Implementing Privacy Negotiation Techniques in E-Commerce

Sören Preibusch
German Institute for Economic Research
Königin-Luise-Str. 5, 14191 Berlin, Germany
spreibusch@diw.de

Abstract

This paper examines how service providers may resolve the trade-off between their personalization efforts and users' individual privacy concerns through negotiations. The analysis includes the identification of relevant and negotiable privacy dimensions for different usage domains. Based on a formalization of the user's privacy revelation problem, we model the negotiation process as a Bayesian game where the service provider faces different types of users. Finally an extension to P3P is proposed that allows a simple expression and implementation of negotiation processes.

1. Introduction and Related Work

Online users are facing a large and increasing complexity of the web, due to its size and its diversity. In the domain of online retailing, online stores are constantly expanding their assortment in width, depth and quality levels, which makes it impossible for users to examine all possible alternatives without effective guidance through automated recommender systems. As personalization relies on stored user-related data, privacy issues have to be taken into account.

A common way for websites to express their privacy principles are "privacy policies", expressed in P3P [9] or EPAL [4]. Although the first drafts of the P3P specification included negotiation mechanisms, these parts had been removed in favour of easy implementation and early and wide adoption of the protocol. APPEL1.0 [8], developed in addition to P3P, excludes explicitly the capability to express negotiation strategies from its scope. Using APPEL as a negotiation protocol is neither supported by its semantics nor is the language designed for this purpose.

EPAL allows enterprises to express data handling practices in IT systems [4]. The language focuses on the internal business perspective, and is not intended for customers to express their own privacy preferences. Although EPAL does not target the direct dialogue with the end-user – which is needed for negotiation – privacy guarantees for the customers can sometimes be deduced from the stated internal procedures and then be expressed in P3P.

Parallel to the development of privacy-related technologies and research in IT-based transactions, negotiation has been studied in various disciplines. The bases had been set up in game theory, where negotiation is modelled as a bargaining game [5, 7]. Recent influences have arisen with the increasing importance of autonomous agents and collaborative computing [3].

2. Privacy Negotiations

Implementing privacy negotiation processes during the transaction between the service provider (seller) and the user (buyer) can help to overcome two major shortcomings of current online privacy handling mechanisms: the "take-it-or-leave-it"-principle (the user can only accept or refuse the provider's proposal as a whole and the "one-size-fits-all" principle (the same privacy policy is proposed to all interested users).

2.1. Negotiable Privacy Dimensions

As it is not feasible to negotiate about 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 revelation levels exist, monotonously associated with the user's willingness to reveal the data. Privacy dimensions can be identified at different degrees of detail.

Based on the semantics of P3P, a priori all standard parts of a P3P privacy `STATEMENT` are possible negotiation dimensions: 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. The importance of each of the four dimensions as perceived by the users and their respective willingness to provide

Proceedings of the Seventh IEEE International Conference on E-Commerce Technology (CEC'05)
1530-1354/05 $20.00 © 2005 **IEEE**

information depend on the thematic domain of the service.

2.2. Privacy vs. Personalization – User's Individual Utility Calculus

In order to model the user's individual trade-off between personalization and privacy, we present this as a utility maximization problem, taking into account different overall sensitivity levels towards privacy and different importance one may assign to a specific privacy dimension. The formalisation allows solving the negotiation game presented in section 3, giving the service provider the opportunity to choose its optimal strategy.

We denote the user's utility by U, using the following notations:

D^n is a n-dimensional privacy space and
$d_i \in D$ are its privacy dimensions
a_i is the user's data revelation level on dimension d_i
a_i^T is a threshold indicating the minimum required data the user must reveal
α_i is a weighting of dimension d_i
γ indicates the user's global privacy sensitivity
R is the discount provided by the service provider
P are other non-monetary personalization benefits
B is the base utility by the execution of the contract

$$\text{(I)}\ U(.) = -\gamma \cdot \prod_{i=1}^{n} a_i^{\alpha_i} + P(a_1, ..., a_n) + R(a_1, ..., a_n) + B$$

In case that the user is not willing to provide sufficient data for the contract to be executed, the base utility B and the discount R will be zero (II). The user gets the personalization benefits P even if the involved parties do not conclude on a contract. In case P is less than the negative utility the user gets from providing the necessary data, the user will prefer anonymous (or pseudonymous) usage of the services (III).

$$\text{(II)}:\ R(\vec{a}) = 0 \quad \wedge \quad B = 0 \Leftarrow \exists i : a_i < a_i^T$$

$$\text{(III)}:\ P(\vec{a}) < -\gamma \cdot \prod_{i=1}^{n} a_i^{\alpha_i} \Rightarrow \text{anonymity preferred}$$

As the ability to infer a user's identity does not increase linearly when more data is provided, we use a **Cobb-Douglas utility function** instead of an additive composition for the negative utility of data revelation.. In addition, there are two other interesting characteristics in the context of profile data and privacy awareness that are related to each other: first, the different privacy dimensions are not perfectly substitutable. For example, the user's telephone number and her e-mail address constitute two possible ways to contact the user but they are not completely interchangeable. Second, different to an additive composition, the substitution rate between two privacy dimensions (which yields here to $-\alpha_i a_i / \alpha_j a_j$) is not constant or independent from the current level of revealed data. The substitution rate decreases with the amount of data already provided: consider an online fashion retailer, presenting personalized offers based on the user's age. Knowing the month of birth in addition to the year of birth allows only marginal improvements.

