University of Applied Sciences Northwestern Switzerland
School of Business

sponsored by
Ecademy CH

CollECTeR Europe 2006

Proceedings edited by
Petra Schubert and Daniel Risch

Published June 2006

basel, switzerland, june 9-10
CollECTeR europe 2006
collaborative electronic commerce technology and research

Proceedings

University of Applied Sciences Northwestern Switzerland
School of Business
Competence Center E-Business Basel

Peter Merian Strasse 86
4002 Basel

www.e-business.fhbb.ch

Collaborative Electronic Commerce Technology and Research Background of CollECTeR Europe 2006 in Basel, Switzerland

The CollECTeR series of conferences (http://www.collecter.org/) was established to link research centres at universities to form a basis for collaborative research in Electronic Commerce.

Conference Topic 2006: Collaborative Business

The "networked economy" challenges organizations to consider the use of Collaborative Business, namely the combined deployment of groupware and e-business infrastructures. Mobile computing technology and collaboration support have reached a level that makes a seamless integration of communications and data processing economically feasible. This constitutes our notion of Collaborative Business: the timely bundling of communication, coordination, and collaboration activities.

The focus of CollECTeR Europe 2006 is on new forms of Customer Relationship Management (CRM) – including mobile CRM – that cover the whole value chain and use new working modes. This concerns questions related to the optimisation of channels, the improvement of customer acquisition and retention, and after-sales contacts and services.

Aim

CollECTeR Europe 2006 is a forum for researchers to present and discuss their current and ongoing work. In order to stimulate a lively discussion the number of participants is limited to approx. 30 people. The aim of the event is to bring together researchers and practitioners to discuss foundations and industry potentials of Collaborative Business. This includes the exploration of the effective deployment of novel technologies and services.

Contributions are grouped into sessions covering the following topics:

- Digital archiving, privacy and property rights
- Personalization
- Markets and business processes
- Mobile and ambient business
- Communities and Work Group Collaboration
- Social systems
- Security devices and secure communication

All paper submissions to CollECTeR Europe 2006 represent the original work of the authors. There were no rigid guidelines regarding paper size for the final research papers. We asked to submit between 6 and 8 pages.

The social event, the conference dinner, lunches and breaks were sponsored by Ecademy, the National Network of Excellence of the Swiss Universities of Applied Sciences for E-Business and E-Government.

Basel, June 2006 Petra Schubert and Daniel Risch

Table of Contents

Privacy Negotiations enhance Data Collection for CRM

Sören Preibusch

German Institute for Economic Research
spreibusch@diw.de

Abstract

The application of Privacy Negotiation Techniques alleviates the Privacy-Personalization trade-off by reconciling consumers' quest for Privacy with the service providers' personalization efforts. The kind and amount of personal data to be disclosed is individually settled. By applying the mechanisms of privacy negotiations to data collection for customer relationship management purposes, drop out rates can be reduced. The service provider strategically designs the negotiation settings and includes external sources in the data acquisition process. This paper describes the service provider's tasks when designing a successful negotiation scheme and provides two examples of use in telecommunication industry.

1 Introduction

Consumers are facing a large and increasingly complex range of web based services. Recent applications include online retailing, where product information and personalised product recommendations are made available to the shopper. Retail stores are constantly expanding their assortments in width, depth and quality levels. As a result, consumers are confronted with a number of product alternatives that makes an exhaustive comparison impossible [Gross 1994]. Therefore, customers appreciate being offered effective guidance through automated recommender systems [Personalization Consortium, 2000].

On the supply side, service providers face stiff price competition due to the commoditization of digital services. Successful customer value extraction requires attracting and binding customers by new means. Personalized services, individually tailored for a single consumer, create lock-in effects. In addition, enterprises need to identify potential high-value customers to successfully focus their marketing endeavours. A recent survey concluded that knowledge from, for and about customers is a mission-critical factor [Salomann et al. 2005].

Yet Customer Relationship Management (CRM) typically relies on large amounts of data to be collected and kept over time. For new customers, credit assessment or service eligibility evaluation requires the potential user to divulge personal data for at least a one-time use. Careless data collection activities and data misuse are nowadays discussed in mass media and remember customers to care about their Privacy.

