Perceived Privacy in Ambient Intelligent Environments

Maddy D. Janse[1], Peter Vink, Iris Soute, Heleen Boland

Philips Research, High Tech Campus 34, 5656 AE Eindhoven, The Netherlands,
maddy.janse@philips.com

Abstract. User studies were conducted to explore the different conditions and constraints that affect people's perceived privacy in a networked home environment. Context-aware applications for an extended home environment provided the setting and conditions for inducing privacy-sensitive situations. A presence detection and sharing system was placed in people's homes to conduct a longitudinal field test under realistic conditions. People's preferences for masking and hiding information that is being shared were investigated for different types of applications. The results showed that people use various mechanisms to preserve their social privacy. They share their personal information only with a small group of close relatives and friends and only when there is a clear benefit for them. Maintaining control over the level of information that is being shared, is crucial. Design guidelines were derived from these results to address end-users requirements with regard to perceived privacy.

Keywords. Ambient intelligent systems, networked home environment, perceived privacy, context-aware applications, user studies.

1 Introduction

Applications in extended networked home environments are intended to facilitate the communication between users of different households and to provide them with a feeling of a shared ambiance. Connecting people in this way influences their social relationships. Home, as we know it, is a place where people can retreat from society and its social rules. Extended home applications induce intrusions in this familiar and trusted environment. Since ambient intelligent systems are by definition unobtrusive and embedded in the user's environment, users might easily forget their existence and unwillingly have their privacy violated. "Perceived privacy" or how end-users perceive that the system affects their privacy, is one of the key aspects for the acceptance of ambient intelligent systems by users. It is also one of the most complex problems to handle. It is about 'how, when, and to what extent' data about people are revealed to other people within a dynamic social context.

The major challenge with regard to ensuring people's privacy in an ambient intelligent environment is to account for the implications induced by acquiring, collecting and inferring personal information of users. The tracking and collection of significant portions of users' everyday activities and interactions are required to compose user profiles and to model the context in which these user behavior's and interactions occur. The disclosure of this private information to other parties, whether it be friends or family, service providers or commercial traders, in return for benefits like receiving a desired personalized and context-aware service or specific activities being taken care of, induces a delicate balance that needs to be maintained (1) and protected.

An empirical approach was taken to address this problem in which exploratory, field and concept studies were conducted to acquire user input for design guidelines for application development and for specific application implementations. The context in which these studies were conducted was provided by the application scenarios that were developed in the Amigo project (2) for the networked extended home environment. These studies are presented in the following sections.

2 Privacy Handling in Everyday Communications

An exploratory study was conducted to obtain implicit information about people's attitudes towards privacy sensitive situations that might be induced by having an operational networked extended home environment (1). Romero (3) investigated which types of communication media are currently being used, the frequency in which they are used and the contact purpose for which they are being used. Most commonly used media types were mobile phone, home phone, MSN, e-mail and regular mail. They were used for different contact categories based on their content: practical, social, emotional and special occasion. These categories were used as the primary structure for addressing the following questions: what are the privacy needs for the different types of communication media and how do people currently handle their privacy needs?

2.1 Methodology

To acquire information about how people handle their privacy in everyday communications, an ethnographic methodology was used in which people were asked to keep a diary for one week to record all their home-based communications. After that period a semi-structured interview was conducted. The diary served to log all types of one week's communications and to facilitate the interview by having explicit cues available. It excluded face-to-face meetings and communications outside the home. The interview focused on what types of information people regard as highly sensitive and how they make sure that their moments of communication are not disrupted. A storyboard for guided exploration was used to structure the interview. The storyboard presented different potentially privacy violating situations, for example, presence notification, automatic identification and automatic intervention. To accomplish a comprehensive coverage of everyday communication, participants were selected from a wide range of age and social situation. The participants (n=6) were: (a) an 88 year-old grandmother with a large family of children and grandchildren and living with her husband; (b) two middle-aged men (39 and 41) with a young family; (c) a woman, aged 25, in a single household; (d) one man, aged 27, living with a girlfriend; (e) a teenage girl (age 15) living with her parents and a sister. This sample of participants covering a wide range of social conditions was used to explore the handling of privacy in daily communication situations in a qualitative way.

