# Using Context Information and Trust Relations to Build Privacy Enhancing Technologies

**Carsten Röcker**
Fraunhofer IPSI, AMBIENTE – Smart Environments of the Future
Dolivostraße 15, D-64293 Darmstadt, Germany
roecker@ipsi.fraunhofer.de

## 1 INTRODUCTION

Adequate privacy protection is a widely discussed topic since the early days of computing. Although guidelines for privacy enhancement in pervasive computing exist for quite some time [1,2], the implementation of these measures into systems is a very rare sight. To obtain a deeper insight of the requirements for privacy enhancing technologies and as a basis to build appropriate systems we started addressing this topic by investigating the demands of potential users. Based on the results we developed two prototypes which will be introduced in this paper: the Personal Aura and PRIMA. The Personal Aura is an artefact which enables users to control their appearance in a smart environment. PRIMA is a program for dynamic privacy management in public spaces based on context information and individual trust settings.

## 2 USER NEEDS AND PRIVACY

As a foundation for the later development of privacy enhancing technologies we carried out an extensive survey to investigate potential user needs. The emphasis of the survey was on privacy-related questions, especially on the importance of privacy and the acceptance of system-controlled privacy measures. Since the majority of future users will lack a detailed technical knowledge about the environment they inhabit, we aimed at a target group outside the research community to get representative results.

The survey shows that 45.0% of all users rate privacy "important" and 32.8% as "very important", while at the same time over one third (36.6%) never changes their passwords. The results stress again the important role of privacy in ubiquitous computing environments, but also indicate a large discrepancy between users' desire to protect privacy and their willingness to take relevant measures.

Moreover, we investigated the acceptance of privacy-enhancing technologies in group situation as well as the desired degree of system support regarding privacy protection. Our aim was to understand if and how user users want to be supported in protecting their privacy in dynamic group situations. Therefore we asked the participants to imagine a situation where they work with personal data on a large public display and other users are approaching the public display area. In such a situation 83% of all users would wish for an automatic reaction of the system to help protecting their privacy. Out of this group one third favors to be warned and would like to take necessary steps on their own, while the other two thirds prefer a system that automatically hides private data (see Fig. 1).

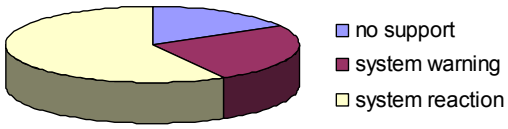


Figure 1: Desired system support regarding privacy protection in group situations.

While automated privacy support seems to be favored by the majority of users, most of them are very reluctant to provide all the necessary information to auto-configure their privacy settings. For example less than 10% of the users would accept the collection of biometric information even it is used to reduce their workload.

The results show, that system developers must not rely on active user participation when implementing measures to safeguard user privacy, but should aim at designing easy and intuitive ways to handle personal privacy in everyday situations.

## 3 THE PERSONAL AURA

In real life, every person adopts different social roles, depending on the present situation and current social environment. A person usually has several social roles which constantly change during the day and over the person's lifetime. For example, the same individual can take up the roles of a family father, project manager, supermarket customer and member of a sports club during his daily routine. Within its professional role there might exist different social profiles depending on project or team requirements. In all this roles an unintentional disclosure of personal information might result in serious privacy infringements.

### 3.1 Concept and Requirements

The purpose of the Personal Aura (PA) artefact is to put users in control of their appearance in a smart environment. In most sensor-enhanced environments users are automati-

cally and irrevocably identified in the moment they enter the monitored areas. With the Personal Aura we are enabling persons to decide on their own whether they are "visible" and in which "social role" they want to appear.

The development of the PA artefact focuses on the design of easy and intuitive user interfaces for recurring changes of personal profiles. Continuous changes over longer periods (e.g., changes in the personal preferences over time) have to be regarded more as a problem of adequate data management rather than UI design and hence will not be addressed here.

Context and location based services usually require identification of the user within his environment and towards other individuals or artefacts. The PA artefact aims at enhancing the user's awareness for tracking and identification events by giving optical and acoustic feedback. Short-time deactivation is realized through a "privacy switch" that allows invisibility without disassembling the artefact.

