Paper from the Conference "INTER: A European Cultural Studies Conference in Sweden", organised by the Advanced Cultural Studies Institute of Sweden (ACSIS) in Norrköping 11-13 June 2007. Conference Proceedings published by Linköping University Electronic Press at www.ep.liu.se/ecp/025/. 

# Threat Awareness – Social Impacts of Privacy Aware Ubiquitous Computing

Alexander De Luca and Heinrich Hußmann
Media Informatics Group, University of Munich, Germany
alexander.de.luca@ifi.lmu.de, heinrich.hussmann@ifi.lmu.de

At first glance, privacy and ubiquitous computing seem to be highly incompatible, due to the ubicomp characteristic of being invisible. There are projects, trying to overcome this problem with different feedback mechanisms. In current literature, this approach is often referred to as privacy mirrors. The goal is to provide privacy awareness. It means making users aware about how their data is used by a specific service. However, there is little scientific work on the social impact of privacy awareness. That is, if privacy awareness is useful, accepted by the users and if it changes their usage behavior. Therefore, in this work, we examined the influence of privacy awareness on users to find the answers. We performed a user study with a privacy aware mobile service and conducted an online survey, which lead to interesting results, which we will present in this paper.

## Introduction

Ubiquitous computing, more than any other technology, originates privacy risks. This makes privacy protection even more important in this field of computer science as stated in (Langheinrich 2001). One of the problems is outlined by Jiang et al. (Jiang et al. 2002). It is called the Principle of Minimum Asymmetry and describes privacy problems in ubiquitous computing that arise due to asymmetric information flows between data owners and data collectors or data users respectively. In short: data owners disclose more information than they get in return. Solutions for this problem rely on decreasing data flows from the owner or increasing them to the owner of the data, which in the second case means providing feedback mechanisms (Jiang et al. 2002). Hence, this is how most projects are trying to overcome the ubicomp privacy problems. In current literature and projects, this approach is mostly referred to as privacy mirrors like described by Mynatt (Mynatt et al. 2001) and Ngyuen (Ngyuen et al. 2001). The goal is to provide privacy awareness. That is, making users aware about how their data is used by a specific service or system.

One of the first questions that come to mind when thinking about privacy awareness is the kind of information that has to be provided to users. That is, which information is useful and which is not. The work done in (Ngyuen et al. 2001) tries to give an answer to this question. The authors Ngyuen et al. define Privacy Mirrors, a framework that describes different characteristics that have to be considered when providing privacy in socio-technical systems. These characteristics include for example history and feedback. One early approach of a privacy aware system is called Privacy for the RAVE environment (Belotti et al. 1993). It uses physical hints for users to show them what is going on in the RAVE computing system. For example they put up figures of camera men in rooms with video surveillance to make the people aware that in this room they will be filmed. It is one of the earliest works containing concrete implementations of privacy aware interfaces or better privacy hints. Privacy at the user interface level has also been addressed in other projects. In Ubi's World (Heckmann 2003), Dominik Heckmann describes a system that uses a website to configure the access rights on every possible data belonging to a user by three different criteria: Access, Purpose and Retention.

For P3P (W3C 2002), a privacy description language for websites, there are various implementations available that try to protect the users' privacy based on P3P policies. Even the Internet Explorer provides a small implementation for P3P, hidden in the options menu: A small scale that can be used to edit the amount of privacy protection regarding cookies. A more elaborate P3P tool is Privacy Bird (CMU 2006), which integrates into the Internet Explorer and signals the users whether a website's P3P policy fits their privacy settings or not. For that, it uses different colors and sounds. The Orby Toolbar (YOUpowered 2001) works very similar, but provides a so-called trust meter which allows more fine-grained comparison of policies to settings.