2.2 Results and conclusions

Privacy sensitive communications are usually personal and/or emotional according to most participants. Examples of disruptive situations for them are: someone at the door, someone on the other phone line, bad telephone connections and noisy children in the house. Escaping to the attic or keeping children busy with a movie was used as a strategy to maintain privacy. The participants' opinions of the location and presence awareness system that was presented in the storyboard scenario varied a lot. The family men saw no use for it; they would not share their presence and location with others, only maybe for staying in touch with their family when traveling. The grandmother doubted the usability and usefulness of the new technology. The single woman would like to know the availability for communication of her family and friends, but she would not share her availability with them. That is, an asymmetric attitude towards the information. The teenage girl didn't trust the privacy protection of the system. Automatic identification wasn't considered as a privacy risk. People assumed that if they would use it, they would also know the privacy risks. Automatic presence notification was an ambiguous concept for the participants. They would prefer to set their own presence and availability for communication, but they also acknowledge that this would require too much effort. Also, they didn't trust others to set their presence and availability. The young adults (in their twenties) were frequent users of MSN and Skype programs, but they rarely used the availability information. As message senders they ignored the status information as it is not always accurate because it is automatically set to 'away' when the user is not active on the computer. As message recipients they used the status information to ignore incoming messages in a socially acceptable way. Automatic intervention to protect user's privacy was considered neither useful nor desirable. According to the participants, it is rude, asocial and inconsiderate to shut off communication automatically without warning all the users involved.

In sum, the most important ways in which people handle their privacy is to isolate themselves from other family members and outside interruptions. To achieve such isolation, they retreat to private rooms or have agreements for not being disturbed. They also use plausible excuses for not communicating. For example, 'failure of technology' to mask their real reasons like 'not being in the mood to communicate'. Their strategies are rather ego-centric as they are more appreciative of being able to see someone else's presence or availability than showing their own presence. They only tend to see the implications of their privacy settings, but not what the implications of these settings are for other people.

3 Sharing Presence Information - in the Field

Isolation appears to be one of the most important strategies for people to protect their privacy in familiar communication situations. To understand how this behavior in actual privacy sensitive situations is affected, a field study was conducted in which presence information was shared between two connected homes. A functional prototype was placed in the homes that could be used for 2 weeks and for which the experiences of the users could be investigated. Perceived privacy was measured with questionaires that addressed five composite concepts: perceived social presence (4), perceived control (5), perceived effort, perceived connectedness and social presence (6). Automatic and manual presence detection conditions were used.

3.1 Methodology

Four pairs of friends/relatives participated in the study; one person per household. Two of the participant pairs had a parent-child relationship (children: mid-twenties; parents: mid-fifty), one pair were sisters (mid-twenties) and one pair were very close friends (mid-twenties). The two households were connected by two HomeLamp systems that showed the presence of persons in their homes. The systems supported a basic form of location-tracking to detect whether a person was at home or not. The HomeLamp-system consisted of a small-form-factor computer, an amBX-lamp and a sensing device for detecting wireless tags (7). The tags were attached to a key ring. They had a button for toggling between ’present’ and ’not present’ status. Users could set the presence status in the manual condition and override it in the automatic status. The range of detection was 300m. When people entered or left their home, their presence was detected by the system and shown by the lamp. The amBX-lamp generated different color patterns. Each participant had a personal color to indicate presence status. When a participant was at home, then this was also shown in the other home by light and color indication (Figure 1). The systems were permanently connected to the Internet and the presence information was shared by using the Jabber protocol. The information that is shown on one system, is identical to the information that is shown on the other, connected system.

