Privacy Negotiations with P3P

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

ABSTRACT
This paper examines how negotiation techniques can resolve the trade-off between service providers' personalization efforts and users' individual privacy concerns and demonstrates how they can be integrated into existing technologies to overcome the shortcomings of static privacy policies. The analysis includes the identification of relevant and negotiable privacy dimensions. An extension to P3P is proposed that allows a simple expression and implementation of negotiation processes. Support for this extension has been developed for the Mozilla Web browser.

INTRODUCTION
The Web's complexity both in size and diversity has led online retailers to offer their customers individually targeted products and services. Personalization efforts have been implemented in the vast majority of popular sites. Their inherent need for personal information and the long-time storage of these data drew attention to the induced privacy issues. Still, the Privacy-Personalization trade-off is only one example for increased awareness of privacy issues. Personal identifiable information is collected during almost every Web interaction.

The obvious need for better communication of the data handling procedures in place gave rise to several technical approaches both in research and in practice – with notable involvement of W3C's Platform for Privacy Preferences (P3P) initiative. These technologies can be classified according to the market structure and the targeted transaction phase, while abstracting from further explanation in the light of this Workshop's expert audience: (a) Service providers publish P3P Policies that are retrieved by a user agent (UA) acting on the user's behalf. (b) The UA checks if the P3P Policy is compatible with the user's privacy preferences. Latter can be coded using the privacy preference languages APPEL [18] or XPref [2]. (c) Intra- and inter-organizational guidelines governing the handling of collected data can be expressed using EPAL [6].

The depicted set of existing privacy languages are evidence that the design of privacy technologies has extent beyond user-facing front-ends. Yet, the initially agreed upon privacy policy between a service provider and its customers (whether this policy is textual or a P3P privacy policy) will govern all subsequent data flows. Yet these privacy policies are usually static and all customers are offered the same privacy settings regardless their individual privacy preferences. A privacy-focused "meta-personalization" does not take place.[1]

Posting "privacy policies" on websites is a rigid approach and hampers users providing an informed consent as the compensation for data disclosure is not apparent. The empirical proof of users' stated privacy preferences diverging from their actual behaviour is a symptom of this burden [14].

Our contribution is to depict how negotiation techniques can overcome current drawbacks of static privacy policies, and reconcile privacy and personalization. We investigate how negotiations can be implemented using existing technologies, namely P3P.

The implementation of PRINT by extending W3C's Platform for Privacy Preferences (P3P) is soundly explained and detailed information is provided how language support for PRINT can be integrated in P3P in a straightforward way.

RELATED WORK: EXISTING PRIVACY LANGUAGES
P3P is an XML-based language developed by the World Wide Web Consortium (W3C) [21]. It became a recommendation in 2002 and aims "to inform Web users about the data-collection practices of Web sites" [22]. P3P has become widely adopted by service providers but it remains restricted to the "take-it-or-leave-it" principle: The service provider offers a privacy policy; the potential customer has to accept as a whole if she wants to use the service. A negotiation process between the involved parties is not intended. Although the first drafts of the P3P specification included multi-round negotiation mechanisms, these parts had been removed in favour of easy implementation and early and wide adoption of the protocol. The latest version of the P3P 1.1 specification [22] does not mention negotiations either. Still, a reintroduction has been discussed at the P3P Workshop in Kiel (2003) [19] and is planned for future versions of P3P [20].

The relevance and suitability of APPEL and XPref along with the role of the Enterprise Privacy Authorization Language (EPAL) have been developed in [9]. In summary, privacy preference languages are improper to implement

[1] Meta-personalization describes personalization of the means and methods being used for the actual offerings' personalization

PRINT. However, privacy preferences formulated in these languages can be used for negotiation support systems. EPAL does not target the customer interface – where the negotiation takes place. However literature discusses mapping P3P policies (potentially reached by negotiation) to EPAL policies to govern internal data processing procedures. The tight link between negotiation and enforcement becomes obvious as enforcing individually concluded privacy policies – for instance by sticky policies – is challenging.

Negotiations are studied in various disciplines. The bases had been set up in game theory, where negotiation is modelled as a bargaining game [7], [15]. Recent influences have arisen with the increasing importance of autonomous agents and collaborative computing [5]. Frameworks for carrying out negotiations have been developed [12].