When speaking about ubiquitous and pervasive computing, not only invisibility but also mobility is an important characteristic. Thus, mobile devices seem to be appropriate for displaying privacy related information because users may permanently switch between locations. A first attempt on using mobile devices for providing privacy awareness is found in the PaWS system (Langheinrich 2005) by Marc Langheinrich which comes with a small PDA interface for viewing service descriptions and a list of active services in a ubiquitous environment. Additionally, it enables the users to decline services if they think they might harm their privacy. However, there is little scientific work on the influence of privacy aware technologies on the users respectively the social impact, even though it raises several questions including: Do users need and want privacy awareness? Does privacy awareness

increase the complexity of services? Will users change their way of thinking about services and service usage because of privacy awareness?

Therefore, in this work, we examine the influence of privacy awareness on users to find answers to questions like these. For gathering the needed data we created a privacy aware mobile computing system at our labs and performed a user study with it. Privacy awareness in this work is defined as providing mechanisms to make the users aware about how their data is used at service side and also to provide them with the possibility to control their data. Thus, if a service is used, be it actively or passively, users can retrieve information about the data collection practices from the service, can decide how strict services are handled, can manually cancel services etc. When conducting the user study, we noticed an effect that we called threat awareness. This will be outlined later in this paper. Additionally, we conducted an online survey which contributed to getting a basic set of interesting information.

In this paper, we will present the results of our work. Therefore, we describe the scenario of our prototype as well as the prototype itself. To see what the participants of the user study had to do and how we got the here presented results, we will outline the user study and its different tasks as well as the online survey. After that, the results will be presented in detail.

## Scenario and Privacy Threats

As mentioned, the goal of this work is to examine the current state of awareness about privacy threats in ubiquitous computing and thus, the need and acceptance of privacy awareness mechanisms. Furthermore, the goal is to analyze possible social impacts of privacy awareness. Therefore, a prototype was required that on the one hand is easy to use and on the other hand relies on normal data collection practices of current services. This means that designing a service that behaves extremely badly regarding privacy laws and common practices would have been contra-productive because it would stimulate reactions that cannot be compared to state of the art services. Therefore, for our prototype, we chose a scenario, which is comprehensible and useful for the participants of possible user studies. In our case, we planned to perform the studies with students from different faculties and thus, a university scenario seemed to be appropriate. The requirements for the prototype as well as for the scenario are to confront the participants with the disclosure of their personal data and with privacy aware user interfaces.

### *The University Scenario*

The scenario takes place at a university's facilities. Information about lectures for the running semester is available online as well as offline on small posters placed all over the buildings. These posters contain a short description of the lecture, its dates, the lecturer's name, and other information. Additionally, they are enhanced with RFID tags, which contain data for a mobile service that allows students to automatically create their timetables just by adding and removing lectures with their mobile phones by interacting with these tags. The tags themselves are not visible but appropriate icons are displayed on the posters that indicate their functionality as shown in Figure 2. Touching the "add lecture" tag respectively the "remove lecture" tag will invoke these functionalities. Furthermore, print terminals offer a service that can be used to print the timetable directly at the university building.

### *Privacy Threats*

The here explained services contain several privacy threats. They are dealing with personal data of the users for different reasons. For using the services, the students have to be registered at a central server to retrieve a username and a password. The lectures are stored with references to the students to be able to create the corresponding lists and the timetables for each student. That is, the service providers will be able to retrieve full knowledge about

which student is visiting or interested in which lecture. To a greater extent, this means having the knowledge about when a student will be at the university and thus, will not be at home, which is an information, criminals might be interested it. This shows, that besides the normal privacy problems occurring with a data collection service, further problems might occur, depending on the kind of service. Since most users do not even know about the normal problems, providing privacy awareness seems a logical step in future service provision technologies and must be examined on its impact on the users. How privacy awareness has been realized for our prototype will be described in the next chapter.

## Prototype

### *Paper Prototype*

The prototype for the above mentioned scenario has been implemented in two steps. At first, a paper prototyping has been conducted to validate the services and improve the interfaces as shown in Figure 1. Thus, the interfaces for the implemented prototype were built upon the improved versions from the paper prototyping. Improvements mostly relied on comments of users. Most of these were marginal problems like confusing labels for buttons etc. Renaming them was appropriate in adapting the prototype.