The depicted situation is known as the Privacy-Personalization trade-off. A common way for websites to communicate their data-handling practices is to post “privacy policies” on their website. Though, this approach is too inflexible and impractical. Privacy Negotiation Techniques (PRINT) can overcome current drawbacks of static privacy policies, and reconcile privacy and personalization.

Our contribution is to depict how privacy negotiations can be used to enhance the data collection activities for CRM. It will be shown that individually negotiable revelation schemes lower drop-out rates due to customers aborting transactions when too much personal data is asked for [IFAK 2002]. Well-crafted negotiation strategies and data combination from multiple sources allow enterprises to gain access to previously private information.

The remainder of this paper is organized as follows: Section 2 will briefly explain the mechanisms and advantages of privacy negotiations. Section 3 focuses on the strategic design of privacy negotiations and describes the service provider’s tasks. Before concluding with a summary and outlook, a detailed application scenario in telecommunications is provided in section 4.

2 Advantages of Privacy Negotiations

Thompson defines negotiations as an “interpersonal decision-making process necessary whenever we cannot achieve our objectives single-handedly” [Thompson 2005]. Distributive negotiations are carried out in case the amount to be distributed is fixed and the stakeholders only discuss how to allocate it. Due to the scarcity of goods, distributive negotiations lead to win-lose situations. Multi-attribute negotiations, however, offer the opportunity to find an integrative solution which is beneficial for all parties involved. Such mutually beneficial bargains increase welfare and unleash additional economic potential [Ströbel 2000]. When applied to privacy levels, integrative negotiations between a service provider and a user can overcome two major shortcomings of existing online privacy handling mechanisms:

- The first shortcoming is the “take-it-or-leave-it” principle. The user can only accept or refuse the provider’s privacy policy proposal as a whole.
- The second shortcoming is the “one-size-fits-all” principle. Once the service provider has designed his privacy policy, it will be proposed to all potential customers – regardless 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.

Due to the limned shortcomings, the provider fails to tap the users’ full potential. It has been demonstrated that the drawbacks of static privacy policies persist even if the service providers offers several of them. Similarly, a market-driven specialization of competing service providers, each of them focussing on a user group with given privacy preferences will not succeed [Preibusch 2006a].

Privacy negotiations can be implemented in Web applications by extending the Platform for Privacy Preferences (P3P) developed by the W3C [W3C 2006]. P3P enables service providers to express their data collection practices in standardized machine-readable policies. Via P3P’s built-in extension mechanism, multiple negotiation options can be coded smoothly and displayed to the user at his choice [Preibusch 2006b].

3 Strategic Design of Privacy Negotiations

As observed in the previous section, the economic benefits and the ease of implementation plead for service providers to migrate to dynamic, i.e. negotiable privacy policies. When putting privacy negotiations into practice, service providers have to perform several consecutive tasks, each of them being portrayed in the following sub-sections.

3.1 Service Provider's Tasks

3.1.1 Choosing the Negotiable Privacy Dimensions

Apparently, it is not feasible to negotiate entire privacy policies. Typically, a privacy policy is composed of parts that can be subject to negotiations and parts that are fixed and not suitable for individual agreements. As an example, consider the meta-information contained in a privacy policy, stating expiry dates, issuer data, and contact information. These parts are unchanging.

Hence, 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 [Preibusch 2006a].

The four top-level privacy dimensions are the recipient of the data, the purpose for which the data are collected, the time they will be stored, and the kind of data. These four dimensions (recipient, purpose, retention time, and data) are in accordance with European privacy legislation [European Parliament 2002a, 2002b].

The importance of each of the four dimensions as perceived by the user as well as her respective willingness to provide information depends on the thematic domain of the service. Yet, it is common to focus on the amount and kind of data to be revealed. Hence, the service provider has to choose a subset of the privacy dimensions spanning the data space. Examples for second-level privacy dimensions under the data dimension are: the user's name, her birth date, postal address, and telecommunication details.

