Design Guidelines for Analysis and Safeguarding of Privacy Threats in Ubicomp Applications

Elena Vildjiounaite[1], Petteri Alahuhta[1], Pasi Ahonen[1], David Wright[2], Michael Friedewald[3]

[1] VTT Technical Research Centre of Finland, Kaytovayla 1, 90580, Oulu, Finland
{FirstName.LastName}@vtt.fi
[2] Trilateral Research and Consulting, 12 Tybenham Road, London SW19 3LA, UK
david.wright@trilateralresearch.com
[3] Fraunhofer Institute Systems and Innovation Research, Breslauer Strasse 48, 76139 Karlsruhe, Germany
michael.friedewald@isi.fraunhofer.de

Abstract. Realisation of the Ubicomp vision in the real world creates significant threats to personal privacy due to constant information collection by numerous tiny sensors, active information exchange over short and long distances, long-term storage of large quantities of data, and reasoning on collected and stored data. An analysis of more than 100 Ubicomp scenarios, however, shows that applications nowadays are often developed without considering privacy issues. This paper suggests guidelines for estimation of threats to privacy, depending on real world application settings and on choice of technology; and guidelines for developing technological safeguards against privacy threats.

1 Introduction

Development of new applications and enabling technologies in Ambient Intelligence / Ubiquitous Computing (these terms are equally common) often starts from writing an application scenario: a script that describes in which settings a new technology will be used. After having reviewed more than 100 Ubicomp scenarios (e.g., [1-8]), we found that often proposed applications do not consider privacy issues, even though many researchers [9-11] have already pointed out privacy threats arising from Ubicomp (its continuous attention to human activity and increased autonomy of computer actions) and from rapid technology development, especially the increase in computers' abilities to acquire, store and process more and more different kinds of information from different sources. Detailed analysis of privacy threats in the Ubicomp world is beyond the scope of this paper; such analysis can be found e.g. in [10-12].

After acknowledgement of privacy threats, work on privacy protection has started [9, 13, 14]. Such work has mainly considered information privacy, i.e., the personal right of an individual to control which information about him/ her is collected, stored and shared, while privacy also has other important aspects [11, 15], e.g., “the right to be left alone" is very important for personal development because people need relative insularity for developing goals, values and conceptions of self [15].

The work [9] suggests how the fair information practices (listed in current data protection laws) can be applied to Ubicomp applications, and shows how difficult it might be to apply them. The work of Lahlou et al. [14] focuses "on the specific issues of the data collection phase", although such generic design guidelines as "think before doing" and "understand the way in which new technologies change the effects of classic issues" (i.e., existing solutions in the physical world) can be applied not only to data collection. Our work makes these generic design guidelines more specific.

The work of Hong et al. [13] proposes privacy risk models based on two aspects: first, social and organizational context in which an application is embedded (who are data shares and data observers; what kinds of personal information are shared; what is the value proposition for information sharing; its symmetry, etc.). The second aspect is technological (how are collection, storage and retention of personal data organized; who controls the system; is there any possibility to opt-out). This is close to our understanding of privacy threats, but we suggest taking into account other aspects also, especially probability of accidental (not intended by designers) information flow.

Currently most of research on privacy protection is concerned with protection of information privacy in network applications and with security of personal devices, and considers privacy protection for current technology settings. The main privacy protecting principles in network applications are stated to be anonymity (possibility to use a service without disclosure of user identity); pseudonymity (possibility to use a service without disclosure of user identity, but still be accountable for that use); unlinkability (possibility to use multiple services without others being able to discover that these resources were used by the same user) and unobservability (possibility to use a service without others being able to observe that it is being used).

Even in current technology settings, however, these principles are not yet fully implemented [16]. Implementation of these principles in future settings (as they are described in scenarios) would be more challenging and not always possible. In network applications, users have some understanding of which data are collected and means to restrict data collection (e.g., to use Internet cafe for accessing web sites). In Ubicomp environment, full of numerous invisible sensors, it is difficult (if not impossible) for users to understand and to control data collection and to achieve unobservability, anonymity and pseudonymity, because the user and his/ her data are not physically separated anymore. Another important difference between network applications and emerging applications is that neither mobile devices nor web usage penetrates through such strong privacy protecting borders as walls and the human body, while physiological, video and audio sensors, proposed for future settings, have much stronger capabilities to identify a person and to reveal personal activities and feelings.