The prototyping has been conducted with 11 people. The youngest user was 25 and the oldest 32 years old. The average age was 27 years; 8 were male and 3 female. Only 42% of them had ever used a context sensitive service before. All screens of the mobile application were created in a painting application and printed to fit a mobile phone's screen size. For the test they were attached to the screen of a real mobile phone as depicted in Figure 1, for providing realistic interaction feelings to the users. The participants of the prototyping performed the same tasks and answered the same questionnaires that were planned and conducted for the final user study. This will be outlined later in this paper.


**Figure 1: Users performing the Paper Prototyping.**

Of course, also the privacy awareness features have been validated in this step. As mentioned before, the scenario offers different control functionalities to the users. At first, each user can define privacy settings which are compared to the services and will alert the user in case of a mismatch. In case of an alert, the users are provided with an error message and a service description and can then decide whether to accept the service anyway or to decline it. The error message includes information on why the settings did not match the service description. Additional privacy awareness features contain for example a list of accepted services, which can be used to decline services even though they have been accepted previously. This will invoke the deletion of all user –service related data inside of the system.

***Prototype Implementation***

For the final service implementation, a web service architecture has been chosen. A service offers an interface that can be used by any client to invoke the service's functionalities. If a client is starting the service for the first time, the server transmits its privacy policies to the client, which describes the service including its data collection practices. These policies are used for automatic comparison to the user's settings and are translated to a human readable format for displaying them to the user. This translation is also part of the privacy awareness features.

The client on the mobile phone is implemented with Java Micro Edition and connected to an external RFID reader via Bluetooth as shown in Figure 2. The posters, which were already used during the paper prototyping, have been enhanced with RFID tags and configured to interoperate with the client respectively the services. The front as well as the back side of one of the posters can be seen in Figure 2.


**Figure 2: Prototype setup: Mobile phone with RFID reader (left). A poster with RFID tags (right).**

## User Study

Like the paper prototyping the final user study took place at a normal building of the university, that is, a location in which this service fits exactly. The participants had to perform three different tasks:

1. Edit the privacy settings of the mobile application to fit their preferences.
2. Interact with the posters and add at least one of the lectures to the timetable.
3. Print the timetable at one of the available printing terminals.

**Figure 3: Participants performing different tasks of the study. Printing (left) and adding lectures (right).**

Additionally to the practical part, the participants were asked a questionnaire before as well as after performing these tasks. To avoid learning effects, no users from the paper

prototyping were accepted for participation at the final study. There were 11 participants, 8 male and 3 female. The average age was 27 years. The youngest was 22 and the oldest one 46 years old. All but one were students of different areas including informatics, design and medicine. The average time of the interaction with the prototype was 30 minutes. Figure 3 shows three different users performing some of the tasks.

## Results

The results presented in this section are mostly based on the outcome of the user study. To get a broader base for the general questions, we additionally performed an online survey on this topic. 71 participants filled out this survey. 18 of them were female and 53 male. The average age was 27 with the youngest participant being 20 and the oldest 57 years old. For the questions we decided to use a Likert scale from 1 (I do not agree) to 5 (I highly agree).

### *Views on Privacy*

The elemental factor in designing privacy aware systems is to provide privacy to its users. Even though there are privacy regulations like the European Commission directive 95/46/ec (European Commission 1995), the term privacy cannot be defined. This is deeply rooted in the users themselves. Users experience privacy in their context of living and their affectations. The aforementioned questionnaire contained a question, which kind of personal data the participants considered to be private data. The results were extraordinary manifold. They reached from “only my bank account information” to “all my personal data”.