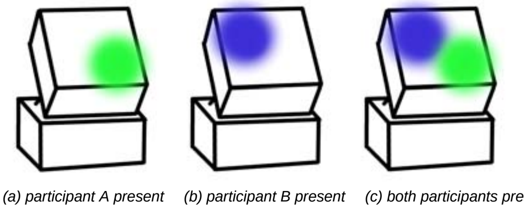
(a) participant A present *(b) participant B present* *(c) both participants present*

Fig 1: Presence status of participant A (light grey) and participant B (dark grey) as indicated by the lamp

3.2 Field Study Results

The results of the questionnaires were summarized over all participants and analyzed separately for social presence, connectedness, social privacy and control and effort. In addition, the reliability of the rating scales was measured and if it was sufficiently high non-parametric tests were used to test the difference between the manual and automatic conditions. The ‘feeling of social presence’, was rated significantly higher in the automatic condition (mean rating 5.1) than in the manual condition (mean rating 4.5) on a scale of 1 (least) to 7 (most). The concepts ‘connectedness’ and ‘social privacy’ were measured by means of 5 separate items: Expectations, Invasion of privacy, Obligations, Sharing experiences, Staying in touch, Thinking about each other. The ratings for these separate items showed large variability, meaning that the participants did not agree on them.

The items for invasion of privacy are rated higher than the items for feelings of expectation and obligation. Thinking about each other and staying in touch are rated higher than sharing experiences. These differences were, however, not significant. The items concerning effort had slightly higher ratings with less variability across participants than the items concerning control. There were no clear differences between the automatic condition and the manual condition except for the amount of attention that the system required.

The results of the interviews were analyzed and clustered based on consensus between two independent analyses of the audio data. The most salient groupings are reported here. They concern aspects of ‘perceived effort and control’ and ‘perceived sharing and connectedness’.

3.2.1 Perceived Effort and Control

People preferred the automatic condition over the manual condition. According to them, it would take too much effort; they had to think about it and conduct an intentional action to show being at home. Some participants wanted to be in control of the HomeLamp, irrespective of whether they used that control or not. Agreements were made between participants on how to use the HomeLamp. They preferred to show their availability rather than their presence, if it wouldn’t take too much effort to do so. The presence information was only shared with a very small group of close relatives and friends and didn’t go beyond sharing more information than their availability or presence in the house. Detailed location information as well as detailed activity information was considered to be too privacy sensitive. The information in the manual condition was considered less reliable than the information in the automatic condition because participants occasionally forgot to turn the HomeLamp on (in the manual condition) and they also expected the other party to forget it as well.

3.2.2 Perceived Sharing and Connectedness

Most participants preferred a social solution over using the system for sharing their availability. They preferred to simply tell the other person that they were not available instead of using the system to show this. The HomeLamp increased a feeling of connectedness, which was in most cases a positive feeling. However, for the parent-child relationships it felt sometimes as an overload of information. Children felt being monitored and parents became anxious when their child, for example, was not present or did not answer a call when expected. Friends or sibling pairs did not associate negative feelings with such unexpected situations. Multi-person situations between household members did not pose specific privacy issues for the participants. The children in the parent-child relation used deception. They felt uncomfortable about hiding information, but they also felt forced to use such deception.

In addition to the responses of the participants to the interview questions, specific observations were made. First, everybody has a different kind of Internet connection and households with more than one person, usually have one person who is the administrator. Second, people didn’t feel monitored in the automatic condition. The only comparative comments for the manual and the automatic conditions concerned the difference in effort and the difference in reliability. Third, the behavior of the participants in the manual condition showed that they became more casual with regard to turning the lamp on or off when they changed their presence situation.

3.3 Conclusions

For most participants the HomeLamp definitely increased their feeling of connectedness. But, this benefit also depended on how they normally keep in touch. As for the conditions, the manual condition took too much effort. The feeling of social presence is higher for the automatic than for the manual condition. Arguably, this might be connected with the fact that the perceived reliability of the manual presence indication was low because participants sometimes forgot to use the system.

Sharing information about being home is about as detailed as the participants liked it. More detailed information was generally considered to be too privacy sensitive. However, this remains a matter of subjective preferences and depends on how well the other can interpret the information. Participants only wanted to share their location information with a small group of people. Sharing information might not only have a negative effect on the sharer, but also on the receiver. Too much information might lead to anxiety, especially if the receiver has some sort of caring function.

