Privacy-Enhanced Personalization

Alfred Kobsa
Department of Informatics
University of California, Irvine
Irvine, CA 92697-3425 USA
kobsa@uci.edu

Ramnath K. Chellappa
Goizueta Business School
Emory University
Atlanta, GA 30322-1059 USA
ram@bus.emory.edu

Sarah Spiekermann
Berlin Research Centre on
Internet Economics
Spandauer Str. 1
10178 Berlin GERMANY
sspiek@wiwi.hu-berlin.de

CHI 2006, April 22–27, 2006, Montreal, Canada.
ACM 1-xxxxxxxxxxxxxxxxx.

Abstract
Consumer surveys show that online users value personalized content [5]. At the same time, providing personalization on websites seems quite profitable for web vendors [2, 6-8]. This win-win situation is however marred by privacy concerns since personalizing people's interaction entails gathering considerable amounts of data about them. As numerous recent surveys have consistently demonstrated, computer users are very concerned about their privacy on the Internet. Moreover, the collection of personal data is also subject to legal regulations in many countries and states. Both user concerns and privacy regulations impact frequently-used personalization methods. This workshop will explore the potential of research on "privacy-enhanced personalization," which aims at reconciling the goals and methods of user modeling and personalization with privacy constraints imposed by individual preferences, conventions and laws.

Keywords
Personalization, privacy, e-commerce, user modeling, user profiling, personal data

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous. K4.4. Electronic Commerce, K.4.1 Public Policy Issues

Introduction

It has been tacitly acknowledged for many years that personalized interaction and user modeling have significant privacy implications, due to the fact that personal information about users needs to be collected to perform personalization. [11] was arguably the first to discuss this problem in a 1990 article in AI & Society, but the paper had little impact. The only privacy "solution" of these days was to ascertain that users could store their models on a diskette (R. Oppermann, GMD) or PCMCIA card (J. Orwant, MIT [14]) and carry them with. The situation changed completely in the late 1990s, for three main reasons:

Personalized systems moved to the web
Web retailers quickly realized the enormous potential of personalization for customer relationship management and made their websites user-adaptive. This had significant privacy implications. While user models were previously confined to stand-alone machines or local networks, people's profiles were now collected by dozens if not hundreds of personalized websites. Widely publicized security glitches and privacy breaches as well as aggressive telemarketing have led to a wide-spread (~60-80%) reluctance of Internet users to disclose personal data and being tracked online. This however endangers the basic foundations of personalization [16].

Personalized systems move to mobile devices
Mobile devices can provide useful personalized services that are based on usage patterns and users' current location. Both are tracked in central servers, which creates new privacy problems. Users are not merely "online" any more and sheltered behind IP addresses, but become identified individuals who are being observed and contacted by their surrounding environments.

Restrictions are imposed by privacy legislation
Many countries, states and provinces have introduced privacy legislation which severely affect not only commercial websites but also experimental research on user modeling (in many cases even when it is done "just with IP numbers", "just with our students", or "just for testing purposes") [12]. Areas that are specifically affected include data mining for personalization purposes, adaptive tutoring systems that include learner models, and adaptation to the needs of people with disabilities.

As a consequence, the topic of "Privacy and Personalization" has received considerable attention from industry and academia in the past few years. Three industry conferences on this topic were held in 2000-01 (in New York, London and San Francisco) with a participation of about 150 people. The *Communications of the ACM* published two articles on this topic in 2000 [17] and 2002 [12]. The Ubiquitous Computing conferences have held privacy workshops in the past four years[1] that address (among other things) privacy in context-aware systems. The European Network of Excellence ProLearn devoted half a day of a workshop in 2005 to privacy and security issues in user modeling.

In July 2005, twenty researchers met for a first workshop on Privacy-Enhanced Personalization at the 10th International User Modeling Conference in Edinburgh.[2]

---

[1] See the links at http://www.cs.berkeley.edu/~jfc/privacy/

[2] See http://www.isr.uci.edu/pep05/

It did not focus on a specific application domain, and also aimed at finding integrated socio-technical solutions rather than pursuing technical, organizational or legal approaches alone.

Topic, goal and target audience of this workshop

This workshop will explore the potential of research on "privacy-enhanced personalization," which aims at reconciling the goals and methods of user modeling and personalization with privacy constraints imposed by individual preferences, conventions and laws. It will look at, e.g., the following questions:

- How much personal data do individual personalization methods really need? Can we find out in advance or in hindsight what types of data contribute to reasonably successful personalization in a specific application domain, and restrict data collection to these types of data?
- What are motivators for people to disclose personal information [4, 9], and what motivators are present in what kinds of personalization? How can the presence of such motivating factors be conveyed to users?
- If discrepancies between users' stated privacy attitudes and observed privacy behavior are rampant [10, 15], what methods should be chosen under what circumstances to conduct empirical research on privacy?
- If privacy decisions are impaired by limited information and bounded rationality [1], how can we help people make better choices?
- In this context, what is the status of "privacy preferences"?
- How much can we benefit from anonymity or pseudonymity infrastructures and trusted third parties, and are there limits that should be observed?
- Are distributed user models an answer or a problem from a privacy perspective?
- Does personalization in mobile and ubiquitous computing contexts pose additional challenges? How can they be overcome?
- Is client-side personalization a possible answer to privacy concerns and legal restrictions [3, 13]? What technical, legal and business obstacles will have to be overcome?
- What should an ideal legal framework look like from the perspective of privacy-enhanced personalization?