As a consequence, this fact highly influences privacy awareness and privacy visualization in general. When users say “I don’t want the system to warn me about thing I do not care about”, they mean it. This means, that adaptability is an important aspect of a good privacy aware system because it not only enables the users to have partial control over the system it also offers them the possibility to adapt it to their personal privacy. Accordingly, providing privacy settings or privacy preferences is inalienable for a privacy aware computing environment.

### *Acceptance of Privacy Awareness*

The evaluation of the questionnaires showed that there is a high approval for the idea of introducing privacy aware user interfaces to mobile devices. All participants agreed on the importance of protecting the users’ privacy with 4.7 and the benefit of privacy awareness before and after performing the tasks with 4.6. This has also been approved by the online survey. Users rated that they would want to be notified of privacy threats (4.4) and that they would prefer privacy aware services to unaware service (4.7). Whereas asked for reasons, they mainly stated that in their opinion, privacy awareness would increase their trust in a ubiquitous computing system and in a service. For the users it seems also important that privacy awareness provides some sort of control about the personal data.

When interacting with the prototype, participants also noted disadvantages of such a system. They rated it more complex then normal approaches since it requires additional interaction with the application (notification, visualization, etc.). But all agreed that the advantages would legitimate the disadvantage since it is “just some more clicks” as one user stated. Nevertheless, for human computer interaction, even more on small devices, this issue has to be handled carefully. This means proper interface mechanisms are required to keep the complexity at a minimum.

### *Threat Awareness*

The most interesting and unexpected result during the user study was found regarding the question about user concerns. The participants were asked whether they would be concerned

about their privacy when using ubiquitous services. The question was asked as well before as after performing the tasks. When comparing the resulting values, we found out that users were not concerned about privacy issues before they performed the tasks and the average result of rating their concerns was only 3.4 (2.7 during the paper prototyping). But after they performed the tasks, the average rose to the high value of 4.3 (4.4 during the paper prototyping). We call this effect Threat Awareness. It describes that nowadays, most users do not know about the technological possibilities of computing systems and thus, they do not know about privacy threats. Furthermore, it seems there is hardly any comprehension about data collection practices. And in contrast, there is a huge amount of inappropriate trust in service providers.

Since our prototype is privacy aware, every service had to reveal such information to the user by the privacy aware interfaces. Therefore, users got a deeper understanding of the services since it showed them possible privacy threats. Consequently, privacy awareness does not only increase the users' security while using ubicomp services, it also increases their understanding of possible threats and moreover about the background processes of ubicomp.

As mentioned above, we claim that the majority of people has no understanding of what is going on in current services and of what consequences may be implied when using them. This gap is even bigger if it is about ubiquitous computing. In the online survey, we found out that even for more apparent privacy threats, the knowledge is minimal. Surprisingly, 30% of the participants said they had never noticed privacy warning signs like camera surveillance in public spaces. When asked for specific notification signs as depicted in Figure 4, the number was even higher. Therefore, we claim that privacy awareness is also an important step in providing the comprehension about the new possibilities in the computing environment.