When examining traditional data collection practices, one notices that the data requested from the user coincides with the data to be used in the subsequent business processes. However, when enhancing data collection with privacy negotiations, this identification no longer stands: the service provider faces different types of users having different revelation preferences for each of the privacy dimensions in concern [Preibusch 2006a]. By taking advantage of complementarities between personal data, the service provider may offer alternative privacy dimensions from which the user can choose. Data complementarities are largely based on inference rules. For instance, the user's home country (privacy dimension: postal address) can be inferred from her international telephone code (telecommunication details). The case study in section 4 will further stress on this issue.

3.1.2 Choosing the privacy Revelation Levels

After having decided the negotiable privacy dimensions, the service provider fixes different discrete revelation levels and a revelation threshold for each of the privacy dimensions. The revelation levels correspond to increasing detailedness. For instance,

the dimension ‘birth date’ may have the revelation levels ‘none’, ‘year’, ‘year and month’, ‘year, month and date’, and ‘year, month, date and hour’. Obviously, the service provider will not include irrelevant facts like the hour of birth – thus, he imposes an *upper limit* for the revelation levels.

The thresholds indicate the minimum detail level to be revealed and are usually openly communicated. They correspond to the *lower limit* for the revelation levels. In implementations, hints like ‘required field’, ‘required information’ or form fields marked by an asterisk are common practice. The obligation to reveal those data can be deduced from the nature of the transaction: It is obvious that an online bookstore cannot achieve postal delivery if the user refuses to provide her shipping address.

The different degrees of detail corresponding to the revelation levels are usually easily deducible from the data type. Users can be guided to a given revelation level by a wisely chosen rebate structure (cf. next section). Thus, setting the thresholds is the major scope for designing the negotiation environment.

3.1.3 Designing the rebate structure

Private information being of value to both the information holder and the information seeker, the customer expects to get compensation when revealing personal data. The user’s benefits can be divided into non-monetary personalization benefits and monetary benefits. Latter are well assessable and can thus be subject to planning; the service provider develops a discount scheme, indicating the rebate on the purchase price granted to the customer when revealing a given combination of private information. The rebate structures maps every possible privacy negotiation outcome to a percentage. (Note: Coupons of a fixed amount are often used in practice. They are equivalent to a percentage discount worth at most the ratio of the minimum purchase price.)

The design of the rebate structure constitutes the service provider’s major possibility to make customers prefer one negotiation alternative over another. Yet, the setting has to fulfil the constraints of incentive-compatibility as described in the next section.

3.2 Incentive-Compatible Rebate Structures

The service provider faces different types of users with diverging privacy preferences [Preibusch 2006a]. Though he knows that different types exist, such like identity concerned or marginally concerned customers [Spiekermann 2001], the service provider is unable to tell a user’s type at the time when revealing her the rebate structure. It can be acknowledged that every user prefers higher discounts over lower discounts and less detailed revelation over more detailed revelation; yet the concrete preference subtleties are unknown to the service provider. Thus, the final rebate structure has to incentivise *all* users so that they opt for negotiation outcome beneficial to the service provider *regardless their type*.

Incentive compatibility has to be fulfilled at the time when the customer makes his decision about which data to reveal. Yet, CRM efforts are targeted to long-term relationships and participants’ attitudes may vary over time: a participant may be initially very open in terms of providing personal information for a CRM system, but later decide to draw back information. We consider it to be hard for participants to take these changes in attitudes into account. Privacy preference transformations are often triggered by external events like misuse of data or other bad experience, unforeseeable by the user.

The correct discounting of uncertain future utility values is a challenging if not unattainable cognitive task. Still, these multi-period aspects are consistent with our model when interpreting the user's utility values as present values.[1]

Consider the following example where the service provider faces a marginally concerned consumer (index 1) and an identity concerned user (index 2). The parties negotiate about the customer revealing her birth date and her email / name as an identifier. For the dimension 'birth date', the revelation levels 'none' (0), 'year of birth' (Y), and 'year, month, and day of birth' (YMD) exist; for the dimension 'name', the revelation levels 'none' (0), 'email' (E), and 'email, first name, and last name' (EFN) exist, with the revelation threshold being to divulge at least the 'email' address. The following figure (Fig. 1) depicts the global rebate (R) and the disutility values U_{DD} for both user types: this negative utility value must be compensated at least by an appropriate discount, before the consumer is willing to disclose the respective information [Preibusch 2006b].