In short, this field study showed that people will share their information with only a small group of close relatives and friends, the sharing of the location information should have a clear benefit, users need a feeling of being in control and the desired level of detail of the location information is subjective. Furthermore, the large variability in the behavior of people in privacy sensitive situations induced by, for example, presence sharing applications has implications for the design and use of awareness systems. Individual differences, varying social relations and application specifics have to be considered.

4 Maintaining Privacy in Application Specific Situations – Using Different Types of Noise

To investigate what people do to maintain their privacy in application-specific privacy sensitive situations, a conceptual design study was conducted. The focus of this study was on how people want to hide information that is being shared to maintain their privacy. One of the most important conclusions from the HomeLamp field study was that people want control over the level of detail in which their information is shared. Price et al. (8) propose a model for user control of privacy that incorporates ”noise” by introducing ambiguities in the information. This model deals specifically with location and identity information and is divided into five types of “noise”:

- Anonymizing: hiding the identity of the user.
- Hashing: disguising the identity of the user.
- Cloaking: making the user invisible.
- Blurring: decreasing the accuracy of the location
- Lying: giving intentionally false information about location or identity.

The conceptual design study investigated how well these noise forms fit extended home environment applications and which noise forms are desired by the users.

4.1 Methodology

People’s perceived privacy is influenced by how they appreciate the usefulness of presence sharing information. To study these effects, application concepts were used for which the perceived usefulness differs. The following application concepts were investigated: 1) the sharing of photos, 2) the sharing of location, that is, knowing where the other person is, and 3) the sharing of health information. Participants were shown sketches of these concepts. The information that could possibly be privacy sensitive was identified for each application concept and noise forms from (8) were adapted to each of them. Participants were asked to evaluate three application concepts and indicate in what form they would want to share their data. The participants (N=18, age 25-52 yrs.) were asked with whom they would like to share the application and in which context they would use it. They also had to rank the applications according to their preferences. Three tasks were carried out for each application and participants had to indicate and explain which noise forms they would: (a) optionally want in the proposed application, (b) have as their default setting, and (c) rank highest regarding perceived importance. A thinking-aloud methodology was used (9). Cards were used to present each information type. An example of the task presentation and its setting is shown in (Figure 2).

4.2 Results

The photo sharing application was preferred the most, followed by sharing health information. Least preferred was sharing location information. The preferences for noise forms differed per application. Correlation between rankings was calculated using the Kendall coefficient of concordance.

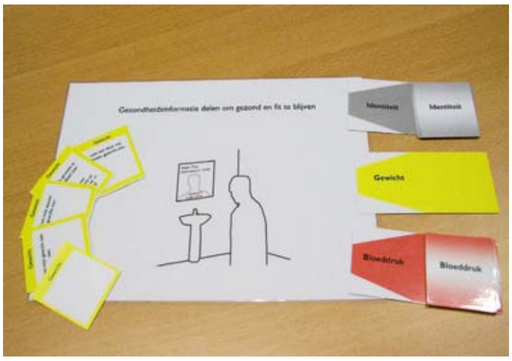

Fig.**2** Example of task assignment for the conceptual design study. This application can unobtrusively monitor your health, for example your blood pressure and weight, but also other health factors can be measured. Each morning the information is collected and sent for example to your physician, or to your sport coach, etc. How would you handle these situations and which noise forms (exact data, less detail, free data choice, no show) would you select in each situation?

The ranking results are shown in Table 1. The rankings for the photo sharing application showed that no background video and audio is preferred over blurring the background video and distorting the audio. Regarding identity, the use of nicknames (hashing) and partial identity (blurring) was preferred over using a chosen identity (lying). Partial identity (blurring) was liked the most and showing no identity (anonymizing) the least for the location sharing application. Showing their location in less detail (blurring) was preferred over giving a free-choice location (lying). For the location information sharing application settings there was less agreement amongst the participants then for the photo sharing application settings. Agreement among participants was highest for the health information sharing application. Sharing the exact weight and blood pressure (no noise) was preferred above a chosen weight and blood pressure (lying). Sharing their exact identity (no noise) was liked the most and sharing a chosen identity (lying) was liked the least.

Table 1. Ranking results for Photo sharing, Location sharing and Health sharing applications as participants' choices (n=18).

