Chapter LI
Theory and Application of the Privacy Regulation Model

Jaakko T. Lehikoinen
Nokia Research Center, Finland

ABSTRACT

Privacy is one of the most essential topics to be investigated when assessing user acceptance of new applications and services enabling disclosure of personal information. Mobility increases the demand on taking privacy into consideration when designing and developing these kinds of systems. This chapter presents a privacy management model, which facilitates evaluation of privacy aspects of communication technology. The applicability of the model is tested in a field trial that was carried out to assess user acceptance of a mobile social awareness system. Gathered evidence shows that the model helps researchers and designers to deal with privacy aspects of mobile technologies.

INTRODUCTION

Privacy is often seen as a design problem in the fields of human-computer interaction (HCI), computer supported cooperative work (CSCW), and ubiquitous computing (ubicomp). Privacy and its regulation play a significant role in defining acceptability of new communication technological solutions. However, user-perceived privacy threats may not correspond with the real risks related to the technology. For instance, Adams’ (1999 and 2000) studies point out that new technologies are often considered acceptable if the invasion of privacy is not personally faced, even if the technology has major potential privacy risks.

In a mobile domain, privacy as a design factor is even more important than in stationary contexts of use. Mobile devices, such as mobile phones, are carried along throughout the day in a variety of situations. This has itself caused both threats and possibilities in personal privacy regulation. For example, receiving a phone call in a crowded situation may be inconvenient for the recipient due to the fact that one needs to carefully think about how to filter words in the ongoing conversation. On the other hand, mobility makes it possible to
go to a peaceful place to talk with the other party. In addition, text messaging allows a user to have extremely private dialog regardless of a context. However, in many ubicomp scenarios, privacy is a real concern.

Before continuing privacy needs to be defined. It is a complex concept and can be understood only in relation to the surrounding social world. Philosophers and social scientists have produced different kinds of definitions of privacy. Schoeman (1992) has distinguished three most typical definitions. Firstly, privacy can be identified as the measure of control an individual has over information about himself, intimacies of personal identity, and/or who has sensory access to him. Secondly, privacy can be understood as a state or condition of limited access to a person. Thirdly, privacy can be thought as a claim of individuals to decide about dissemination of information concerning themselves. One of the most frequently referred philosophers, Alan Westin (1967), extends the latter definition by saying “Privacy is the claim of individuals to determine for themselves when, how and to what extend information about themselves is communicated to others.”

Privacy can also be defined as a border between society and one’s personal affairs (Soppera & Burbridge, 2004). Marx (2001) uses the following border categories: natural borders (governed by senses and physical boundaries), social borders (the expectation that information is shared within a social group), spatial or temporal borders (separate aspects of one’s life), and ephemeral borders (based on the assumption that information is not preserved longer than expected). He also argues that the terms public and private are more ambiguous than what is generally understood.

Altman (1975), whose theory is used as a foundation for the privacy regulation model presented in this chapter, brings yet another definition of privacy; he understands privacy as a dialectic and dynamic boundary regulation process. In interpersonal relations, especially in face-to-face settings, the dynamic boundary regulation process means that an individual manages social interaction and personal privacy through different behavioral mechanisms, such as verbal behavior (content of speech), paraverbal behavior (voice intensity), personal spacing (distance from others), and territorial responses (personalizing and controlling geographical areas and objects). Depending on the circumstance, an individual uses these mechanisms in different ways; one mechanism may substitute the other according to changes in the social context. Altman also states that behavior may change in a process of time, thus the process of privacy regulation is dynamic.

Altman (1975) uses the concepts of desired privacy, interpersonal control mechanisms, and achieved privacy to illustrate privacy regulation process. Achieved privacy represents the actual amount of interaction with others and it may be more or less than the desired privacy, or it can match it. An optimal level of privacy exists, when the achieved privacy equals the desired privacy. When the actual amount of interaction is less than desired, Altman talks about isolation and when it is more, he uses the term crowding. The terms inputs and outputs describe people’s behavior in a social situation. For instance, listening to other’s conversation represents inputs from the others and attending actively to a discussion, and presenting one’s own views to the subject matter represent the outputs from self to others. To conclude, in a state of desired privacy the inputs and outputs are in a level that an individual wishes.

Privacy is often seen as a design problem in the arena of communication technological research and development. Palen and Dourish (2003) bring out two essential factors affecting privacy management; recordability and unawareness of the final audience. The first factor refers to the fact that mediated communication can be recorded, which means that the mediated information can be retrieved and re-used after the information disclosure. This makes the control of personal information difficult or even impossible once it has been disclosed. Recordability and the fact that mediated communication is, in most cases, taking place in such environments where the communication parties cannot see each other, cause unawareness of the final audience. One of the most typical examples addressing these two cases is forwarding someone’s e-mail without asking permission from the original sender.