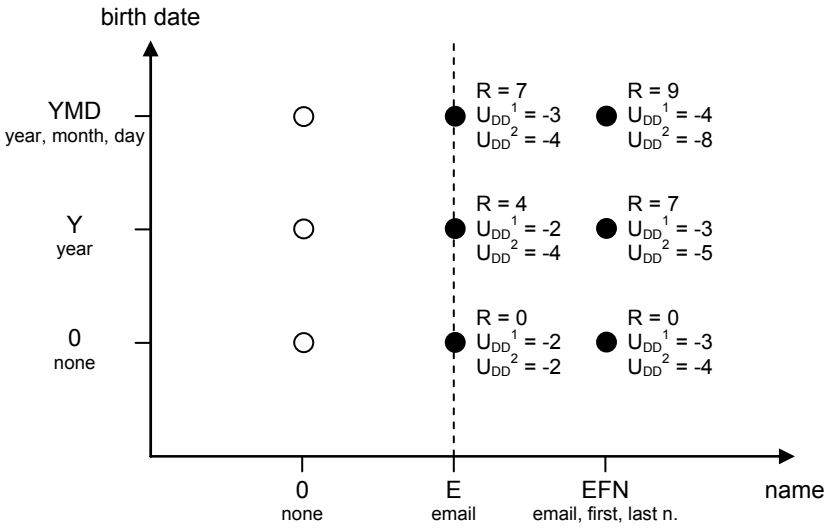

Fig. 1: Rebates (R) and disutility values (UDD) for two types of users. Negotiation outcomes not fulfilling the revelation thresholds are excluded from further analysis.

Each user chooses the negotiation option that yields to the maximum positive total utility $U = U_{DD} + R$.

Based on the current rebate structure, both users would disclose their full birth date, but only the marginally concerned user (1) would also reveal her full name details. The identity concerned user (2) would only disclose her email address (cf. Fig. 2). Though, in multiple settings (cf. section 4 for an example from telecommunications), the service provider valuates access to a user's name details higher than to the birth date details: For customer segmentation based on ages, only the year of birth is necessary, as is for majority checks. In addition, as shown in the next section, the first name can be used to impute a user's age and validate her statements concerning her age.

[1] Privacy-friendly systems may respond to changing user preferences by setting relatively short data retention times, allowing for renegotiation after a given period.

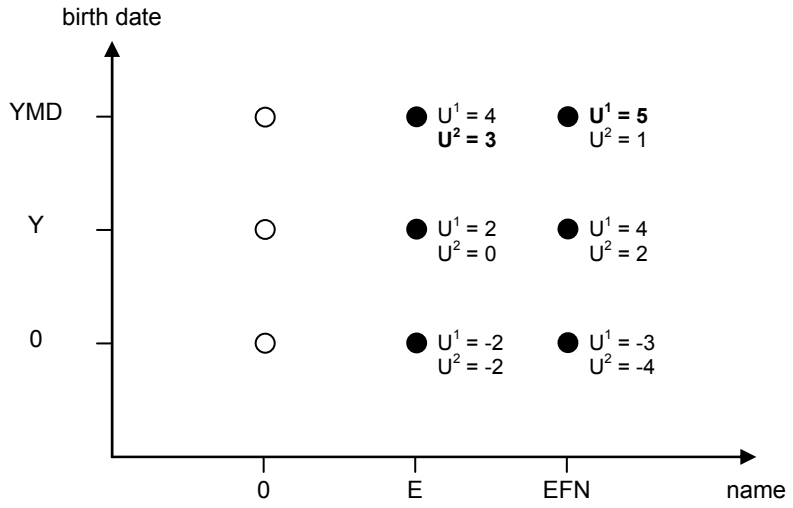

Fig. 2: User 1 would choose the negotiation option (EFN, YMD) and user 2 the option (E, YMD).

The service provider thus has to revise its negotiation design so that all users reveal their name details. The first alternative is to increase the threshold on the 'name' dimension. This, however, would result in a rather rigid setting, more comparable to static privacy policies than to privacy negotiations. The second alternative is to change the discounts. The service provider can either (a) increase the rebates for desired outcomes, or (b) reduce the rebates for unwelcome outcomes.