In this paper, we present dimensions of privacy threat analysis and suggest guidelines for privacy protection for future Ubicomp applications.

2 Traditional Privacy Protecting Borders

In the work of Lahlou et al. [14], it is suggested that privacy protection requires understanding of how new technologies change the ways developed in physical world. In the physical world, personal privacy is protected by the following borders [11]:

- *Natural Borders:* physical borders of observability, such as walls, clothing, darkness, facial expression (a natural border against the true feelings of a person).
- *Social Borders:* expectations with regard to confidentiality in certain social groups, such as family members, doctors and lawyers, e.g., the expectation that your colleagues do not read personal fax messages addressed to you.
- *Spatial or Temporal Borders:* expectations by people that parts of their lives can exist in isolation from other parts, both temporally and spatially, e.g., a previous wild adolescent phase should not have a lasting influence on the current life of a father of four; a party with friends should not affect relations with colleagues.
- *Borders due to Ephemeral or Transitory Effects:* expectations that certain action or spontaneous utterances will be soon forgotten or simply unnoticed because people's attention and memory are limited.

Physical borders are perhaps perceived as most reliable, which can be illustrated by, e.g., how poker players control their faces or by the custom of knocking at a closed door of somebody's private room or office. People also have a well-developed mental model of the limits of their own or others' ability to notice and to remember details of what's going around. For example, people in a conference room usually expect that others' attention and memory are devoted to contents of a presentation rather than to the auditory side. Concerning social and spatial borders, people perceive them as not so strong, e.g., the likelihood of encountering the same people in different circumstances or of broken confidentiality is not negligible. Generally, the stronger is personal belief that certain border is reliable, the more difficult will be adaptation to its violation by a new technology. Experiments in the research area of computer-supported collaborative work suggest one example of the adaptation difficulty. In order to facilitate awareness and communications between colleagues, video cameras were installed in the offices of participants. Although awareness has proved to be useful, the experiments have shown that people often act according to an "old" mental model of being reliably hidden by office walls [17].

3 Dimensions of Privacy Threats Analysis

We think that privacy risks fall into two major groups: first, application domain-dependent risks, which depend on the supported personal or organizational activity. For example, health data are considered sensitive, and designers of applications for hospitals follow corresponding privacy-protecting regulations. Second, privacy risks are caused by a mismatch between personal expectations about current privacy level and reality, which do not depend on an application domain. If a person perceives his current situation as private (e.g., being alone at home), but in fact he is being monitored, the chances that personal secrets will be discovered are higher than if the person perceives the current situation as public (e.g., making a presentation in a large meeting) and takes care of own privacy himself.

After reviewing Ubicomp application scenarios, we observed that the possibility of privacy being violated accidentally is not always considered. For example, in [1], it is suggested to make video recordings of meetings, so that writing "meeting minutes" is not needed. Such recordings of presenter mistakes, personal conversations, spontane-

ous remarks, laughter or bored faces, however, can affect one's personal career negatively, because playback of a video recording (with the possibility of watching the same scene many times) reveals many more details than physical presence at the meeting when people are concentrated on the main points of working problems.
We suggest the following dimensions for analysis of privacy threats:

- Dimensions of the real world:
    - Personalities of humans
    - People's activity
    - Environment where activity takes place
- Dimensions of technology functionality
    - Information flow
    - Computer control level vs. personal control level
    - Balance between different aspects of technology (storage and communication vs. reasoning capabilities and control level)

3.1 Dimensions of Real World: Humans, Activities and Environment

The notion of what is considered private and what is not depends on a person and on a situation (context) [15]. For example, the chances that a wife or children accidentally access personal data of a married person are fairly high; however, secrets from family members are not unusual. We suggest that application designers should consider, first, how privacy-safe is an application for a user who has secrets from family members (who are always nearby); from work colleagues and superiors; and from an insurance company capable of hiring good specialists for acquiring personal data. Second, it is needed to consider how much time and knowledge are needed for configuring privacy protection in a personal device and whether anyone can do it fast.

