NEPP: Negotiation Enhancements for Privacy Policies

Maaser, Michael; Ortmann, Steffen; Langendoerfer, Peter

IHP
Im Technologiepark 25
15236 Frankfurt (Oder)
Germany
Outline

• Motivation

• Negotiation scope

• Negotiation Strategies

• Conclusion
Motivation

• Privacy statements are static described in prose or as P3P policy

• Set out by service providers / data collectors

• Acceptance or disuse of the connected service
  Hardly choices, no means to object

• Does not completely meet the privacy requirements of all users

• Accommodation of both sides

• Increasing acceptance of online offers
  30% of all online purchases are not completed due to hesitation of the potential customer to give away personal information
Nature of the negotiation

- No knowledge about the opposite side

- Negotiation similar to bargaining on a bazaar
  Exchange of proposal and counterproposals
  Until agreement or decision not to agree at all
  Decisions for proposals based on preferences and strategy
  Different strategies may result in different consents
  In-deterministic number of negotiation steps

- NOT to compare with negotiations used in networking techniques
  Like SSL negotiation
Initiatory Example of a Navigation Service

• **Service navigating passengers through an airport**
  Needs the passengers location
  Needs remuneration
  May ask for passenger’s name and email to customize the service

• **Privacy aware user of such service**
  Agrees to provide own location for guiding purpose
  Willing to pay for service usage
  Hesitant to give her name respective email address
  Ready to give her email address for a voucher

• **Respective preferences**
  Service: **require** longitude, latitude, accuracy \( \leq 10 \) meter, \( \geq 0.05\)€/min
  **optional** name, email
  User: **allow** for guiding longitude, latitude, \( \leq 0.10\)€/min
  **prohibit** name
  **prohibit** email address unless voucher is granted
Negotiation Scope

- **Extended data item with intervals**
  - Single- or double-bounded
  - I.e. accuracy of position

- **Added special data item denoting the charge for using a service**
  - Semantics similar to data with interval
  - Has dedicated XML-tag
  - Allows complex dimension including currency and charge unit, i.e.
    \(<eur/>\langle perSecond\rangle\)

- **Added rewards, such as**
  - Personalization benefits,
  - Discounts or
  - Similar rewards
Data items with intervals

Service provider preferences

<POLICY>
  <STATEMENT>
    <PURPOSE>
      <guiding/>
    </PURPOSE>
    <RECIPIENT>
      <ours/>
    </RECIPIENT>
  </STATEMENT>
  <DATA-GROUP>
    <DATA ref="#user.location.accuracy">8</DATA>
    <negotiationbase>5</negotiationbase>
    <atmost>10</atmost>
  </DATA-GROUP>
</POLICY>

Client preferences

<POLICY>
  ...
  <STATEMENT>
    <PURPOSE>
      <guiding/>
    </PURPOSE>
    <RECIPIENT>
      <ours/>
    </RECIPIENT>
  </STATEMENT>
  <DATA-GROUP>
    <DATA ref="#user.location.accuracy">8</DATA>
    <negotiationbase>5</negotiationbase>
    <atmost>10</atmost>
  </DATA-GROUP>
</POLICY>
Service provider preferences

<POLICY>
  <STATEMENT>
    <PURPOSE>
      <guiding/>
    </PURPOSE>
    <RECIPIENT>
      <ours/>
    </RECIPIENT>
    <DATA-GROUP>
      <CHARGE>
        <atleast>0,10</atleast>
      </CHARGE>
    </DATA-GROUP>
  </STATEMENT>
  . . .
</POLICY>

Client preferences

<POLICY>
  <STATEMENT>
    <PROHIBITED/>
    <PURPOSE><guiding/></PURPOSE>
    <RECIPIENT><ours/></RECIPIENT>
    <DATA-GROUP>
      <CHARGE>
        <atleast>0,05</atleast>
      </CHARGE>
      <perMinute/>
    </DATA-GROUP>
  </STATEMENT>
  . . .
</POLICY>
Rewards

Service provider preferences

<POLICY>

. . .