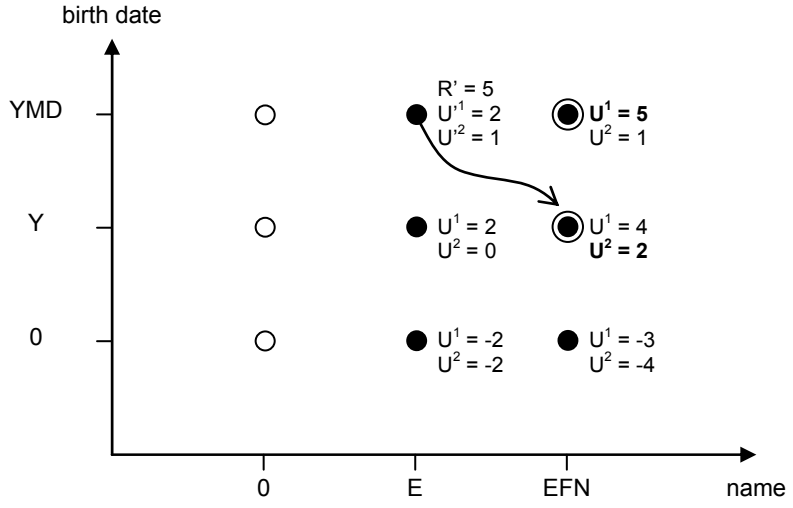

Fig. 3: Revised rebate structure: Both users choose negotiation options where they reveal full name details.

(a) The service provider may increase R(EFN, Y) by 2. However, the user 1 would then switch to (EFN, Y) which is an undesirable result. The service provider may also increase R(EFN, YMD) by 3. Yet, this would result in R(EFN, YMD) being 12 – an unjustifiable high value.

(b) The service provider may decrease R(E, YMD) by 2. User 1 would stay with the option (EFN, YMD) and user 2 would switch (EFN, Y). Consequently, both users would reveal full name details.

3.3 Strategic Alignment of Privacy Negotiations

The service provider's overall strategy aims at exploiting competitive advantages. Hence, all sub-strategies need to be targeted at acquiring new customers, at retaining existing relationships, and at performing in customer value extraction.

Accordingly, the service provider's privacy negotiation strategy has to be embedded in and needs to be aligned with its corporate strategy. As accentuated in the *customer profile life cycle* [Schubert/Koch 2002], data collection must be governed by a collection strategy. This also holds for privacy negotiations: As depicted in the previous section, the rebate structure as a core element of the negotiation environment requires revision if need be: the existing discount scheme was adapted as it formerly gave the wrong incentives. The following section illustrates the process of implementing such a goal-supporting privacy negotiations strategy based on a real-world case-study.

4 Case Study: Implications for CRM in Telecommunications

Having shown that strategically well-crafted privacy negotiations support data collection for CRM, we will now provide evidence from telecommunication industry for the successful application of these methods. Considering the case of Deutsche Telekom, we show that determining the age of potential customers is crucial and how imputation mechanisms for customer ages can be used. Second, considering the case of Vodafone, we will demonstrate how these findings can be integrated in existing data collection scenarios.[2] In addition to the results of section 3.2, we will highlight the importance of revelation thresholds in simplified privacy negotiations.

4.1 Deutsche Telekom: Determining the age of potential customers is crucial

In summer 2005, Germany's leading telecommunication provider for landline network, T-Com, planned the introduction of a new family rate [microm 2005]. T-Com is a division of Deutsche Telekom AG and operates primarily in the German market, with representations in Hungary, Macedonia, Montenegro (through Magyar Telekom), Croatia (through T-Hrvatski Telekom), and Slovakia. With about 41.7 million narrowband connections and 7.7 million broadband connections, T-Com is one of the biggest fixed network suppliers in Europe [Deutsche Telekom AG 2006].

The analysis of data from the billing system, the customer relationship management system, and the contract management helped identifying the customers *not* susceptible to adopt the new rate. However, identifying the right customers remained a challenge. The age of the customers, beside their turnovers, was recognized to be the key indicator for targeting the customer group. The existing data about turnovers and provided birth date were not sufficient for a satisfying identification of families [microm 2005]. Mainly the analysis of the customers' first names helped to close the gaps in the age-related data. The third party analysis provider "microm Micromarketing-Systeme und Consult GmbH" supplied the necessary matching between first name and age.