Personal activity is an important dimension for privacy risk analysis because an activity consumes and produces information flow, e.g., a lot of financial data are involved in paying bills; health and identity data are involved in a call to a doctor. Environment is an important dimension because people's mental models of current privacy levels are based on traditional perceptions of an environment (e.g., "now I am alone in my office, thus, nobody can see me") and people behave more or less freely depending on their estimation of current privacy levels. We suggest that applications should take into account the following:

- traditional perceptions of the environment (e.g., perception of a home as private environment; perception of a wall as a non-transparent object)
- common activities in the environment (e.g., in an office people usually work)
- other probable activities in the environment (e.g., calling a doctor or flirting with a colleague in an office environment).

Privacy threats coming from real world settings can be roughly categorized as high, medium and low. We suggest that high threats appear in the instance of activities dealing with health care, finances and communications between family members and close friends; high threats also appear in the home or office environment (because people can not avoid dealing with private issues at work and are highly dependent on their work). Medium threats to privacy appear in shopping, learning and mobility

activities (by mobility, we mean travelling within a city as well as holiday and work trips); and relatively low threats are associated with entertainment activity.

3.2 Dimensions of Technology Functionality

A typical view of an Ubicomp application is presented in Figure 1. Thin arrows indicate information which is collected (pulled) by the system and exists there for a short or long time, which carries a potential threat that personal data become available, against a user's wishes, to others (neighbours, government, insurance companies, etc) if they get access to them. Thus, threats appear either if access control to information fails (e.g., communications are intercepted, or stored data are unprotected) or if data contains accidentally acquired secrets (e.g., something in the image background).

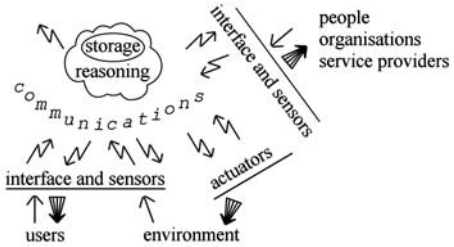

Fig. 1 Generic view of Ubicomp application: thin arrows indicate information which is collected and exists in the system, thick arrows indicate information push.

Thick arrows indicate information push, which implies that message contents will be certainly delivered to their destination and will be available to receivers (or will cause an automated action, such as opening a door lock in office access control applications). Consequently, more threats appear: first, access control to a message can fail; second, message contents can tell the recipient more than the sender intended; third, a message can be delivered at a wrong time; and last, harm can be caused by actuators' actions (e.g., failure to lock a door allows everybody to enter a room).

3.2.1 Information Flow and Application Control Level

Information flow starts from data collection performed by sensors. The most popular sensors in Ubicomp scenarios are audio, video, positioning, physiological and safety and comfort sensors, as well as logging of human-computer interaction actions.

From the privacy point of view, physiological sensors are most dangerous because they detect what is inside a person's body, i.e., they "break" into the most private sphere. These sensors are the basis for building health care applications, where strict rules for protection of health data exist. Ubicomp scenarios, however, suggest these sensors for purposes other than health and wellness. Detection of a person's mood and emotions is an active research area [18], and suggested applications include detection of interesting scenes for automatic audio and video capture for lifetime personal store

[8] and estimation of a user's liking of TV programmes [2]. However, if physiological data are linked to the contents of TV programmes and to the presence of other people, personal feelings become dangerously "naked" and can, for example, reveal to parents with whom their child is in love; or can be used by government for monitoring the loyalty of citizens. Physiological sensors can also detect health problems, but this data will not be properly protected because data protection requirements in the domain of TV personalization are not very strict.

