

Communication of Privacy and Personalization in E-Business¹

Maximilian Teltzrow
Institute of Information Systems
Humboldt-Universität zu Berlin
Spandauer Str. 1, 10178 Berlin, Germany
teltzrow@wiwi.hu-berlin.de,
<http://www.wiwi.hu-berlin.de/iwi>

Alfred Kobsa
School of Information and Computer Science
University of California,
Irvine, CA 92697-3425, U.S.A.
kobsa@uci.edu,
<http://www.ics.uci.edu/~kobsa/>

1. Introduction

Privacy plays a major role in the relationship between companies and Internet users. However, results from consumer surveys indicate that the communication of privacy on the Internet has so far not yet been addressed effectively enough to alleviate consumer concerns: 64% of Internet users indicated having decided in the past not to use a website, or not to purchase something from a website, because they were not sure how their personal information would be used [1]. 90% want businesses to seek permission before they use their personal information for marketing [2]. 76% of users find privacy policies very important [3] and 55% stated that a privacy policy makes users more comfortable with providing personal information [4]. However, right now privacy statements are usually written in a way which gives the impression that the authors do not really want users to read them.² Thus, online tools communicating a company's privacy standards are necessary to decrease consumer concerns. Privacy protection is particularly interesting for personalization web sites [6] as these sites require detailed user information inferring higher privacy risks.

This work contributes to the improvement of privacy communication in personalized systems, giving users more control over personal data and personalization features. We propose a privacy tool that allows users to more objectively assess privacy threats and possible personalization benefits, and weigh them against each other. Studies have shown that users are highly concerned about their privacy [6] but often do not act accordingly [7]. Thus, better support tools are necessary to inform them about the privacy impacts of their online actions.

We first give an overview of existing approaches to communicate privacy to Internet users, indicate their shortcomings and then propose new ways to communicate privacy in a personalized context.

2. Existing Approaches and their shortcomings

We specifically focus on techniques to communicate privacy standards to visitors on commercial web sites. The currently predominant approach to this endeavor is the Privacy Preferences Protocol (P3P). It provides web site managers with a standardized way to disclose how their site collects, uses, and shares personal information about site visitors. However, the current P3P adoption rate on the top 100 web sites is only 30% [8]. This relatively low

¹ This research has been supported by the National Science Foundation (grant DST 0307504), Deutsche Forschungsgemeinschaft (DFG grant no. GRK 316/2) and by Humboldt Foundation in its TransCoop program.

² And this is indeed not the case: whereas 73% of respondents reported that they usually read privacy policies [1], web site operators report quite low attention to privacy policies. For example, on the day after the company Excite@home was featured in a 60 Minutes segment about Internet privacy, only 100 out of 20 million unique visitors accessed that company's privacy pages [5].

adoption of P3P seems to be due to P3P's problematic legal implications on the one hand [9], and insufficient support to users evaluating a site's P3P policy on the other hand.

The second problem is being partly addressed by AT&T's Privacy Bird [10], which allows users to specify their own privacy preferences, compares them with a site's P3P-encoded privacy policy when users visit this site, and alerts them when this policy does not meet their standards. Upon request, the Privacy Bird also provides a summary of a site's privacy policy and a statement-by-statement comparison with the user's privacy preferences.

A few browsers also allow users to specify certain limited privacy preferences and compare them with the P3P policies of visited websites. For example, *Internet Explorer 6* (IE6) allows users to initially state a very few privacy preferences and blocks cookies from sites that do not adhere to these preferences. The *Mozilla* browser goes one step further and allows users to enter privacy settings for cookies, images, popup windows, certificates and smart cards.

All these systems suffer from the following major shortcomings:

- 1) They require users to make privacy decisions in advance, without regard to specific circumstances in a particular site context. This disregards the *situational nature of privacy* [11]. In fact, initially stated privacy preferences and actual usage behavior often differ significantly [7].
- 2) Furthermore, the systems do not provide information about the *benefits* of providing the requested data. For instance, users indicate to be willing to share personal data more willingly if the site would offer personalized services [13].
- 3) They do not enhance users' *understanding* of basic privacy settings. For example, most users still do not know what a cookie is and what it can do.

