In: Jörg Schreck (2003): Security and Privacy in User Modeling.
Dordrecht, Netherlands: Kluwer Academic Publishers.

Foreword

User-adaptive (or ``personalized") systems take individual characteristics of their current users into account and adapt their behavior accordingly. Several empirical studies demonstrate their benefits in areas like education and training, online help for complex software, dynamic information delivery, provision of computer access to people with disabilities, and to some extent information retrieval. Recently, personalized systems have also started to appear on the World Wide Web where they are primarily used for customer relationship management. The aim hereby is to provide value to customers by serving them as individuals and by offering them a unique personal relationship with the business. Studies show that web visitors indeed spend considerably more time at personalized than at regular portals and view considerably more web pages. Personalized sites in general also draw more visitors and turn more visitors into buyers.

Personalization therefore would look like a win-win technology for both consumers and online businesses. However, it has a major downside: in order to be able to exhibit personalized behavior, user-adaptive systems have to collect considerable amounts of personal data and ``lay them in stock" for possible future usage. Moreover, the collection of information about the user is often performed in a relatively inconspicuous manner (such as by monitoring users' web navigation behavior), in order not to distract users from their tasks.

Numerous recent surveys have consistently shown that computer users are very concerned about their privacy on the Internet. A large majority of them are hesitant to divulge personal information on the web and are concerned about being tracked online. In order to alleviate these concerns, two different approaches are possible with respect to personalized systems. In one approach, users would receive guarantees that their personal data will be used for certain purposes only. Such guarantees can e.g.\ be given in individual negotiations, in publicly displayed privacy commitments (so-called ``privacy policies"), or they can be codified in privacy laws.

The other approach is to allow users to remain anonymous with regard to the personalized system and the whole network infrastructure, whilst enabling the system to still recognize the same user in different sessions so that it can cater to her individually. Anonymous interaction seems to be desired by users (however, only a single user poll addressed this question explicitly so far). One can expect that anonymity will encourage users to be more open when interacting with a personalized system, thus facilitating and improving the adaptation to this user. The fact that privacy laws do not apply any more when the interaction is anonymous also relieves the providers of personalized systems from restrictions and duties imposed by such laws. Finally, anonymous interaction is even legally mandated in some countries if it can be realized with reasonable efforts.

J\"org Schreck's pioneering book explores the feasibility of this second approach. It discusses existing security methods that would allow users of personalized systems to be unidentifiable for everyone, allow the interaction between users and a system to be unobservable for everyone except the user-adaptive system, and allow different sessions of the same user to be unlinkable for everyone except the system. Moreover, users' data need to be secure during

transport and may be accessed by authorized requesters only. A special difficulty is the fact that personalized systems are storing user data increasingly in central servers whose location must also be hidden to guarantee users' anonymity. On the basis of his theoretical discussions, the author develops a reference model for pseudonymous interaction between users and web-based applications in which full personalization can nevertheless take place.

Schreck’s book offers a wealth of information on the topic of security for privacy in user-adaptive systems, as well as an application-independent technical solution that allows users of personalized systems to remain anonymous whilst still benefiting from full personalization. A number of obstacles may complicate its deployment in practice though. Hardly any readily-available distributed anonymization infrastructures that he requires have as yet been put in place. Anonymous interaction is currently difficult to maintain when payments, physical goods and non-electronic services are being exchanged. Anonymity on the Internet may harbor the risk of misuse, and currently even seems to have an air of disreputability. Finally, web retailers also have a considerable interest in identified customer data as a business asset. While pseudonymous data would be equally helpful for an analysis of shopping behavior and for customer segmentation, they cannot be used for "cross-channel" personalization (sending a web customer a targeted brochure by mail, recognizing him in a brick and mortar store and serving her individually). This becomes increasingly important since the number of web-only businesses continues to decline. The factual deployment of personalized anonymous interaction will thus strongly hinge on social factors, such as regulatory provisions that mandate anonymous and pseudonymous access to electronic services, and articulated consumer demand which gives businesses that offer personalized anonymous interaction a competitive advantage that outweighs its commercial downsides.

Alfred Kobsa
University of California, Irvine