[2] The cases are based on publicly available information from the mentioned companies.

The age of a customer, beside her purchasing power and her marital status, is one of the most important variables in customer targeting. Several products only come into question for a narrow age-group. If age data is missing for all or for some entries in a customer database, first name analysis can help to induce the missings. Yet, the imputation of a customer's age is not trivial as remarkable regional differences in the naming behaviours can be observed. For instance, a typical "Johannes" is 65 years old when living in the East of Germany, but only 46 years when living in the South of Germany [microm 2006]. [Huschka, Gerhards, Wagner 2005] provide additional background information on the naming differences in divided Germany based on the data of the German Socio-Economic Panel Study (SOEP), supporting the thesis of naming patterns differing across regions.

Still, in an online transaction context, the availability of additional information can drastically improve the accuracy: When one knows whether the potential consumer lives in Erfurt or in Essen, the regional naming differences can be used for precise imputations. By combining automatically collectible data from the user's explicit profile (like the IP-address) with implicit profiles (e.g. the mapping from IP-addresses to regions), the data inference algorithms can be notably improved [Schubert 1999]. Services like IP2Location™ [IP2Location.com 2005] or GeoIP® [MaxMind 2006] identify visitors' geographical location i.e. country, region, city, latitude, longitude, ZIP code, ISP and domain name using a proprietary IP address lookup database, partly free of charge.

4.2 Vodafone: Consequences for Web-based data collection

According to the findings of the previous section, the general contact form on the German Vodafone Web site has been designed: First name and last name are collected for each inquiry even though only the email address would be necessary to answer the requests.

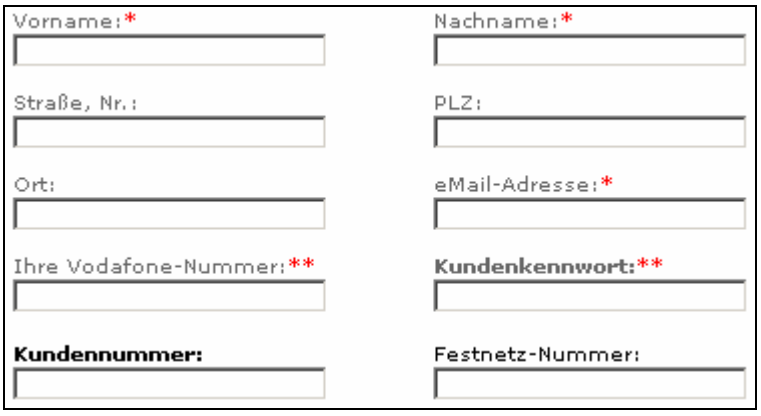

Fig. 4: Contact form on the German Vodafone Web site [Vodafone 2006]

Unlike the adaptation of the rebate structure in section 3.2, the service provider assures relevant data to be collected by setting restrictive revelation thresholds. This procedure is facilitated as there is a *social norm* for supplying the own full name when initiating a communication. Hence the visitor will probably not be surprised to be asked for her name – as it would be when asked for her birth date.

Implementing a contact form allowing for a negotiable data revelation scheme would alleviate the restrictiveness and provide customers with enhanced privacy, fulfilling the

principle of sparing data collection. As demonstrated in section 3.2, the service provider may still get the desired information as by offering the participant an enhanced CRM experience in return.

5 Conclusion and Further Research

Privacy negotiations can reconcile the personalization efforts of service providers with the privacy worries of its customers. The static privacy policies of traditional approaches are replaced by an individually negotiated revelation scheme. The service provider does not ask for every data item finally necessary; instead, data revelation alternatives are offered. The information seeker's task is to strategically shape a negotiation setting that sets the right incentives. The service provider chooses the negotiable privacy dimensions, fixes data revelation levels and thresholds, and maps out a rebate structure. By combining multiple possible input data with implicit profiles, missing data can be imputed and supplied data can be validated or checked for plausibility. The ratio of users to be lost due to excessive gathering of personal data will be reduced, as the users themselves can choose their revelation option. By the cases of Deutsche Telekom and Vodafone, we illustrated that these mechanisms are on the way to be implemented in large scale CRM.

