Pers Ubiquit Comput (2004) 8: 389–390
DOI 10.1007/s00779-004-0306-7

EDITORIAL

Chris Schmandt · Mark Ackerman

Personal and Ubiquitous Computing

Issue on privacy and security

Received: 10 December 2003 / Accepted: 10 June 2004 / Published online: 23 October 2004

These days, it seems that wherever computers are, privacy and security problems arise. From identity theft to feelings of invasion by spam email to evidence in criminal cases from surveillance cameras, privacy and security are hot topics, even in the popular press.

There are many aspects of the ''privacy problem'' and the ''security problem.'' When Chris recently opened a bank account for his daughter, he witnessed many of them in an environment that was far from ''ubiquitous computing.'' First, she refused to give the bank clerk her social security number (a financial ''national identity number'' in the US) because she had learned that one must safeguard this information to protect against identity theft. The clerk, revealing as much information as many ''input error'' Web pages, simply said, ''I can't open an account for you without a social security number.'' Chris patiently explained to his daughter that, legally, the bank was required to report certain information to the government. These data were indexed via the social security number.

Then, the clerk wanted to know the mother's maiden name (a standard question in the US for banks). Chris' daughter got upset, since her mother's ''maiden name'' was her surname; she had never changed it on getting married. (Even if she had, she may have changed it back upon divorce; privacy expectations change with social customs.) This time the clerk was able to provide some explanation: this was supposed to be personal information that could be used to verify her own identity in future transactions with the bank; in other words, it was a password to protect her account. But, as Chris' daughter pointed out, it would be easy for someone, especially with Web access, to discover her mother's current last name. The clerk suggested that any other bit of personal information could be used instead of the maiden name. It then became clear that the bank forms (infrastructure) did not have any way of recording the appropriate challenge which would remind her of the appropriate response in the future (the ''password problem''). The whole interaction left several people very suspicious of the bank, its security, and their privacy.

Now, in this scenario, the computation was hardly ubiquitous! What happens in the brave new world envisioned by those of us who publish in this journal? Ubiquitous computing implies that computing is everywhere, and perhaps, so much a part of our digital environment that we cease to notice it. Since (digital) privacy seems to ''happen'' at the intersection of computers and people, and privacy is already a major concern even in the early stages of ubiquitous computing, we seem to have a major headache brewing in the near future. Also, the security issues that are already too familiar will increase as computers become invisible and ubiquitous. The sooner the research community addresses these serious concerns, the more likely we are to solve the problems, or more likely, come up with compromise solutions acceptable to most users.

If ubiquitous computing is to be user-centered, the research community must tackle the human–computer interface (HCI) issues inherent in both privacy and security. For users, security and privacy are deeply intertwined. While at times they are very distinct (and it is helpful analytically to separate them), users do not always distinguish between them in considering their data or in envisioning pervasive environments. Several of the papers in this issue reinforce that premise. In any case, it is clear that user-centered pervasive environments will require new ways of looking at privacy and security.

In this issue of *Personal and Ubiquitous Computing*, we present a selection of papers dealing with various aspects of privacy and security. Clearly, it is a rather expansive domain covering many different aspects of ubiquitous computing, and this is reflected in the

C. Schmandt
Media Lab, MIT, Cambridge, MA, USA

M. Ackerman (✉)
Department of Electrical Engineering
and Computer Science and School of Information,
University of Michigan, Ann Arbor, MI, USA
E-mail: ackerm@umich.edu

breadth of our contributions. All of the papers here, nonetheless, present the complexity of the tradeoffs inherent in privacy and security within pervasive environments. Allowing users to determine or understand these tradeoffs will be difficult. Requiring them to do so may make adoption improbable. These papers begin the arduous HCI effort of understanding how to tackle this complexity so as to provide users with something they can comprehend and control.

Dourish, Grinter, de la Flor, and Joseph examine security as experienced by users in contrast to much of the security literature. The authors note that users often consider security to be the dual of privacy—security is there to protect their data and prevent misdeeds. The paper goes on to examine how the experience of security in everyday activity differs from the mechanisms themselves. The paper is a fascinating read in how users "construct" technology and social mechanisms in order to provide themselves with the assistance they need. The authors also point out how users construct rationalizations to explain breakdowns.

Blythe, Wright, and Monk provide an insightful examination into the privacy issues with regard to surveillance. Their ethnographically based study examines the elderly in a British community. The paper points out the importance of considering demographics—particularly age—in considering privacy and its ties to physical security. For example, some seniors do not want assistive technology within obvious sight of a window, since it marks their houses as inviting targets. The paper goes on from this ethnographic base to consider potential surveillance devices and their demographic and societal effects. The paper concludes with an interesting note about the role that the changing percentage of elderly in the population might have on societal considerations about privacy and physical security.

Roussos and Moussouri consider a possible ubiquitous application; that of grocery shopping in an intelligent environment. Based on their user study, they bring out the important privacy and trust dimensions that will prevent or retard adoption. They found that many of their consumers, for example, do not want one of the standard ubiquitous computing scenarios; kitchens that signal grocery stores as to their needs. In fact, some prospective consumers saw such an application as a flagrant privacy violation, although others were willing to examine the potential benefits from the data transfer. Roussos and Moussouri stress the importance of aligning the interests in data capture as well as maintaining users' control over data transfer.

Ackerman explores issues related to a technical mechanism for ensuring privacy in the exchange of personal information over the Internet, which he terms "labeling protocols," an example of which is the MIT/W3C Platform for Privacy Preferences Project (P3P). These protocols allow an interchange as to what may or may not be done with particular pieces of private data. He argues that some such protocol is essential, but that bringing the full protocol and components out to the user will probably not be a viable solution for pervasive computing. This is similar to the findings of Lederer, Hong, Dey, and Landay in their evaluation of their original system. Ackerman considers the lessons from the P3P experience, particularly with regard to pervasive environments.

If end users are to have control over and confidence in privacy protection mechanisms of software presenting personal information to others, this must be expressed in the user interface. This raises the serious question of the level of granularity at which users wish to control what is revealed about them, and how those choices are expressed. Lederer, Hong, Dey, and Landay address these issues as a set of design guidelines that are motivated in part from the failure of their earlier system. It is refreshing for researchers to admit their mistakes, and we can learn from their five guidelines, which provide simple yet general coverage over a wide range of privacy issues, together with supporting examples.