Since the Personal Aura also enables access to personal as well as confidential information, providing adequate security is a major issue. We meet these requirements by adopting the concept of key and lock. Only if two matching pieces are put together you get full functionality. Therefore, every ID Stick has a unique profile of rails on its surface. These rails work like a key and fit only in one ID Emulator which guaranties, that a misuse by a third party isn't possible.

### 3.2 Technical Realization

The PA artefact consists of two matching parts: the ID Emulator which is able to "emulate" different identities or social roles, and the ID stick containing a unique identity and optional personal information (see Fig. 2).

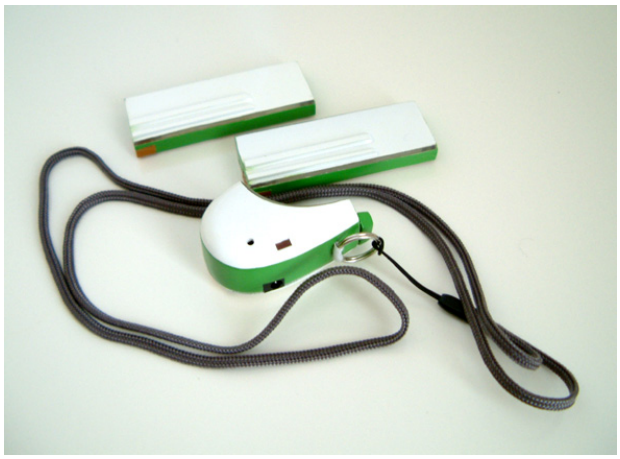

Figure 2: Personal Aura with two different ID sticks.

All prototypes are based on active RFID transponders and allow detection ranges of up to 30m within buildings. The existing circuit boards were modified and integrated in the two pieces of the PA artefact. One comprises the battery, antenna and input/output controls, the other contains the transponder electronics, identification information and memory. To display the status of the PA artefact all of the prototypes are equipped with an additional LED to signal power-on. While the original transponders signal read/write access via a LED, a part of the transponders for the PA artefact are modified to give acoustic feedback. This should enhance peripheral awareness even if the artefact is not constantly in the user's field of vision.

## 4 PRIMA

The demand for active privacy support in ubiquitous computing environments led us to the development of PRIMA, a system that enhances privacy in group situations based on context information and trust settings. In the first version we focus on context-dependent information concealment for large displays in public areas.

Our goal was to give users the freedom to work on large public displays without the fear of privacy infringements through passing people. To guarantee satisfactory privacy protection and at the same time minimize the interruptions during the work process, it is essential to know which information should be hidden from whom and when.

The necessary information about nearby individuals is collected via a two-step sensing infrastructure. Infrared and active RFID sensors constantly monitor the area around each public display. People approaching a public display are detected by the infrared sensors and are simultaneously identified according to the current settings of their Personal Aura artefact. If people have deactivated their PA, the data collected from the infrared sensors still allows to detect the presence of people in the vicinity of the display.

The software consist of three components. The main component is responsible for hiding applications and files depending on the proximity of other users and individual privacy settings. These settings are managed in the second component, the "policy manager". Each application and document can be classified individually or assigned to a group with predefined privacy settings. Additionally, it is possible to use these settings in combination with arbitrary catchwords. The policy manager also allows to define and edit the trust levels for single users or user groups. This enables users to easily define rules like: hide all websites that contain the words "music" or "football", if the individuals "a,", "b" or the group "project team c" is near the display. The information about running programs and open documents are provide by the third component called "file system watcher". It permanently monitors the local file system and transmits all relevant changes to the main program.

## 5 REFERENCES

[1] Victoria Bellotti, Keith Edwards. Intelligibility and Accountability: Human Considerations in Context Aware Systems. HCI. Special Issue on Context-Aware Computing, Vol. 16, 2001.

[2] Marc Langheinrich. Privacy by Design - Principles of Privacy Aware Ubiquitous Systems. In: Proceedings of Ubicomp 2001, Sep. 30- Oct. 2, 2001, Atlanta, GA.