<STATEMENT>
  <OPTIONAL/>
  <PURPOSE>
    <guiding/>
  </PURPOSE>
  <RECIPIENT>
    <ours/>
  </RECIPIENT>
  <DATA-GROUP>
    <DATA ref="#user.home-info.online.email"/>
  </DATA-GROUP>
  <REWARDS>
    <VOUCHER>
      <atleast>3</atleast> <eur/>
    </VOUCHER>
  </REWARDS>
</STATEMENT>

<POLICY>

. . .

<STATEMENT>
  <PROHIBITED/>
  <DATA-GROUP>
    <DATA ref="#user.home-info.online.email"/>
  </DATA-GROUP>
  <REWARDS>
    <VOUCHER>
      <atmost>5</atmost> <eur/>
    </VOUCHER>
  </REWARDS>
</STATEMENT>

</POLICY>

Client preferences

<POLICY>

. . .

<STATEMENT>
  <PURPOSE>
    <guiding/>
  </PURPOSE>
  <RECIPIENT>
    <ours/>
  </RECIPIENT>
  <DATA-GROUP>
    <DATA ref="#user.home-info.online.email"/>
  </DATA-GROUP>
  <REWARDS>
    <VOUCHER>
      <atleast>3</atleast> <eur/>
    </VOUCHER>
  </REWARDS>
</STATEMENT>

. . .
Negotiation Scope

• Extension of service side preferences
  Differentiation of required and optional statements

• Extension of client side preferences
  Prohibitions and Permissions

• Permissions allow
  Any of the stated data items
  Implicitly prohibiting everything else

• Prohibitions prohibit
  The combination of the stated data items
  Implicitly permitting everything else
Explaining the difference of Permission and Prohibition (Example)

- Prevention of data misuse on eBay accounts
  - The permission allows to release the user’s name, her postal address or her birth date respectively.
  - It further prohibits every other data like i.e. credit card or social security number.
  - The prohibition however prohibits to release the named data items at a time.

- A proposal requesting
  - only the user’s name and her postal address can be accepted
  - only the user’s name and her birth date can be accepted
  - the user’s name and her credit card number cannot be accepted
  - the user’s name and her postal address along with her birth date cannot be accepted

```xml
<POLICY>
  <STATEMENT>
    <ALLOWED/>
    <PURPOSE>
      <interest/>
    </PURPOSE>
    <RECIPIENT>
      <ours/>
    </RECIPIENT>
    <DATA-GROUP>
      <DATA ref='#user.name'/>
      <DATA ref='#user.home-info.postal'/>
      <DATA ref='#user.bdate'/>
    </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
    <PROHIBITED/>
    <DATA-GROUP>
      <DATA ref='#user.name'/>
      <DATA ref='#user.home-info.postal'/>
      <DATA ref='#user.bdate'/>
    </DATA-GROUP>
  </STATEMENT>
</POLICY>
```
Negotiation Strategies

- Service and User Preferences each span a negotiation space
- The solution space is the intersection of both negotiation spaces
- Neither party has knowledge of the opposite preferences
- Solution space cannot actually be determined by any party
- Outcome of the negotiation is an element of this solution space
- Element depends on the strategies used by the negotiation parties
- It may occur that no such element is found even if the solution space is not empty
Negotiation Strategies

- Implemented Simple Service Strategy proposes 5x the minimal charge (0.50 Euro)

- Implemented Simple Client Strategy chooses the edge of the own prohibited interval while proposal is above the limit (0.20 Euro)

- Simple Service Strategy accepts

- Outcome of the negotiation is 0.20 Euro
Negotiation Strategies

- Another possible Service Strategy proposes 4x the minimal charge (0.40 Euro)
- Some Client Strategy may choose its own negotiation base to counter propose (0.05 Euro)
- Service Strategy may counter propose 0.30 Euro
- Client Strategy may accommodate with a proposal of 0.10 Euro
- Service Strategy may accept now or try to push this further with 0.20 Euro
- Whereas the client strategy may accept now or again respond with 0.15 Euro
- Both may finally accept 0.15 Euro
Conclusion

• Identified need for dynamic privacy statements

• P3P extended with tags to describe negotiation scope

• Algorithm exists to decide on acceptability of proposal

• Counterproposals are generated by exchangeable strategies

• Implementation, proven to be functional
  Runs on PC and PDA
  Downward compatible to static P3P 1.0 on server
  Downward compatible to P3P tool Privacy-Bird on client
  Offline demonstration possible
Discussion

Thanks for your attention.
Any questions?