Chapter XIII
Privacy-Enhancing Technologies

Yang Wang
University of California, Irvine, USA

Alfred Kobsa
University of California, Irvine, USA

ABSTRACT

Privacy-enhancing technologies (PETs), which constitute a wide array of technical means for protecting users' privacy, have gained considerable momentum in both academia and industry. However, existing surveys of PETs fail to delineate what sorts of privacy the described technologies enhance, which in turn makes it difficult to differentiate between the various PETs. Moreover, those surveys could not consider very recent important developments with regard to PET solutions. The goal of this chapter is two-fold. First, we provide an analytical framework to differentiate various PETs. This analytical framework consists of high-level privacy principles and concrete privacy concerns. Secondly, we use this framework to evaluate representative up-to-date PETs, specifically with regard to the privacy concerns they address, and how they address them (i.e., what privacy principles they follow). Based on findings of the evaluation, we outline several future research directions.

INTRODUCTION

Privacy has been recognized as a fundamental human right at least since the seminal treatise of Warren and Brandeis (Warren & Brandeis, 1890). However, it is only in recent decades that privacy issues have attracted substantive attention in society, due to the proliferation and advancement of innovative information technologies such as computers, the Internet, and recently mobile and ubiquitous computing applications. Despite its importance, the concept of privacy is difficult to

grasp. Privacy is a truly multi-dimensional notion. It involves, but is not limited to, cultural, social, legal, political, economic and technical aspects.

Privacy-enhancing technologies (PETs), which constitute a wide array of technical means for protecting users' privacy, have gained considerable momentum in both academia and industry. A number of overviews of the PET landscape have already been published (Blarkom, Borking, & Verhaar, 2003; Burkert, 1997; Camp & Osorio, 2003; Goldberg, 2002; Senicar, Jerman-Blazic, & Klobucar, 2003; Tavani & Moor, 2001). However, most of these studies fail to delineate what sorts of privacy the described technologies enhance, which makes it difficult to differentiate between the various PETs. Moreover, those surveys could not consider very recent important developments with regard to PET solutions. We will therefore focus on these newer solutions here (specifically on privacy policy languages and systems aimed at empowering users in their privacy decisions), and conduct an in-depth examination of the privacy landscape in which these PETs are supposed to make meaningful contributions. More classical PETs such as authentication and identity management systems as well as systems that provide authorization and access control will only be briefly mentioned in the passing. So does another class of very specialized PETs, namely privacy-preserving personalization methods, which have been described in (Y. Wang & Kobsa, 2008).

The goal of this chapter is to provide an analytical framework upon which to chart past, present and future research on PETs. It is our belief that a deeper understanding of their underpinnings will enable us to identify gaps that may still exist, and research directions in developing next-generation PETs.

The remainder of the chapter is organized as follows. Firstly, we provide a review of current privacy-related regulatory requirements and users' privacy concerns and preferences. Secondly, we introduce our analytical framework consisting of privacy principles and privacy concerns. Thirdly, we use this framework to evaluate representative PETs, specifically with regard to the privacy concerns they address, and how they address them (i.e., what privacy principles they

Figure 1. The hierarchy of potential privacy constraints