PRIVACY NEGOTIATIONS

Thompson defines negotiations as an "interpersonal decision-making process necessary whenever we cannot achieve our objectives single-handedly" [16]. Especially in the case of integrative negotiations, negotiations can unleash the integrative potential that lies in conflicting interests and preferences and turn it into efficient contracts. Two major shortcomings of current online privacy handling mechanisms can be overcome if PRINTs are implemented during the transaction between the service provider and the user:

The first shortcoming is the "one-size-fits-all" principle: once the service provider has designed its privacy policy, it will be proposed to all interested users – no matter what their individual preferences are. There may be users who would have accepted offers with less privacy protection and would have agreed to the provider's proposal even if more personal data would have been asked. Thus, the provider fails to tap the users' full potential.

The second shortcoming is the "take-it-or-leave-it" principle, i.e. the user can only accept or refuse the provider's proposal as a whole. The provider is always the one who moves first, he makes the initial offer; the user cannot take the initiative.

The economical model of privacy negotiations is omitted from this Position Paper. However, we cordially reference the interested reader to [9]: The user's individual utility calculus is developed within a microeconomic model, taking into account different overall sensitivity levels towards privacy and different importance one may assign to a specific privacy dimension. The user's optimal choices are formally deduced subject to participation constraints. Using backward induction methods, the service provider can design an incentive-compatible privacy negotiation: as the provider cannot distinguish anonymous users whose privacy preferences are private information, a negotiation scheme leading to self-selection is crafted. Negotiable privacy dimensions, revelation levels and thresholds and the compensation structure are conceived [10], [11].

Negotiable Privacy Dimensions

Apparently, as it is not feasible to negotiate the entire privacy policy, one important aspect is to identify relevant and negotiable privacy dimensions. We define a *privacy dimension* as one facet of the multi-dimensional concept 'user privacy'. For each dimension, different discrete revelation levels exist, monotonously associated with the user's willingness to reveal the data. Privacy dimensions can be identified at different degrees of granularity [8].

The four top-level privacy dimensions are the recipient of the data, the purpose for which the data are collected, the period they will be stored, and the kind of data. These four dimensions (recipient, purpose, retention time, and data) correspond to the constituting elements of a P3P privacy policy `STATEMENT`.

It is obvious, that the importance of each of the four dimensions as perceived by the users as well as their respective willingness to provide information depends on the thematic domain of the service. Some recent work proposed to negotiate the recipient of the data in different application scenarios, among them are medical help [23], distance education [24], and online retailing [5]. We will focus on negotiating the amount of data to be revealed. The drill-down of privacy dimensions to lower levels is obvious for the data dimension, following the P3P base data scheme [22].

Negotiating the 'data'-Dimension

While the recipient may be the relevant negotiation dimension for distance education or health services, we propose the extent and amount of shared data as negotiation dimension for online retailing. First, the willingness of customers to provide personal information is mainly determined by the service provider's reputation, who is the (nonnegotiable) initial recipient of the data. Second, disclosure practices are often determined business processes (e.g. outsourced billing services or delivery by third-party companies). Third, the relevance of the retention time is rated considerably less important [1]. Finally, all data carries with it a more or less pronounced intrinsic purpose that cannot be subject to a negotiation (e.g. phone numbers are used for personal contact and telemarketing). In P3P, this intended use is expressed via the `CATEGORIES` element. Hence, negotiating the kind of data seems appropriate in the case of online retailing.

Generally spoken, for a type of data to become part of the negotiation process, it must at least meet the following criteria:

- the user must be able to provide the data
- the data must not be off-topic; the user should see at least a slight reason for the necessity of providing it

- it must not be indispensable for the execution of the contract, either by its nature or by the level of detail (i.e. no negotiations for revelation levels below the revelation threshold)
- the service provider must gain the user's favour for collecting the data, i.e. the data is part of an explicit profile [13]

The empirical findings of [1] allow establishing a cardinal ordering of types of data according to the willingness of user's to provide the information. Ackerman et al. found significant differences in comfort level across the various types of information.