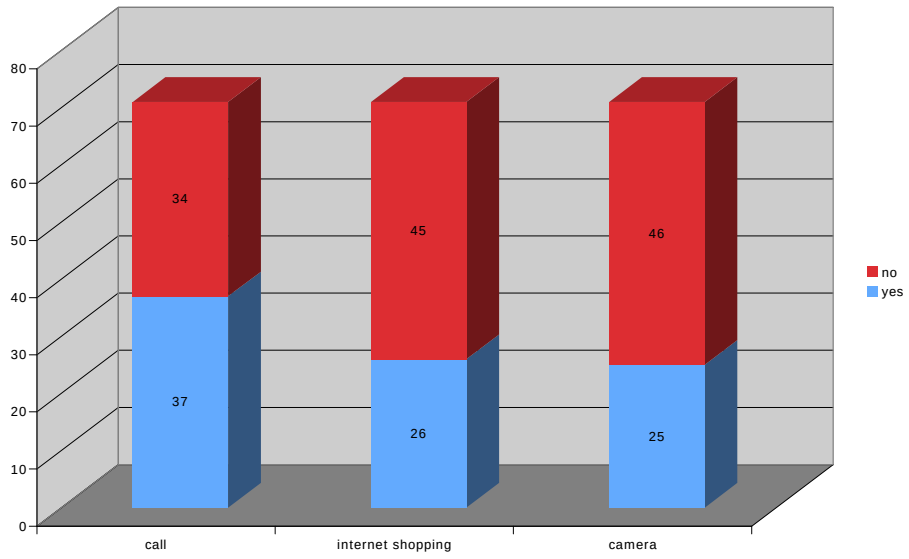


**Figure 4: Participants asked if they ever noticed warning signs or notifications in specific situations.**

## Discussion and Summary

Privacy awareness is changing the way that users experience services and in which they interact with them. Even more, if these services are executed in a ubiquitous computing environment, which enables the collection of various personal data without the users consent. People get aware about the privacy threats surrounding them and change their attitude about the usage of such services. We call this effect Threat Awareness. This is the most interesting thing we learned, when we performed the work for this paper. Additionally, we were also

able to show, that until now, there is only little understanding of privacy threats and that privacy awareness mechanisms are perfectly capable of increasing this knowledge. This may not be something that service providers like, but it definitely is for the good of the users. Also, privacy awareness may have the potential of increasing service quality in general since it could lead to a privacy-quality-gap between privacy respectful and privacy disrespectful services. This is one of the reasons, why users prefer privacy aware to unaware services and why the users in general very well accept privacy awareness.

To learn these things, we implemented a privacy aware service environment at our labs and performed a user study with it. For the more general questions (e.g. about the users' general privacy threat knowledge), we additionally performed an online survey, which has been filled out by 71 participants. This has been done to get a broader data set on these topics. Since the Threat Awareness effect has been found while working with one prototype, the next logical step will be to perform the user study with different privacy aware systems and services and a bigger amount of participants. Therewith, it can be found out whether the effect can be applied to privacy aware services in general or if it is an effect of the study setup. The effect may also vary if the amount of privacy awareness is changed or if different user interfaces are utilized.

## References


Bellotti, V., Sellen, A. Designing for Privacy in Ubiquitous Computing Environments. In: ECSCW 93. Milan, Italy. September 1993.

CMU Usable Privacy and Security Laboratory. Privacy Bird. 15.03.2006. http://www.privacybird.org (cited 8 May 2007).

European Commission. Directive 95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, November 1995.

Heckmann, D. Integrating Privacy Aspects into Ubiquitous Computing: A Basic User Interface for Personalization. In: AIMS 2003. Seattle, USA, October 2003.

Jiang, X., Hong J. L., Landay, J. A.. Approximate Information Flows: Socially-based Modeling of Privacy in Ubiquitous Computing. In Ubicomp 2002. Goteborg, Sweden 2002. pp. 176-193.

Langheinrich, M. Privacy by design – principles of privacy-aware ubiquitous systems. In proceedings of Ubicomp, pages 273-291. Spring LNCS, September 2001.

Langheinrich, M. Personal Privacy in Ubiquitous Computing – Tools and System Support. Dissertation, University of Bielefeld, Bielefeld, Germany, 2005.

Mynatt, E., Nguyen, D. Making Ubiquitous Computing Visible. CHI 2001. Workshop: Building the Ubicomp User Experience.

Ngyuen, D., Mynatt, E. Privacy Mirrors: Making Ubicomp Visible. In CHI 2001. Seattle, WA.

W3C. The Platform for Privacy Preferences 1.0 (P3P1.0) Specification. 16.04. 2002. http://www.w3.org/TR/P3P/ (cited 8 May 2007).

YOUpowered Inc. Orby Toolbar. 2001. http://www.pixelcode.com/youpowered/products_orbyintro.html (cited 8 May 2007).