Very recent work takes first steps to address some of these deficiencies. For instance, [14] aims at further enhancing the management of cookies and users' privacy in the *Mozilla* browser. Among other things, the authors study contextual issues such as how to enhance users' understanding of discrete cookie settings, at the time when cookie-related events occur and in a form that is least distracting. [15] is concerned with the communication of privacy choices under the European Union Data Protection Directive [16]. From the privacy principles in this Directive, the authors derive four HCI guidelines for effective privacy interface design: (1) comprehension, (2) consciousness, (3) control, and (4) consent. Since single large click-through privacy policies or agreements do not meet the spirit of the Directive, the authors propose "just-in-time click-through agreements" that are supposed to facilitate a better understanding of decisions since they are made in-context.

3. Privacy Support Tool

We introduce a tool that provides context-related information about privacy and personalization options. For users who want to have more control over their data and personalized features, the system provides a useful navigation support: it displays a specific situational communication dialogue, whenever user information is about to be collected. As the tool is specifically geared for usage in personalized systems, it also conveys information about potential personalization benefits that the user could enjoy in return for the required personal information. Thus, it allows users to make and reverse privacy decisions more deliberately. Furthermore, hyperlinks to additional explanations allow users to explore the implications of their privacy decisions in more detail.

In contrast to systems described in Section 2, our system provides the following advantages:

- No (or limited) presetting of privacy sensitivity is necessary. The tool supports users to more objectively balance privacy protection and personalization benefits:
 - Particularly, it allows the communication of privacy policies in a site-related and situational context.
 - Furthermore, it breaks up long privacy policies into smaller, more understandable pieces.
 - Communication of potential personalization benefits to the users take place at the time when privacy decisions are being made.
 - Personalization features are communicated before data is collected.
- The use of the system is optional and flexible.
- The tool may incorporate P3P policies but P3P is not a requirement.
- The tool gives users individual privacy choices, thereby possibly increasing trust.

4. Screenshots of Prototype

The following screenshots demonstrate the basic idea of the suggested privacy prototype. An advanced prototype version will be tested in experimental usage scenarios on different (simulated) web sites.



Fig 1: Optional Support with Privacy Tool on Sample Site Amazon.com

Permission to set cookies and explanation of cookie impacts

Simultaneous communication of potential personalization benefits

The screenshot shows the Amazon.com homepage. Two callout boxes are overlaid on the page:

- Privacy Support Tool:** Contains text explaining that personal information will remain anonymous and that users can accept or decline cookies. It includes a "Send" button and radio buttons for "Yes" and "No".
- Personalization Benefits:** Contains text explaining that giving permission to store cookies will allow Amazon to offer better service, such as optimized screen layouts and personalized recommendations. It also includes a "Send" button and radio buttons for "Yes" and "No".

The background shows the Amazon.com navigation bar, search bar, and various product recommendations like "DVD Save up to 35% on top sellers" and "Today's Top Sellers".

Fig. 2: Acceptance of Cookies

User choice of how site may use personal information

Personalization benefits for user's privacy selection

The screenshot shows the Amazon.com checkout page. Two callout boxes are overlaid on the page:

- Privacy Support Tool:** Contains text asking users to specify how they want their personally identifiable information used (current transaction only, future transactions, or marketing). It includes radio buttons for "Yes" and "No".
- Personalization Benefits:** Contains text explaining that providing personal information allows users to benefit from a variety of personalization features on the site. It also includes radio buttons for "Yes" and "No".

The background shows the checkout form with fields for "Full Name", "Address Line 1", "Address Line 2", "City", "State/Province/Region", "ZIP/Postal Code", "Country", and "Phone Number". There is also a "Continue" button and a note at the bottom regarding shipping restrictions.