IMPLEMENTATION

Privacy dimensions in P3P

The four top-level privacy dimensions (recipient, purpose, retention time, and data) identified above can be mapped directly to P3P. P3P policies express the service provider's data processing practices using STATEMENTs; each of those statements having child elements indicating the RECIPIENT of the data, the PURPOSE for which the data will be used, the RETENTION time and what kind of DATA will be collected.

Other optional child elements of a privacy statement, such as the CONSEQUENCE element or possible EXTENSIONs may not be included in the negotiation process: the consequence is only a short summary or a human-readable explanation of the data processing practices described in the (rest of the) statement. The user agent is supposed to show contents of this element to a (human) user. As for possible extensions, the semantics of issuer-defined additions may be ambiguous and one cannot presume that issuer-defined extensions will be understood by all user agents.

Integrating Privacy Negotiations into P3P

The negotiation process as described in the previous section can be implemented using the already mentioned extension mechanism of P3P, which can be used both in a policy reference file and in a single privacy policy. The extensions in the privacy policies will not be optional, but in order to ensure backward compatibility, these extended policies will only be referenced in an optional extension of the policy reference file. Hence, only user agents capable of interpreting the negotiation extension will fetch extended policies.

In a P3P policy, two extensions can be added: a NEGOTIATION-GROUP-DEF in the POLICY element, and a NEGOTIATION-GROUP in the STATEMENT element. The mechanism is comparable to the tandem of STATEMENT-GROUP-DEF and STATEMENT-GROUP in P3P 1.1 [22].

The STATEMENT-GROUP-DEF extension is used to define an identifier and optionally properties that can be applied to a group of STATEMENT elements using the STATEMENT-GROUP extension. A statement group allows service providers to describe what sections of their P3P policy apply to different user interactions with their site/service. A statement can be associated with a statement group by having at most one STATEMENT-GROUP extension. A STATEMENT-GROUP element can carry at most two attributes: The id-attribute associates a STATEMENT with a certain group of STATEMENTs to cluster them together. The name-attribute associates a name to a certain statement. User agents may use this name to improve the display of the policy to the user in a human readable format.

A NEGOTIATION-GROUP-DEF element defines an abstract pool of alternative usage scenarios. One or several statements (identified by the attribute id) code a possible usage scenario; the pool membership is expressed by the NEGOTIATION-GROUP extension in the statement (attribute groupid), which describes relevant parameters of the given scenario, such as the benefits for the user. The fallback contract can be indicated via the fallback-attribute of the NEGOTIATION-GROUP-DEF element. The standard-attribute indicates which scenario is offered as default. By means of the selected-attribute, the currently active alternative can be marked, as for persistent storage of a negotiation state or for the final agreement.

The following example illustrates the usage: users of a website can subscribe to a generic or a personalized newsletter (see next page). The generic newsletter will contain only unpersonalized information; the personalized newsletter includes addressing the subscriber per name and promotions targeted towards her interests. Note the additional DATA elements to be collected as well as the additional PURPOSE. The RECIPIENT and the RETENTION time remain unchanged.

Note that the benefits given in human-readable format need to be displayed concisely by the user agent. The example above shows that the human-readable privacy policy and other information resources on the site must work hand in hand with the P3P policy. The exhaustive machine-readable coding of the benefits is a remaining challenge – especially for multi-dimensional phenomena other than just a reduced purchase price. ebXML and its sub-standards, e.g. the Core Components Technical Specification by UN/CEFACT by the United Nations Centre for Trade Facilitation and Electronic Business, may be used as the basis for further development [17].

Please also note that the extensions follow the design principles of P3P by abstracting from request-response acknowledgements of the negotiated privacy policy. Instead, as for standard P3P policies, the user confirms the acceptance of the policy by fetching the URI resource to which the policy is associated. The serviceuri-attribute specifies the respective URI. Withal, standard P3P policies may be bound to these URIs for providing backward-compatibility.

