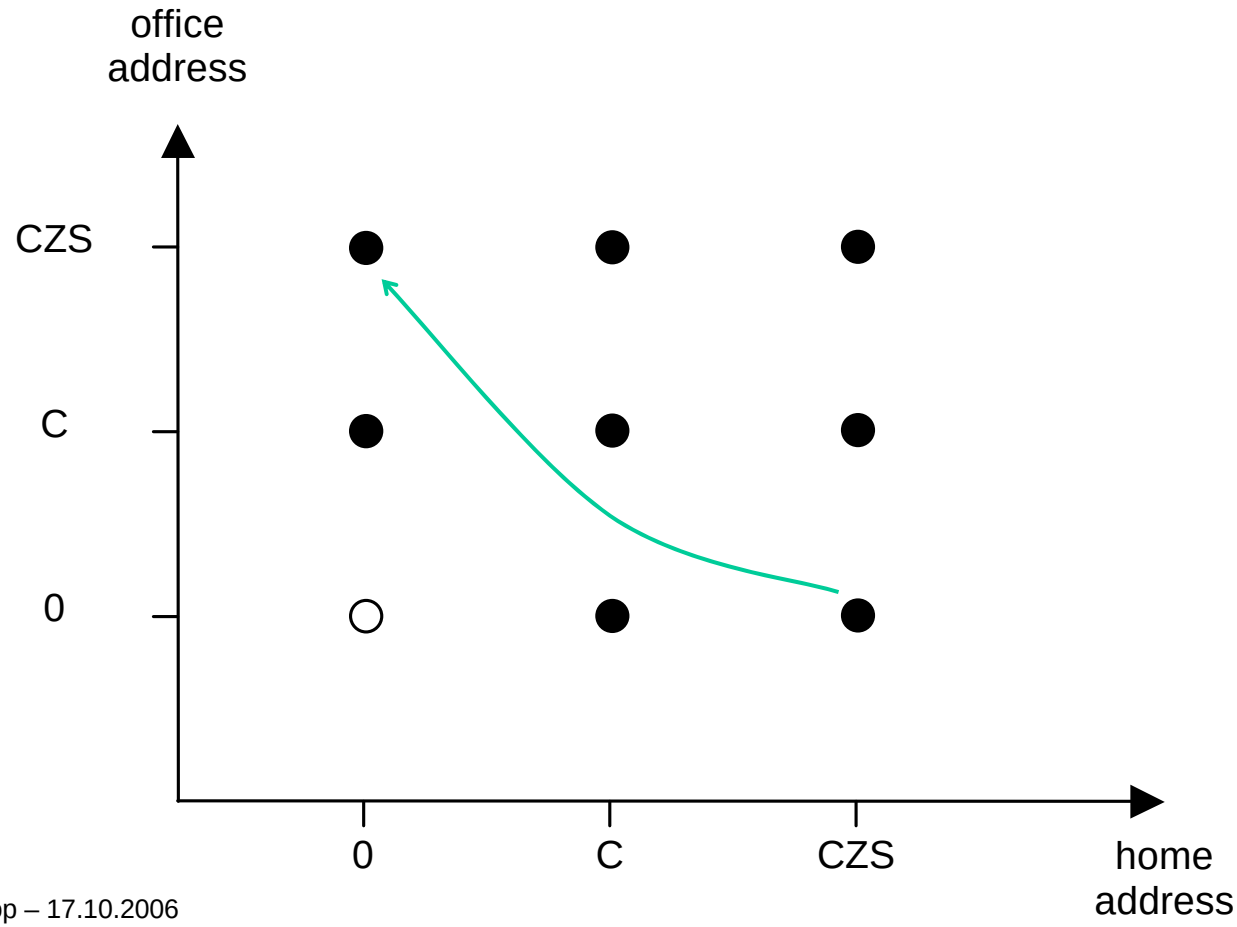
Presenting all alternatives at once

- 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