Fig. 3: Input of Personally Identifiable Information

Non-intrusive presentation of personalization results

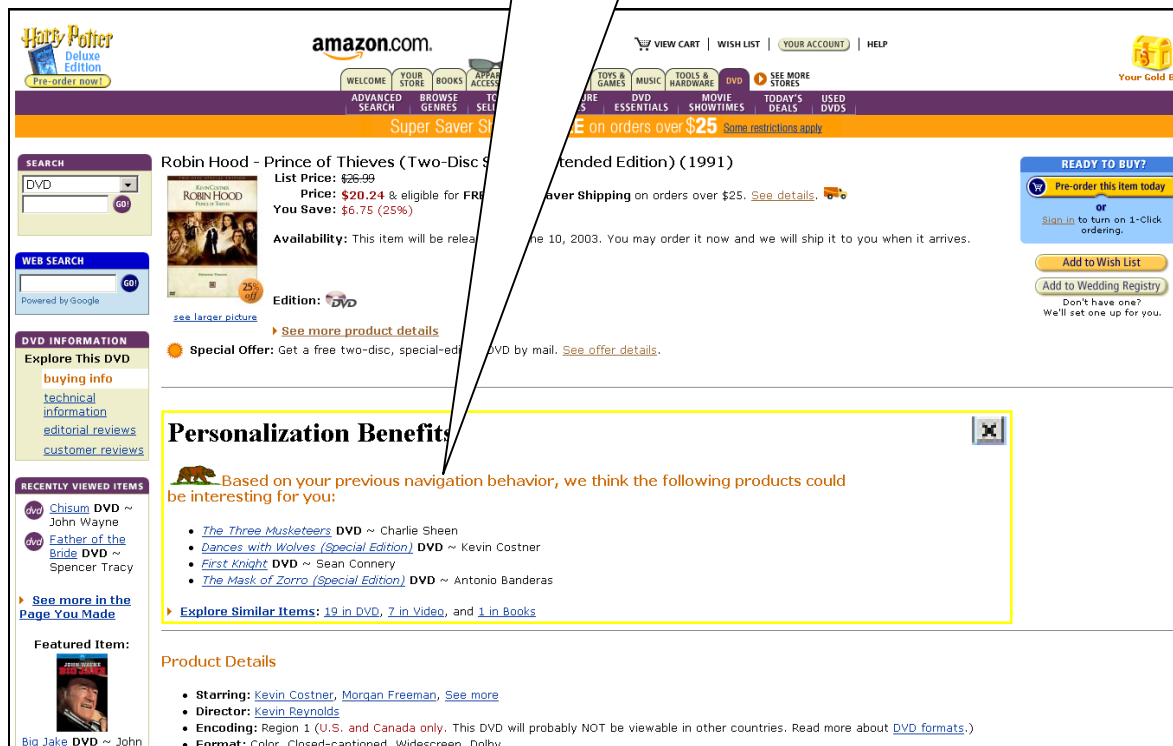


Fig. 4: Personalization Benefits

The screenshots describe parts of the prototype’s functionality. First, the visitor is introduced to the privacy tool (see Fig. 1) and can decide to interact with the tool or not. If the user clicks “yes” in the lower left corner, a frame appears whenever personal information is about to be collected (see Figs. 2-3). A short explanation is given for what purpose the data is used. The privacy explanations may refer to the P3P scenarios in Table 1 and depend on the company’s privacy policy. Furthermore, a brief explanation is given of how the consumer may benefit from personalization features in return for sharing personal with the web site (see Fig. 4). Thus, the user can decide in advance whether or not (s)he wants to disclose personal. The communication dialogue may help users to better manage the trade-off between privacy and personalization.

5. Further Work

Further work addresses typical data collection and adaptation scenarios in e-business. We are currently developing an improved version of our privacy support tool to help users better understand the purpose of data collection and personalization benefits on a site. Usability requirements will be integrated in the latest prototype version. We believe that this incremental and situational privacy support has advantages over the privacy tools described in section 2.

In Table 1, purposes for data collection have been summarized as described in the P3P specifications [17]. The privacy support tool will be based on these scenarios and communicate purposes of data collection and benefits of personalization to the users. The willingness to share data will be tested experimentally with two different user groups – one group will be supported with the tool and the other not.

Users’ satisfaction and willingness to share data on specific retail web sites will be measured. Study participants will be asked to perform specific tasks such as *registration* or

perform a product purchase. The influence of personalization parameters will be measured. Control factors such as site reputation, Internet experience, gender or trust will be included in the modeling process. Aversion types according to [18] will be determined after the experiment.