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


<STATEMENT>

  <EXTENSION optional="no"> <PRINT:NEGOTIATION-GROUP   id="newsletter_generic"
    groupid="newsletter"  erviceuri="/services/newsletter/unpersonalized"
    description="Generic newsletter with no personalization"
    benefits="You get a standard newsletter and no personal data is collected" /> </EXTENSION>

  <CONSEQUENCE>We use your email address for sending you our newsletter.</CONSEQUENCE>

  <RECIPIENT><ours/></RECIPIENT>
  <PURPOSE><contact/></PURPOSE>
  <RETENTION><stated-purpose/></RETENTION>

  <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"
    description="Personalized newsletter, tailored to your personal preferences"
    benefits="You get a personalized newsletter, promoting only the products you are interested in" /> </EXTENSION>

  <CONSEQUENCE> We use your email address for sending you a newsletter targeted to your interests. </CONSEQUENCE>

  <RECIPIENT><ours/></RECIPIENT>
  <PURPOSE><contact/><individual-decision/></PURPOSE>
  <RETENTION><stated-purpose/></RETENTION>

  <DATA-GROUP>
    <DATA ref="#user.name"/><DATA ref="#user.home-info.online.email"/>
    <DATA ref="#dynamic.miscdata"><CATEGORIES><preference/></CATEGORIES></DATA>
  </DATA-GROUP>  </STATEMENT>  </POLICY>
```

Listing 1. Example of an extended P3P policy, including the proposed elements `NEGOTIATION-GROUP-DEF` and `NEGOTIATION-GROUP` (fragment)

Additional Examples

Additional case-studies on how privacy negotiations can be coded have been developed for instance for negotiating user identifiers in multi-channel retailing [9] and for delivery details of physical and digital goods [14]. The insightful application of the PRINT concepts to existing Customer Relationship Management in the telecommunication industry and the relevance of Privacy Negotiations in the context of an integrated data processing strategy is presented in [11].

User Agent Support

We have integrated basic negotiation support into the Mozilla Web browser, thence extending its P3P support: a site's privacy policy can be accessed via the "Policy", "Summary" and "Options" buttons in the "Page Info" dialog, directly available from the status bar [9]. As the proposed extension to P3P is not restricted to a specific privacy dimensions, neither is the implementation. Any privacy dimension can be negotiated as long it can be expressed using the P3P data scheme.

Negotiable P3P privacy policies can be checked against the XML Schema Definition for the portrayed extensions (cf. next section).

Moreover, a XSLT file for translating the alternatives coded in a negotiable P3P privacy policy into a set of alternative standard P3P policies is available. Thus, service providers may generate backward compatible P3P policies for each usage scenario of their web resources.

Reference Documents

The XML Schema Definition for the proposed extensions is available at the following URIs (along with full example files):

- `http://preibusch.de/namespaces/PRINT/PRINT_PRF.xsd` for the Policy Reference File (`namespaces/PRINT/examples/PRF.xml`)
- `http://preibusch.de/namespaces/PRINT/PRINT.xsd` for the Privacy Policy (`namespaces/PRINT/examples/newsletter_negotiable.xml`)
- `http://preibusch.de/namespaces/PRINT/PRINT2.xsd` for an alternative specification for the Privacy Policy (`namespaces/PRINT/examples/newsletter_negotiable2.xml`)

CONCLUSION AND FURTHER WORK

This Position Paper has presented the advantages of a negotiation about privacy principles in a relationship between service provider and customer. Negotiating allows a better matching between the seller's needs and the buyer's disclosure restraint and helps to reduce the trade-off between personalization and privacy. With the extension mechanism of P3P, there is no limitation in coding web resource usage alternative even for complex cases involving diverse privacy dimensions: We proposed two new

elements that follow the structure of the current P3P 1.1 grouping mechanisms and allow software-supported negotiations in E-Commerce.