Noise form	Card sorting choice	Default choice*
	Photo Sharing Application	
Identity		
• Exact identity	9	5
• Partial identity	15	9
• Use of nick name	13	4
• Chosen identity	8	0
• No identity	6	0
Video		
• Full view	17	4
• Blur	6	0
• No background	13	7
• No video	12	4

Audio		
• All audio	14	5
• Voice only	17	11
• Fade audio	2	0
• Distort audio	5	0
• No audio	10	1
	Location Sharing Application	
Identity		
• Exact id	9	5
• Partial id	15	9
• Nick name	13	4
• Chosen id	8	0
• No id	6	0
Location		
• Exact location	12	3
• Less detail	17	11
• Chosen location	9	0
• No location	13	3
	Health Sharing Application	
Identity		
• Exact id	15	9
• Partial id	10	3
• Nick name	6	3
• Chosen id	4	1
• No id	8	2
Blood pressure		
• Exact blood pressure	18	10
• Less detail	11	4
• Chosen blood pressure	1	0
• No blood pressure	8	3
Weight		
• Exact weight	18	10
• Less detail	8	4
• Chosen weight	1	0
• No weight	10	3

* Not all participants could make a choice

4.3 Conclusions

The highest level of agreement was found for the use of video and audio background information as noise in the photo sharing application and for weight and blood pressure data in the health application. That is, people don't want to protect their privacy by blurring video and audio backgrounds if they share photo's and they don't want to lie about their blood pressure and weight if it is for their health's benefit. The lowest level of agreement was found for identification information in photo sharing and sharing health information, that is, there is no common preference in noise form to mask identity information.

In sum, there was no decisive result, but in general, giving less detailed information is preferred over exact information. This confirms also the findings from the HomeLamp field study. Participants provided a multitude of contexts for which they would use different noise forms to maintain social norms and values. Preferences for noise forms differed per application. These contexts are quite complex, as they dynamically change depending on with whom the information is shared and on the participant's perceived benefit. In general people prefer to share information at the lowest level of detail that is appropriate but they desire to add noise (e.g. by lying) for social acceptability. This implies that it should be easy for users to switch between noise forms depending on the dynamic nature of the context.

5 Conclusion

We started our research into perceived privacy in ambient intelligent environments in an exploratory fashion, followed by a targeted study that involved limited implication effects and continued by studying different application specific contexts. Within this approach, we limited the scope of the studies to the specific environment provided by the Amigo project to provide input and guidance to the design of the Amigo system. During the exploratory study, people were asked about their daily communications and related privacy issues. In the field study, a system for presence detection in the home and sharing that information across homes was developed and evaluated. The conceptual design study was conducted to find out how people would like to be able to mask or hide information that is being shared between different parties for three different types of applications. The main conclusions are:

- people use many diverse mechanisms to preserve their social privacy,
- people will share their personal information only with a small group of close relatives and friends,
- information sharing should have a clear benefit for users,
- users should have the possibility to control the level of detail of the information that is being shared, and
- users need a feeling of being in control, for example, automatic location detection is appreciated by users, but they also need to be able to influence the automatic detection mechanism.

5.1 System Design Implications

Although the qualitative and quantitative results and observations from the user studies provided a wealth of information on the perceived privacy of users. They didn't provide information on how data should be secured, stored, or encrypted to support and advice application development. Initially, it was proposed to handle privacy at the middleware service level of the Amigo architecture by means of a rule-based filter that incorporated the user's preferences and that would use the preferences to either pass on the data or not. Our field and concept studies showed, however, that such a mechanism for privacy filtering on the Amigo services level is not sufficient. Although there is definitely a need for a component that handles and stores the user's privacy preferences, it is not sufficient for protecting the user's perceived privacy, because it does not offer direct user control. Privacy should also be handled at application level. In particular, the type of information that is shared, the level of detail in which the information is shared, and with whom the information is shared (for example, with groups or individuals), are the most important concepts to take into account.