Video and audio sensors violate natural privacy-protecting borders such as walls, and video cameras can reveal a lot more than audio sensors. In Ubicomp scenarios they are suggested, first, for real-time communications between people, e.g., for helping parents to check what their children are doing [5]. Second, such sensors are suggested for memory augmentation, e.g., recording of work meetings [1] and personal memory aids [8]. The first type of application "breaks the walls"; the second type of application violates people's belief in the limits of others' attention and memory.

Data from safety and comfort sensors (temperature, light, car acceleration; biometric sensors for access control) can reveal personal lifestyle either inside or outside homes. The threat of identity theft may be associated with biometric sensors. Another important issue is that these sensors often initiate information push, e.g., they may give reminders to switch off the stove or employ actuators to do it automatically. This is beneficial for people suffering from dementia or for families with babies. However, if teenagers are assumed to be as irresponsible in caring about home safety as babies, there may be little opportunity left for teenagers to develop a sense of responsibility.

Application control level denotes how much technology does on behalf of users. For example, an application that reminds a user to take pills in case of high blood pressure has a high control level because it initiates a measuring of blood pressure and initiates a dialog with a user. Consequently, such dialog can annoy the individual or reveal personal health details if it happens at a wrong moment or in public. An application which filters shopping advertisements according to user preferences also has a high control level, because the user can never know about certain shopping alternatives if they are filtered out. (For such applications, an important question is who sets filtering rules and how to prevent the favouring of a particular shop.)

3.3 Summary of Technology Threats

With greater information collection, transmission and storage capabilities and higher control levels, technology poses more privacy threats. Most Ubicomp scenarios involve application-dependent information storage and a lot of wireless communications (between objects, people and organizations).

We suggest that significant threats to privacy arise if technology penetrates walls and the human body, e.g., by using physiological, video and/or audio sensors. Significant threats are also caused by high control level of technology (i.e., the capability of a technology to act on behalf of a person, for example, to call an ambulance in an emergency); by biometrics sensors (due to the possibility of identity theft); and by aggregation either of a lot of data about one person, or some data about many people. Medium threats are associated with positioning sensors (used alone, they provide

location data, but not much activity data) and with medium level of technology control (the capability to make proactive suggestions, e.g., to give reminders). Fairly low threats are associated with low control level (e.g., ranking advertisements according to criteria explicitly set by the user), and with comfort sensors (lighting, heating, etc).

4 Design Guidelines for Privacy Protection

Different application domains and components present different threats to privacy and require different safeguards. One of the most generic safeguards is to minimize data collection to what is absolutely needed for application purposes (called "Privacy Razor" in the work of Lahlou at el. [14]). In practice, however, it is not easy to determine what "minimally required data" is, because the same data can be acquired in many ways, each of them presenting different threats for privacy. For example, movie recommendations applications need user feedback data, and ways to obtain it include: use of physiological sensors; analysis of facial expressions; speech recognition; monitoring such user actions as fast forward scrolling (which is safest for privacy).

Another generic safeguard is data encryption during data transmission and storage, but even 100% reliable encryption is not a magic solution; first, because a lot of information can be gained by monitoring the traffic of encrypted data. Second, the crucial problem is proper access control to encrypted data, and this problem is not solved yet. Encryption of data stored in a personal device does not help as long as the device considers itself in the hands of an authorised owner, which is usually for a long time after it has been switched on. Appropriate protection of data stored in personal devices will not be possible until user-friendly access control methods are developed (that is, methods for frequent, reliable and unobtrusive user authentication).

We suggest that the most important safeguards are appropriate access control to data and appropriate intelligence of applications, because only they can help against the dishonest person accessing the data required by a Ubicomp application and against accidental acquisition of sensitive data by the Ubicomp application, which can happen either with a single sensor (e.g., video), or via linkage of several sensors' data.

Consequently, we suggest that if an application poses significant threats to personal privacy in the real world, and if significant threats are caused by choice of technology, both lightweight and strong safeguards, listed below in more detail, should be implemented. In some cases, the required level of privacy protection might be too expensive for the application purposes; or appropriate safeguards may not be mature yet (e.g., automatic detection of sensitive video data is still in its infancy). Research on many strong safeguards has already started, but the results are not yet ready for real life use. In these cases, privacy risks should be decreased by choosing less threatening technology for implementation of a desired functionality: to use other means of information acquisition, or to decrease the control level of a particular technology.