Future work will focus on the practical implementation of privacy negotiation techniques on large scale public websites. We are currently investigating which user interface design best fulfils the usability requirements and how negotiable privacy dimensions are best visualized. Moreover, a taxonomy should be developed to allow a machine-readable coding of the user's benefits for a negotiation alternative. A remaining question is whether users feel more concerned about their privacy when an explicit negotiation process is started. This increasing sensitivity could make take-it-or-leave-it offers more favourable for the service provider.

REFERENCES

1. Ackerman, M. S., Cranor, L.F., Reagle, J.: Privacy in E-commerce: Examining User Scenarios and Privacy Preferences, First ACM Conference on Electronic Commerce, Denver, CO (1999) 1-8
2. Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y. An XPath-based preference language for P3P. In Proceedings of the Twelfth International Conference on World Wide Web, pages 629–639. ACM Press (2003)
3. Buffett, S., Jia, K., Liu, S., Spencer, B., Wang, F.: Negotiating Exchanges of P3P-Labeled Information for Compensation, Computational Intelligence, Volume 20, Number 4 (2004)
4. Cranor, L. F., Resnick, P.: Protocols for Automated Negotiations with Buyer Anonymity and Seller Reputation, Netnomics,. 2(1), 1-23 (2000)
5. El-Khatib, K.: A Privacy Negotiation Protocol for Web Services. Proceedings of the International Workshop on Collaboration Agents: Autonomous Agents for Collaborative Environments (COLA) (2003)
6. International Business Machines Corporation, Calvin Powers, Matthias Schunter (Editors): Enterprise Privacy Authorization Language (EPAL 1.2), W3C Member Submission 10 November 2003 (2003)
7. Karrass, C. L.: Give and Take: The Complete Guide to Negotiating Strategies and Tactics. HarperCollins Publishers, New York, NY (1993)
8. Preibusch, S., Implementing Privacy Negotiations in E-Commerce. in: Frontiers of WWW Research and Development - APWeb 2006: 8th Asia-Pacific Web Conference (APWeb 2006), Harbin, China. LNCS 3841, 604-615 (2006)
9. Preibusch, S., Personalized Services with Negotiable Privacy Policies.CHI 2006 Workshop on Privacy-Enhanced Personalization (PEP06), Montréal / Canada, 29-38 (2006)
10. Preibusch, S., Designing Incentive-Compatible Privacy Negotiations. ETRICS 2006, Workshop: Security and Privacy in Future Business Services, Freiburg / Germany (2006)
11. Preibusch, S., Privacy Negotiations enhance Data Collection for CRM. CollECTeR Europe 2006, Basel / Switzerland, 11-20 (2006)
12. Rebstock, M., Thun, P., Tafreschi, O.A.: Supporting Interactive Multi-Attribute Electronic Negotiations with ebXML. Group Decision and Negotiation. 12 (2003) 269–286
13. Schubert, P.: Virtual Virtuelle Transaktionsgemeinschaften im Electronic Commerce, Josef Eul Verlag, Lohmar, Köln (1999)
14. Spiekermann, S., Grossklags, J., Berendt, B.. E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. in EC'01: Third ACM Conference on Electronic Commerce. Tampa, FL, 38-47 (2001)
15. Ståhl, I.: Bargaining Theory. Stockholm: The Economics Research Institute (1972)
16. Thompson, L.L.: The Mind and Heart of the Negotiator. 3rd edn. Pearson Prentice Hall, Upper Saddle River, New Jersey (2005)
17. United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT): Core Components Technical Specification – Part 8 of the ebXML Framework, Version 2.01 (2003)
18. W3C, A P3P Preference Exchange Language 1.0 (APPEL1.0), W3C Working Draft 15 April 2002, http://www.w3.org/TR/P3P-preferences (2002)
19. W3C, Minutes of the P3P 2.0 Workshop, 2003, http://www.w3.org/2003/p3p-ws/minutes.html
20. W3C, P3P – Future Versions of P3P (2005) (Presentation, slide 10), http://www.w3.org/Consortium/Offices/Presentations/P3P/Overview.html#(10)
21. W3C, The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P/ (2002)
22. W3C, The Platform for Privacy Preferences 1.1 (P3P1.1) Specification", W3C Working Draft 10 February 2006, http://www.w3.org/TR/2006/WD-P3P11-20060210/ (2006)
23. Yee, G., Korba, L.: Feature Interactions in Policy-Driven Privacy Management. Proceedings from the Seventh International Workshop on Feature Interactions in Telecommunications and Software Systems (FIW'03) (2003)
24. Yee, G., Korba, L.: The Negotiation of Privacy Policies in Distance Education. Proceedings. 4th International IRMA Conference (2003)