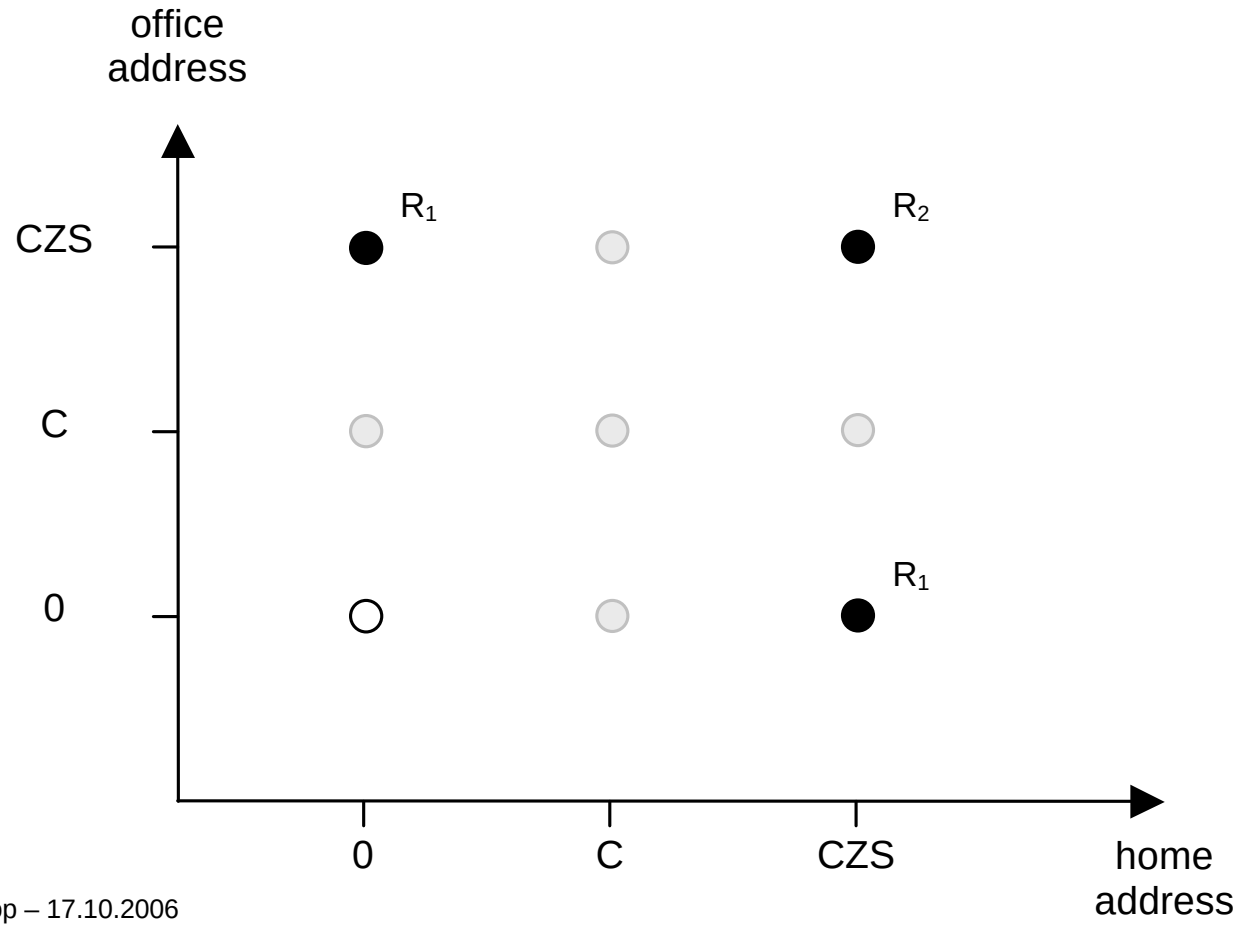
Another application: substitutive data types