The **thresholds a_i^T** are set by the service provider and are usually openly communicated. In implementations, hints like 'required field' or 'required information' are common practice. The necessity to provide this minimum of information can usually be deduced from the nature of the transaction.

The **weightings α_i** for each of the privacy dimensions as well as the global privacy sensitivity γ are private information of the user and constitute her type. The same holds for the valuation of the non-monetary **personalization benefits P** and the **base utility B**, but these two components will be neglected in the further analysis: P can be valuated and subsumed under R and B does not depend on the data revelation levels. Hence, the user's type is determined by α_i and γ.

The influences of the different parts on the user's utility function are described by the **partial derivatives** and their interpretations shown below:

$\partial U / \partial a_i \geq 0$: Any privacy infringement reduces the user's utility unless she does not care.

$\partial U / \partial R > 0$: The user appreciates discounts.

$\partial R / \partial a_i \geq 0$: But the service provider is only willing to grant discounts in case he gets some personal information in return. The case $\partial R / \partial a_i = 0$ is applicable for a privacy dimension that does not matter in the current transaction scenario or for a privacy dimensions on which the service provider does not honour revelation.

$\partial P / \partial a_i \geq 0$: The more data the service provider can access, the better the personalization will be.

2.3. Negotiating on the 'data'-Dimension

Some recent work proposed to negotiate about the recipient of the data in different application scenarios [3, 10, 11]. We propose the extent and kind of shared data as negotiation dimension for online retailing. First, the (initial) recipient is at the time fixed and the disclosure practices are often determined by the provider's business processes. Second, the relevance of the retention time is rated considerably less important by users. Third, the purpose may be a negotiable aspect of privacy practices, but all data carries with it a more or less pronounced intrinsic purpose.

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 across the

various types of information, implying weighting factors α_i. The global privacy sensitivity expressed by γ, will be examined in the following section.

3. The Service Provider's Perspective

3.1. Facing Different Types of Users

The service provider is confronted with different types of customers that first have various global privacy sensitivity levels, and second – for a given sensitivity level – may rate the importance of one kind of data differently. Efficient customer value extraction is based on a combination of discrimination and negotiation techniques. Discrimination relies on the identification of different groups of customers having the same (or a comparable) type. [1] identified a user typology later refined by [6] and summarized in Table 1. The distribution of the types is assumed to be common knowledge.

Table 1: User types [1, 6]

Type: Characteristics, Important factors
θ_{PF} (**privacy fundamentalists**): γ near 1 extremely concerned about any use of their data; θ_{PA} (**profile averse**): γ near 0.5 sensitive about computer equipment, salary, hobbies, health or age θ_{IC} (**identity concerned**): γ near 0.5 sensitive about postal address, e-mail address, phone number or credit card number θ_{MC} (**marginally concerned**): γ near 0 generally willing to provide data

3.1 Modeling the Negotiation Process

We will adopt a game-theoretic modelling approach (also see [2]), proposing a sequential game as framework.

All users must be offered the same bargaining interface in case they are indistinguishable for the service provider. Assuming that privacy fundamentalists are reliably identifiable by means of web usage mining technologies, they may be proposed a take-it-or-leave-it offer, as in most cases, their valuation personal data will be higher than the discounts the service provider can offer. The resulting subgame can be solved by standard procedures. Cf. figure 1 where the nodes for the types θ_{PA}, θ_{IC} and θ_{MC} are in the same information set whereas the node for type θ_{PF} is apart.

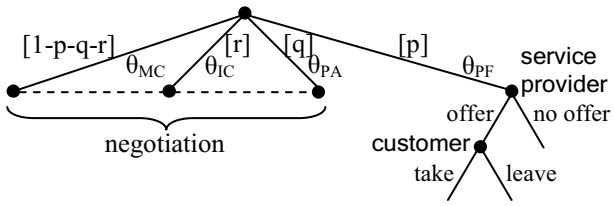

Figure 1: The service provider negotiates with three types he cannot distinguish

In order to determine the service provider's best strategy, one must maximize his total expected outcome while respecting the users' participation constraint (U(.) - B > 0).