The workshop is intended for researchers and practitioners in the field of personalization systems and in the area of privacy and security, and specifically for people who are working in the intersection of both. The workshop participants will look at Privacy-Enhanced Personalization from an interdisciplinary perspective, including the areas of Human-Computer Interaction, Management Information Systems, and Economics. Participation from industry is strongly encouraged, since the results will have direct implications on existing websites.

Program committee

The following individuals assisted in the planning of this workshop and in the selection of submissions:

- Alessandro Acquisti, Heinz School of Management and Public Policy, Carnegie-Mellon University.
- JC Cannon, Privacy Strategist, Microsoft.

- Rahul Hampole, Privacy Analyst, Shopzilla
- Kai-Lung Hui, Department of Information Systems, National University of Singapore.
- Judy Kay, School of Information Technologies, University of Sydney.
- Ajay Nigam, Director of Communication Security Services, VeriSign
- John Riedl, Department of Computer Science, University of Minessota

References

[1] Acquisti, A. *Privacy in Electronic Commerce and the Economics of Immediate Gratification*. in *EC'04 ACM Conference on Electronic Commerce*. 2004. New York, NY, 21-29, DOI 10.1145/988772.988777.

[2] Bachem, C. *Profilgestütztes Online Marketing*. in *Personalisierung im E-Commerce*. 1999. Hamburg, Germany.

[3] Cassel, L. and U. Wolz. *Client Side Personalization*. in *DELOS Workshop: Personalisation and Recommender Systems in Digital Libraries*. 2001. Dublin, Ireland, http://www.ercim.org/publication/ws-proceedings/DelNoe02/CasselWolz.pdf.

[4] Chellappa, R.K. and R. Sin, *Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma.* Information Technology and Management, 2005. **6**(2-3), 181-202, DOI 10.1007/s10799-005-5879-y.

[5] ChoiceStream, *ChoiceStream Personalization Survey: Consumer Trends and Perceptions*. 2005, http://www.choicestream.com/pdf/ChoiceStream_PersonalizationSurveyResults2005.pdf.

[6] Cooperstein, D., et al., *Making Net Shoppers Loyal*. 1999, Forrester Research: Cambridge, MA.

[7] Hagen, P.R., H. Manning and R. Souza, *Smart Personalization*. 1999, Forrester Research: Cambridge, MA.

[8] Hof, R., H. Green, and L. Himmelstein, *Now it's YOUR WEB.* Business Week, 1998. October 5: 68-75.

[9] Hui, K.-L., B.C.Y. Tan, and C.-Y. Goh, *Online Information Disclosure: Motivators and Measurements.* ACM Transactions on Internet Technology, 2006. **6**(4), http://www.comp.nus.edu.sg/~lung/motivators.pdf.

[10] Jensen, C., C. Potts, and C. Jensen, *Privacy Practices of Internet Users: Self-Reports versus Observed Behavior.* Int'l J. of Human-Computer Studies, 2005. **63**: 203–227, DOI: 10.1016/j.ijhcs.2005.04.019.

[11] Kobsa, A., *User Modeling in Dialog Systems: Potentials and Hazards.* AI & Society, 1990. **4**(3), 214-240, http://www.ics.uci.edu/~kobsa/papers/1990-AISoc-kobsa.pdf.

[12] Kobsa, A., *Personalization and International Privacy.* Communications of the ACM, 2002(5), 64-67, DOI 10.1145/767193.767196.

[13] Mulligan, D. and A. Schwartz. *Your Place or Mine?: Privacy Concerns and Solutions for Server and Client-Side Storage of Personal Information*. in *Computers, Freedom & Privacy Conference*. 1999, 81-84.

[14] Orwant, J., *Heterogenous Learning in the Doppelänger User Modeling System.* User Modeling and User-Adapted Interaction, 1994. **4**(2), 107-130, DOI 10.1007/BF01099429.

[15] Spiekermann, S., J. Grossklags, and B. Berendt. *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, DOI 10.1145/501158.501163.

[16] Teltzrow, M. and A. Kobsa, *Impacts of User Privacy Preferences on Personalized Systems: a Comparative Study*, in *Designing Personalized User Experiences for eCommerce*, C.-M. Karat, J. Blom, J. Karat, eds. 2004, Kluwer: Dordrecht. 315-332, http://www.ics.uci.edu/~kobsa/papers/2004-PersUXinECom-kobsa.pdf.

[17] Volokh, E., *Personalization and Privacy.* Communications of the ACM, 2000. **43**(8): p. 84-88.