Additionally, we suggest that application designers should develop some means to escape from Ubicomp applications gracefully, so that nobody understands why the user is inaccessible, similar to the current situation with mobile phones when not answering a phone call is perceived as not unusual (the battery may be discharged; or the user may be in an area where connections don't work well; or the user may be in a

shower, etc) and does not give any hint of the user's activities or intentions. In a future of small powerful hardware embedded into clothes, watches and walls and with improved network coverage, however, escape from communications might not be that easy. For example, if users have switched off a meeting recording, one might assume that they are either discussing work secrets or personal affairs. Thus, an application should always stop in exactly the same way, e.g., a stopping should be always abrupt.

4.1 Minimisation of data collection, transmission and storage

We suggest the following relatively lightweight safeguards:
1. Instead of logging raw data, only data features should be logged by using either hardware filters or by doing as much real-time pre-processing as possible (e.g., logging only the number of peaks or the time period when heart rate was above a predefined threshold; or detect predefined contexts and user actions in real time);
3. Time-stamping of logged data should be limited by making it relative to other application-related information (e.g., " in the first hour after taking a pill, the blood pressure was normal, after that it was elevated") or by averaging and generalising time stamping (e.g., "heart rate was high for two hours"). This should prevent a discovery that, e.g., the heart rate of a boy becomes high each time he meets certain girl;
4. Hardware used for data collection should not have extra memory and extra data transmission capabilities, and no easy plug-ins for increasing them (to prevent spying). This can be achieved, e.g., by giving to each application access rights to a certain memory block instead of giving to all applications access to the main memory;
5. Data should be deleted after an application-dependent time, e.g., when a user buys clothes, all information about their textiles, prices, designers, etc should be deleted from the clothes' RFID tags. If applications require active RFID tags (such as for finding lost objects [7]), the ID of the RFID tag should be changed, so that no links between a shop's database and personal clothes are left;
6. Applications which don't require constant monitoring should switch off automatically after a certain period of user inactivity (for example, video cameras automatically switch off after the end of a game).

Fairly heavy-weight (strong) safeguards (required for applications posing significant privacy threats) would be:
1. Authorisation at the stage of upgrading hardware and adding plug-ins
2. Anti-spyware software on each piece of hardware.

4.2 Privacy protection in networks (transferring of identity and personal data)

Data transfer in Ubicomp applications takes place between remote locations (e.g., in m-commerce applications or web browsing) as well as between diverse sensors in a smart space and between devices which belong to a personal area network (PAN), e.g., several sensors attached to a human body in different placements or several personal belongings. We suggest the following light-weight safeguards:
1. Data filtering on personal device should be preferred, if possible (e.g., instead of sending a user's financial preferences to a jewellery shop, the application can query

the shop about all items, and sort them by price and other criteria already on the personal device. This approach requires more data transmission and does not allow use of certain recommendation techniques known as collaborative filtering, but it has the advantage that users don't feel that a piece of metal decides what can they afford).
2. Data transmission and storage, if they take place over long distances, should allow anonymity or pseudonimity (using different identities with minimally sufficient personal data in different applications, as suggested in [19]) of a data provider (e.g., if a user buys something and has paid for it, the user's identity should be hidden). The ways to do it include, first, methods to prove user authorisation locally and to transmit over a network only a confirmation of authorisation; second, methods to hide user identity, e.g., by distributing this knowledge over many network nodes. The goal of pseudonimity is to prevent a discovery, either from personal contact details or from the ID of a personal device, that the same person has ordered a lot of chocolates and diabetes-related medicines, which might be of interest to an insurance company and result in increase of the person's insurance premium's due to not following a diet.
3. Wherever possible, to implement unobservability in PANs and smart spaces by limiting the communication range so that signals stay within desired spatial limits (inside a room or a car), unlike the current situation when two owners of Bluetooth-enabled phones are aware of each other's presence in neighbouring apartments.

