Chapter XVII
Technical Solutions for Privacy-Enhanced Personalization

Yang Wang
University of California, Irvine, USA

Alfred Kobsa
University of California, Irvine, USA

ABSTRACT

This chapter presents a first-of-its-kind survey that systematically analyzes existing privacy-enhanced personalization (PEP) solutions and their underlying privacy protection techniques. The evaluation is based on an analytical framework of privacy-enhancing technologies, an earlier work of the authors. More specifically, we critically examine whether each PEP solution satisfies the privacy principles and addresses the privacy concerns that have been uncovered in the context of personalization. The chapter aims at helping researchers better understand the technical underpinnings, practical efficacies and limitations of existing PEP solutions, and at inspiring and developing future PEP solutions by outlining several promising research directions based on our findings.

INTRODUCTION

Privacy and personalization are currently at odds (Kobsa, 2002, 2007a, 2007b; Teltzrow & Kobsa, 2004; Wang & Kobsa, 2006). For instance, online shoppers who value that an online bookstore can give them personalized recommendations based on what books they bought in the past may wonder whether their purchase records will be kept truly confidential in all future. Online searchers who are pleased that a search engine disambiguates their queries and delivers search results geared towards their genuine interests may feel uneasy that this entails recording all their past search terms. Students who appreciate that a personalized tutoring system can provide individualized instruction based on a detailed model of each student's understanding of the different learning

concepts may wonder whether anyone else besides the system will have access to these models of what they know and don't know.

Various technical solutions have been proposed to safeguard users' privacy while still providing satisfactory personalization, e.g., on web retail or product recommendation sites. Technical solutions for privacy protection represent a special kind of so-called Privacy-Enhancing Technologies (PETs). In (Wang & Kobsa, forthcoming), we propose an evaluation framework for PETs that considers the following dimensions:

1. **What high-level principles the solution follows:** We identify a set of fundamental privacy principles that underlie various privacy laws and regulations and treat them as high-level guidelines for enhancing privacy.
2. **What privacy concerns the solution addresses:** We analyze privacy solutions along major privacy concerns that were identified in the literature.
3. **What basic privacy-enhancing techniques the solution employs:** We look at the technical characteristics of privacy solutions, to critically analyze their effectiveness in safeguarding privacy and supporting personalization.

The rest of this chapter is organized as follows. Firstly, we describe and categorize major privacy principles from privacy laws as well as other desirable principles in the context of privacy protection (we thereby largely follow (Wang & Kobsa, forthcoming)). Secondly, we discuss privacy concerns and how different privacy principles address them. Thirdly, as the central contribution of this chapter, we describe the techniques that have been used in the main types of privacy-enhanced personalization solutions, and how they relate to the major privacy concerns and privacy principles. Fourthly, we discuss findings from this analysis. Finally, we conclude with future research directions.

PRIVACY PRINCIPLES

Privacy legislation and regulation is usually based on more fundamental privacy principles. In our framework, we select a comprehensive set of major principles from our survey of over 40 international privacy laws and regulations (Kobsa, 2007b; Wang, Zhaoqi, & Kobsa, 2006). Any principle manifested in these privacy laws and regulations was included in our framework if it has impacts on how web-based personalized systems operate. Besides, we also define or identify other principles/properties that are desirable for privacy enhancement and personalization. Additional principles may possibly need to be added in the future, as new personalization technologies with new privacy threats emerge or the concept of privacy evolves. Below we list our principles, grouped by their provenance.

Privacy Principles from Privacy Laws, Regulations and Recommendations

1. **Notice/Awareness:**
   - **Clarity:** *Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data* (Kobsa, 2007b; USACM, 2006);
   - **Notice upon collection:** *Whenever any personal information is collected, explicitly state:*
     - *the precise purpose of the collection,*
     - *all the ways in which the information might be used,*
     - *all the potential recipients of the personal data,*
     - *how long the data will be stored and used;* (USACM, 2006)
2. **Minimization:** *Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and*