In addition to the implications for the system architecture, design guidelines could be derived from the results of the qualitative and quantitative studies to support the development of extended home environment applications. First of all, the most important rule to take into account is: 'Maximize benefit, minimize effort and provide reasonable control for the end-user'. In addition to this rule, the following design guidelines need to be accounted for:

1. Provide proper security and inform users of security measures
2. Provide control on several levels
3. Present the user with a choice of level of detail in which the information should be shared
4. Provide clear feedback over shared information
5. Never automatically share information without user consent
6. Avoid using automatic intervention to maintain user privacy.

These guidelines were worked out with a detailed description, a general problem statement, examples from the Amigo extended home application scenario and a validation (example in Table 2). These guidelines complement existing guidelines for designing for privacy such as the OECD guidelines (Organisation for Economic Cooperation and Development, (10) and the guidelines from Langheinrich (11). While, the latter are very generally applicable and refer mainly to the collection of data, our guidelines are specific for applications in the extended home environment and focus on the sharing of data in a social context.

Table 2. Example design guideline # 3

Design guideline #3	**Present the user with a choice of level of detail in which the information should be shared**
Detailed description:	Each type of information can be shared in several levels of detail and it should be possible for the user to adapt the level of detail to the context in which the information is shared.
General problem:	Although sharing information in the most exact way can sometimes be useful, users often feel a breach in privacy when they are forced to share their exact information all the time.
Example:	John and Maria share information about their physical condition, such as blood pressure and weight, while exercising. However, they only share whether the information is above or below the threshold. This way they can motivate and warn each other, but they don't feel monitored by each other.
Validation:	In the HomeLamp study, users felt comfortable with the system registering when they were either at home or not, and sharing this information. When offered the option of sharing detailed information, e.g. sharing information

Design guideline #3	**Present the user with a choice of level of detail in which the information should be shared**
	about in which room they were located, users indicated that they would not use this as they felt that they were monitored: ”Suppose that the system would show [my friend] that I was in my bedroom for an hour during the day, what would she think?! No, that’s too much information.”

In sum, the guidelines address the following aspects: levels of security, means for end-user control, levels of detail of the shared information, types of feedback to the end user, appropriateness for automatic sharing of information, and possibilities for automatic intervention for maintaining privacy. These guidelines are formulated in such a way that they can be used by system developers to create services and applications that are privacy-safe from an end-user’s point of view.

Acknowledgements

The Amigo project is funded by the European Commission as an integrated project (IP) in the Sixth Framework Programme under the contract number IST 004182.

References

1. M.D. Janse (ed.), Amigo Deliverable D1.2: Report on User Requirements, IST-004182 Amigo, April 2005.
2. Amigo Project – http:/www.hitech-projects.com/euprojects/amigo
3. N. Romero, J. van baren, and B. de Ruyter, Design and assessment of an asynchronous awareness system. Technical Note 2003/00683, Philips Research (2003).
4. P. de Greef, P. and W. IJsselsteijn, Social presence in a home tele-application, *Cyber Psychology and Behaviour*, (4), 307–316 (2001).
5. S. Spiekermann, Perceived control: Scales for privacy in ubiquitous computing environments. In 10th International Conference on User Modeling (2005).
6. J. v. Baren, et.al., Measuring affective benefits and costs of awareness systems supporting intimate social networks. In: A. Nijholt and T. Nishida (eds.), Proc. of 3rd workshop on social intelligence design, CTIT Workshop Proceedings Series WP04-02, 13–19 (2004).
7. Sensite Solutions: Logisphere BN208 Intelligent Tag; Logisphere HBL100 Wireless Network Controller. http://www.sensite-solutions.com/.
8. B.A. Price, et.al., Keeping ubiquitous computing to yourself: A practical model for user control of privacy. *International Journal of Human-Computer Studies*, (63), 228–253 (2005).
9. H.A. Simon and K.A. Ericsson, *Protocol Analysis: Verbal Reports As Data* (Bradford Book, rev. ed. Edition, 1993).
10. Organisation for Economic Cooperation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
11. M. Langheinrich, Privacy by design - principles of privacy-aware ubiquitous systems. In: G.D. Abowd and B. Brumitt (eds), Ubicomp 2001: Ubiquitous Computing: 3d Int. Conf. (Springer Berlin / Heidelberg, 2001). p.273.