Higher-level protection should include the following:
1. Data transmission should not use the ID of a personal device or an object; instead, IDs should be used only for a current communication session (otherwise it is easy to associate a device or an object, e.g., eye glasses, with a person).
2. Data protection by security means and access control methods (see Section 4.3) from malicious actions (eavesdropping, data modifications, denial of service, etc).

4.3 Access control

The traditional understanding of the term "access control" is in regard to granting a person the right to log on to a system or to have access to an otherwise restricted office. Recently, "access control" has also taken on a sense of checking which software accesses personal data and how the data will be processed. Implementation of proper access control methods is one of the most important safeguards. Unfortunately, reliable unobtrusive access control methods for privacy protection do not exist in yet. This situation is best illustrated by usage of mobile phones (which store a lot of personal data), which are not protected at all for a long time after being switched on due to lack of user-friendly authentication methods suitable for frequent user verification. Consequently, loss or theft of a phone presents threats to its owner's privacy.

Proper access control should be also built in licensing languages (methods to impose correctness of data processing and to do privacy audit afterwards [16]). One of a few existing methods to specify personal privacy policy regarding web applications, P3P, neither forces web sites to follow the user's wishes (the user just gets a notification about a mismatch between privacy policies), nor to adhere to their own promises regarding processing of user data.

Lightweight methods of access control include the following:
1. Frequent tests for compatibility and updates of anti-virus and firewall software;

2. Authorisation for accessing not only personal data, but also device characteristics, unlike the current situation with Bluetooth device IDs or IDs of RFID tags, which are easily available [20].

Stronger access control methods include the following:

1. Enforcement of privacy law and policies by expressing legal requirements and personal user wishes in machine-readable rules and by embedding these rules into data in such a way that they can not be ignored or bypassed (similar to how digital rights management methods are aimed at preventing illegal copying of files) [16]. These privacy rules should describe what is allowed to do with data in different contexts (e.g., in case of merging databases), and to ensure that the attached rule is applied. Also needed are methods of facilitating privacy audits (to check correctness of data processing, which should work even in case when the data are already deleted).
2. Access control to sensitive or aggregated personal data should be continuous, unobtrusive and context-dependent (e.g., requiring more reliable authentication if a user starts a more sensitive application). Continuous unobtrusive access control is generally more reliable, and it decreases the risk of identity theft. For example, if a car lock can only be opened by the car owner's fingerprint, there is a danger that criminals will either produce a faked fingerprint sample or will cut off the owner's finger. However, if authentication of the owner were to continue inside the car (e.g., by weight sensors embedded in the seat, by positions of the seat and mirrors, by driving patterns, by voice or even by face recognition), a thief will eventually be discovered.
3. In order to protect against an authorised but dishonest person, unusual patterns of copying and processing of personal data should be detected (e.g., if the next back-up of data takes place soon after a previous back-up, then it may indicate a data theft).

4.4 Artificial Intelligence Methods

All software algorithms are to some extent AI methods. In the context of this paper, however, we call AI safeguards methods of advanced reasoning capabilities, which are not mature solutions yet, although research on them is actively going on. Many privacy threats appear due to the fact that reasoning capabilities of software do not grow as fast as hardware capabilities (storage and transmission capabilities). Advanced AI safeguards are the main means of protecting people from accidental, unintentional privacy violation, such as disturbing a person at a wrong moment or recording some private action. They are needed also for advanced access control and anti-virus protection, by catching unusual patterns of data copying or delays in program execution.

Lightweight AI safeguards can be rule-based, with rules derived from human common sense, e.g., that sensitive data can be more easily acquired when there are only one or two persons in a room than when there are many people. Common sense suggests also giving more freedom and responsibility to teenagers than to younger kids. Since many exceptions to common-sense rules exist, however, we suggest that AmI applications with high control levels should be capable of the following:

1. Detection of sensitive data (e.g., recognition that persons in a photo are naked or kissing or that a conversation is private, even if it takes place in an office);

2. Adaptation to people's ethics (e.g., not to take photos of naked persons automatically; not to provide reminders about private obligations, e.g., taking medicines, in public; not to record personal conversations; to respect everybody's dignity);
3. Adaptation to different cultures and etiquettes;
4. Intelligent online summarisation of records, e.g., online conversion of a meeting audio stream into a text document, which would include only working discussions;
5. Intelligent interpretation of users' commands with natural interfaces: application should have the means to resolve ambiguities (e.g., to understand when the user addresses the application, and when he/ she talks to other humans; and to be able to understand complex language constructions in any context).