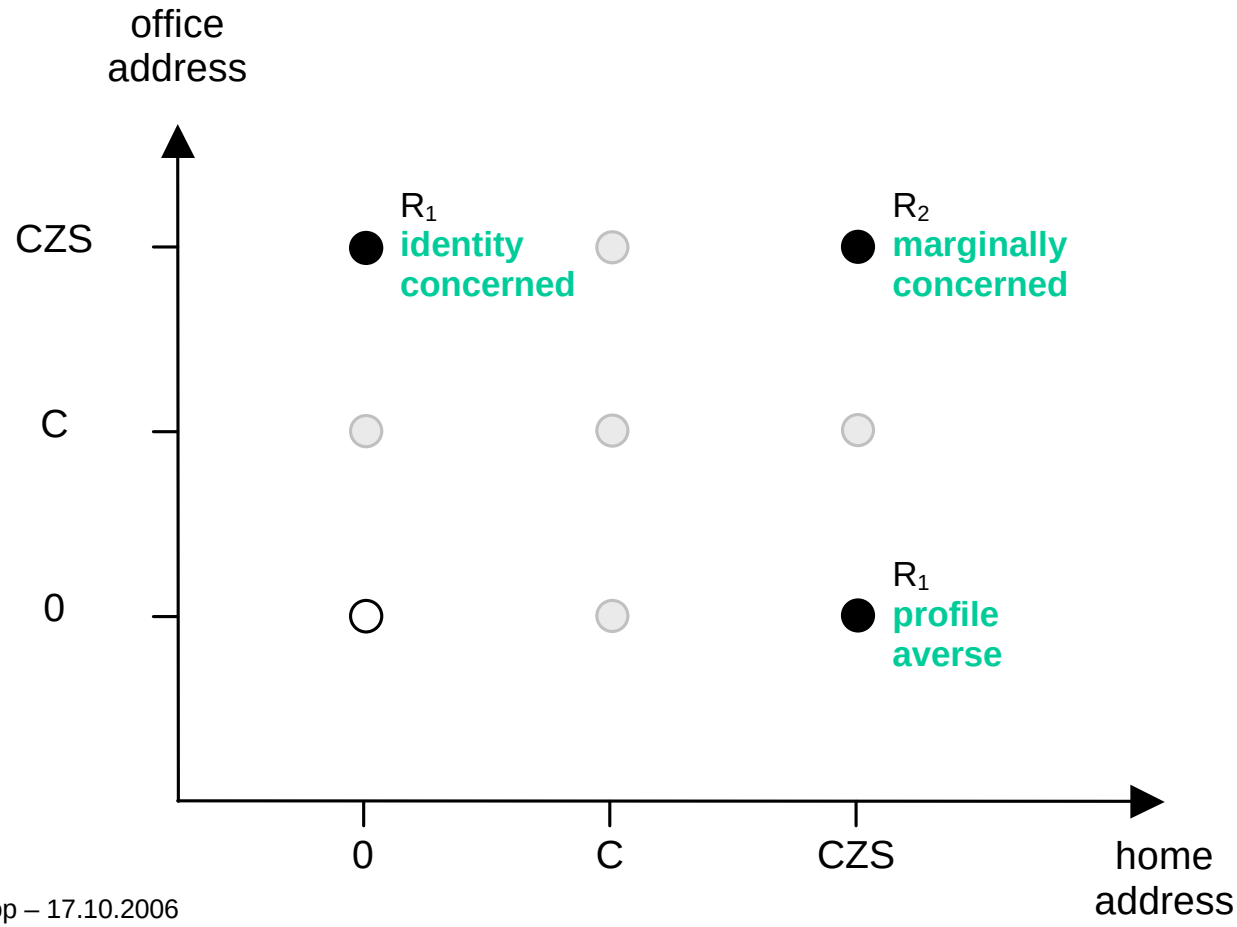
Another application: substitutive data types



Another application: substitutive data types



Another application: substitutive data types



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