The alignment of privacy negotiations with an overall customer data management strategy is of primordial importance. The top-down deduction of the right settings for privacy negotiations is subject of ongoing research. Implementation of an incentive-compatible rebate structure that is suited for different types of users is far from being trivial. The examples of industrial applications encourage us in our assumption that the framework of privacy negotiations will enhance data collection in customer relationship management.

Acknowledgements

The author would like to thank Michael Klafft at Humboldt-Universität zu Berlin for his helpful comments during the setup of this paper.

References

Deutsche Telekom AG (2006): Telekom - - Deutsche Telekom, http://www.telekom3.de/en-p/home/cc-startseite.html

European Parliament, Council of the European Union (2002a): Directive 2002/58/EC on privacy and electronic communications, in: Official Journal of the European Communities, 31.7.2002, L 201, pp. 37-47

European Parliament, Council of the European Union (2002b): Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000, in: Official Journal of the European Communities, 12.1.2002, L 8, pp. 1-22

Gross, P. (1994): The multi options society (original title: „Die Multioptionsgesellschaft"), Suhrkamp, Frankfurt am Main, 1994

Huschka, D.; Gerhards, J.; Wagner, G. G. (2005): Naming Differences in Divided Germany, in: Deutsches Institut für Wirtschaftsforschung, Research Notes 8, 2005

IFAK GmbH & Co (2002): Nur begrenztes Vertrauen der Verbraucher beim Einkaufen im Internet. Research study. Taunusstein. Jan. 18, 2002

IP2Location.com (2005): IP2Location™ Overview, http://www.ip2location.com/ip2location.pdf

MaxMind (2006): MaxMind - GeoIP, http://www.maxmind.com/app/ip_locate

microm Micromarketing-Systeme und Consult GmbH (2005): Krisenbewältigung im Data Mining - Der nutzenorientierte Einsatz microgeographischer Daten bei T-Com, http://www.microm-online.de/de/mcstddtl.htm?id=1199

microm Micromarketing-Systeme und Consult GmbH (2006): Vornamensanalyse, http://www.microm-online.de/de/mcstdlist.htm?cid=230

Personalization Consortium (2000): Personalization & Privacy Survey, 2000

Preibusch, S. (2006a): 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, 2006, pp. 604-615

Preibusch, S. (2006b): Personalized Services with Negotiable Privacy Policies, in: Proc. of the CHI 2006 Workshop on Privacy-Enhanced Personalization (PEP 2006), Montréal, Canada, 2006

Salomann, H.; Dous, M.; Kolbe, L.; Brenner, W. (2005): Customer Relationship Management Survey, Status Quo and Further Challanges, University of St.Gallen, 2005

Schubert, P. (1999): Virtual Communities of Transaction in Electronic Commerce: Management, Marketing and Social Environment (original title: „Virtuelle Transaktionsgemeinschaften im Electronic Commerce: Management, Marketing und Soziale Umwelt"), Lohmar - Köln: Josef Eul Verlag, 1999

Schubert, P.; Koch, M. (2002): The Power of Personalization: Customer Collaboration and Virtual Communities, in: Proceedings of the Eighth Americas Conference on Information Systems, (AMCIS), 2002

Spiekermann, S. (2001): Online Information Search with Electronic Agents: Drivers, Impediments, and Privacy Issues, 2001

Ströbel, M. (2000): On Auctions as the Negotiation Paradigm of Electronic Markets Success Factors, Limitations and Research Directions, in: EM Journal of Electronic Markets, Vol. 10, No. 1, 2000, pp. 39-44

Thompson, L.L. (2005): The Mind and Heart of the Negotiator. 3rd edn. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2005

Vodafone D2 GmbH (2006): Vodafone - Kontaktseite, http://www.vodafone.de/vodafonestars/17076.html

W3C (2006): The Platform for Privacy Preferences 1.1 (P3P1.1) Specification, W3C Working Draft 10 February 2006, http://www.w3.org/TR/P3P11/