The framework for the negotiation process is a dynamic game where the service provider has high bargaining power: He opens the negotiation with a basic offer, consisting of a small discount and a few personal data (the threshold) to be asked. This constitutes the fallback offer in case the user does not want to enter negotiation. In case the user accepts, she will be presented another offer with a higher discount and more data to be asked. On every step, the user may **cancel** (i.e. no contract or the fallback solution are implemented), **continue** to the next step or **confirm** (i.e. the reached agreement will be implemented).

For a given privacy dimension, revelation level is monotonously increasing in the sequence of steps. The service provider can also implement more alternatives for one step, so that the user can choose which data she will provide (for example home address or the office address). A switch to another dimension is performed in case the user refuses to provide further data or the service provider is not interested in a higher detail level for the current dimension

4. Implementation

The described negotiation process can be implemented using the extension mechanism of P3P. 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` as described in [9]. A `NEGOTIATION-GROUP-DEF` element defines an abstract pool of alternative usage scenarios. Each statement can be a possible usage scenario; the pool membership is expressed by the `NEGOTIATION-GROUP` extension in the statement, which describes relevant parameters of the given scenario, such as the benefits for the user. The following example where the user of a bookstore can choose between electronic delivery by mail (e-book) and postal delivery (hard copy) illustrates the usage:

```
<POLICY>
...
<EXTENSION optional="no">
 <NEGOTIATION-GROUP-DEF id="delivery"
  short-description="Choosing medium" />
</EXTENSION>
...
<STATEMENT>
 <EXTENSION optional="no">
  <NEGOTIATION-GROUP id="delivery"
     name="delivery as e-book"
     benefits="10% discount" />
 </EXTENSION> ...
 <DATA-GROUP>
  <DATA ref="#user.home-info.online.email"/>
 </DATA-GROUP>
</STATEMENT>
...
<STATEMENT>
 <EXTENSION optional="no">
  <NEGOTIATION-GROUP id="delivery"
     name="delivery as hard copy"
     benefits="robust hard-cover" />
 </EXTENSION> ...
 <DATA-GROUP>
  <DATA ref="#user.name"/>
  <DATA ref="#user.home-info.postal"/>
 </DATA-GROUP>
</STATEMENT>
...
</POLICY>
```

Note that the benefits given in human-readable format need to be displayed concisely by the user agent. The exhaustive machine-readable coding of the benefits is a remaining challenge, especially for multi-dimensional phenomena.

5. Conclusion and Further Work

This paper has presented the necessity of 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. In the context of identity management systems, negotiation gives the user more control over his personal data and thus may act as privacy enhancing technology (PET).

Using the extension mechanism of P3P, there is no conceptual limitation in coding negotiable alternatives, 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.

We are currently planning an experiment where a bargaining game will be set up. This includes the development of a prototype with support for the proposed extensions and tool support to generate the extensions in through an easy user interface. Inter alia, we want to investigate if there is a "hint effect", i.e. that users feel more concerned about their privacy when an explicit negotiation process is started.

6. 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) pp. 1-8, http://doi.acm.org/10.1145/336992.336995, 1999

[2] Cranor, L. F., Resnick, P., "Protocols for Automated Negotiations with Buyer Anonymity and Seller Reputation", *Netnomics*, http://www.si.umich.edu/~presnick/papers/negotiation, 1999

[3] El-Khatib, K., "A Privacy Negotiation Protocol for Web Services". in: *Proceedings of the International Workshop on Collaboration Agents: Autonomous Agents for Collaborative Environments (COLA)*, 2003

[4] International Business Machines Corporation, "Enterprise Privacy Authorization Language (EPAL 1.2)", W3C Member Submission 10 November 2003 , http://www.w3.org/Submission/EPAL/, 2003

[5] Karrass, C. L., "Give and Take: The Complete Guide to Negotiating Strategies and Tactics", HarperCollins Publishers, New York, NY, 1993

[6] Spiekermann, S., "Online Information Search with Electronic Agents: Drivers, Impediments, and Privacy Issues", 2001

[7] Ståhl, I.: "Bargaining Theory", Stockholm, Sweden: The Economics Research Institute, 1972

[8] W3C, "A P3P Preference Exchange Language 1.0 (APPEL1.0)", W3C Working Draft 15 April 2002, http://www.w3.org/TR/P3P-preferences, 2002

[9] W3C, "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/, 2005

[10] Yee, G., Korba, L., "Feature Interactions in Policy-Driven Privacy Management", in: *Proceedings from the Seventh International Workshop on Feature Interactions in Telecommunications and Software Systems (FIW'03)*, 2003

[11] Yee, G., Korba, L., "The Negotiation of Privacy Policies in Distance Education", in: *Proceedings. 4th International IRMA Conference*, 2003