Data Collection Purpose	Explanation
Completion and Support of Activity For Which Data Was Provided	Information may be used by the service provider to complete the (one-time) activity for which it was provided, e.g. subscription update, mail forwarding
Web Site and System Administration	Information may be used for the technical support of the Web site and its computer system, e.g. web site maintenance
Research and Development	Information may be used to enhance, evaluate, or otherwise review the site, service, product, or market, but no tailoring
One-time Tailoring	Information may be used to tailor or modify content or design of the site where the information is used only for a single visit to the site and not used for any kind of future customization.
Pseudonymous Analysis	Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier, without tying identified data (such as name, address, phone number, or email address) to the record, e.g. a marketer may wish to understand the interests of visitors to different portions of a Web site
Pseudonymous Decision	Information may be used to create or build a record of a particular individual or computer that is tied to a pseudonymous identifier, without tying identified data (such as name, address, phone number, or email address) to the record, e.g. a marketer may tailor or modify content displayed to the browser based on pages viewed during previous visits.
Individual Analysis	Information may be used to determine the habits, interests, or other characteristics of individuals and combine it with identified data <i>for the purpose of research, analysis and reporting</i> , e.g. an online Web site for a physical store may wish to analyze how online shoppers make offline purchases
Individual Decision	Information may be used to determine the habits, interests, or other characteristics of individuals and combine it with identified data <i>to make a decision that directly affects that individual</i> . For example, an online store suggests items a visitor may wish to purchase based on items he has purchased during previous visits to the Web site.
Contacting Visitors for Marketing of Services or Products	Information may be used to contact the individual, through a communications channel other than voice telephone, for the promotion of a product or service. This includes notifying visitors about updates to the Web site.
Historical Preservation	Information may be stored for the purpose of preserving social history as governed by an existing law or policy.
Contacting Visitors for Marketing of Services or Products Via Telephone	Information may be used to contact the individual via a voice telephone call for promotion of a product or service.
Other Uses	Information may be used in other ways not captured by the above definitions.

Table 1: P3P Scenarios

Literature

1. Culnan, M.J., Milne, G.R.: The Culnan-Milne Survey on Consumers & Online Privacy Notices: Summary of Responses. In: Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices (2001). Washington, D.C.
2. Roy Morgan Research: Privacy and the Community. Prepared for the Office of the Federal Privacy Commissioner, <http://www.privacy.gov.au/publications/rcommunity.html>. (2001)
3. Department for Trade and Industry: Informing Consumers About E-Commerce. Conducted by MORI, London: DTI,, <http://www.mori.com/polls/2001/pdf/dti-e-commerce.pdf>. (2001)
4. Gartner G2: Privacy and Security: The Hidden Growth Strategy. Vol. (August 2001)
5. Wham, T.: Workshop on "the Information Marketplace: Merging and Exchanging Consumer Data," Federal Trade Commission. <http://www.ftc.gov/bcp/workshops/infomktplace/transcript.htm>. (2001)
6. Teltzrow, M., Kobsa, A.: Impacts of User Privacy Preferences on Personalized Systems - a Comparative Study. In: CHI-2003 Workshop "Designing Personalized User Experiences for eCommerce: Theory, Methods, and Research" (2003). Fort Lauderdale, FL
7. 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 (2001). Tampa, FL, (38-47)
8. Ernst&Young: P3P Dashboard Report. [http://www.ey.com/global/download.nsf/US/P3P_Dashboard_July_2003/\\$file/E&YP3PDashboardJuly2003.pdf](http://www.ey.com/global/download.nsf/US/P3P_Dashboard_July_2003/$file/E&YP3PDashboardJuly2003.pdf). (July 2003)
9. Cranor, L.F., Reidenberg, J.R.: Can User Agents Accurately Represent Privacy Notices? In: 30th Research Conference on Communication, Information and Internet Policy (2002). Alexandria, VA
10. AT&T: At&T Privacybird. <http://www.privacybird.com/>. (2002)
11. Palen, L., Dourish, P.: Unpacking "Privacy" for a Networked World. In: Proceedings of the Conference on Human Factors in Computing Systems (2002). Ft. Lauderdale, Florida, USA, (129-136)
13. Personalization Consortium: Personalization & Privacy Survey. <http://www.personalization.org/SurveyResults.pdf>. (2000)
14. Friedman, B., Howe, D.C., Felten, E.: Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. In: 35th Hawaii International Conference on System Sciences (2002). Hawaii
15. Patrick, A.S., Kenny, S.: From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interfaces. Third International Workshop, PET 2003, Dresden, Germany, March 26-28, 2003, Revised Papers, (ed). In: R. Dingledine, e.P.E.T. Heidelberg, Germany: Springer, Dresden, Germany (2003)
16. EU: Directive 95/46/Ec of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. Official Journal of the European Communities, Vol. (23 November 1995 No L. 281). (1995) (31ff)
17. P3P: W3C Platform for Privacy Preferences Initiative. <http://www.w3.org/P3P>. (2001)
18. Ackerman, M.S., Cranor, L., Reagle, J.: Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In: Proceedings of the 1st ACM E-Commerce (1999). Denver, Co