4.5 Developing of Transparancy Tools

Unfortunately, implementation of an application that records only working discussions is more difficult than implementation of application that records everything. One partial solution can be raising user awareness about video cameras and data flow. Since it is impossible to provide details of every surrounding sensor and application, especially in public places, a concise and unified form of initial warnings should be developed about most privacy-violating technologies (such as those that record video and audio data, log personal identity data, physiological and health data), similar to a form of road signs. Standardisation of privacy policy has started already for web sites [21]; however, transparancy tools should be applicable to all Ubicomp components.

User-friendly interfaces are needed for providing awareness and for configuring privacy policies. Maintaining privacy should not be a burden for a user, but, on the other hand, if the user is really concerned with privacy protection, he should be able to configure easily the following important settings:
1. the goal of the application (e.g., to record a meeting);
2. the degree of the application's autonomy (what can the application do on its own initiative and in which cases, e.g., will it start recording when all meeting participants arrive; will it suggest to someone that he take a medicine at certain time of a day or when his blood pressure rises above a certain rate);
3. the information flow from the user who should be able to understand and to configure the following:
   - what data are collected and how (e.g., continuous record of blood pressure vs. counting the number of high blood pressure peaks);
   - what happens to the data after collection (what data are processed locally, what are transmitted; what are stored, where and for how long);
   - what patterns are searched (dependency of high blood pressure on absolute time vs. dependency on relative time, e.g., from the moment of taking a pill);
4. the flow of information to the user who should be able to configure the following:
   - how the information is presented (e.g., is a reminder to take a medicine given as an audio warning or via SMS);
   - how the information is filtered (e.g., an application that filters advertisements can either completely block information which is considered as uninteresting; or present a complete list of advertisements ranked by their estimated usefulness).

4.6 Developing Means of Recovery

It seems quite probable that losses of personal data will happen in a future, just as identity thefts happen now. Consequences of data losses can include problems in personal relations, work discrimination, financial problems or even death, and recovering from some data losses can be impossible or require other than technological methods, e.g., legal methods. Nevertheless, some problems can be solved by means of technology. For example, in case of theft of somebody's biometric data, there should exist means to replace compromised biometrics with another authentication method (another biometric, tokens, etc) everywhere (in all credit cards, in all office/ home/ car locks etc), and to do it fast and effortlessly for the person, possibly via networks.

Another problem is recovery from a loss of or damage to a personal device. Protection of personal data in a lost device can be achieved by strict access control and encryption. However, it is also important that the user should not need to spend a lot of time customising and "training" a new device; instead, the new device should itself load user preferences, contacts, favourite music, etc, from some back-up service, probably a home server, and do so in an effortless and secure way for the user.

5 Conclusions

Recent news reports suggest that large-scale surveillance by means of ubiquitous technologies (Internet and phones) has already started [22]. However, analysis of Ubicomp scenarios shows that privacy protection is not yet considered as a necessary design requirement despite the appearance of significant threats to personal privacy.

This paper has presented a model for privacy threats analysis for Ubicomp developers, and suggested guidelines for decreasing privacy threats. A typical approach to privacy threat analysis is to estimate sensitivity of data, which in turn depends on the application domain (e.g., health care data are considered sensitive) and on information consumers [13]. We suggest that privacy protection should also depend on which real-life privacy protecting borders are violated by the technology used, because the likelihood of acquiring sensitive data accidentally is high if technology penetrates through supposedly reliable physical borders. We suggest that developing strong access control methods both for humans and for software is crucial for privacy protection. We also suggest development of a unified, concise way of maintaining user awareness about application functionality, possibly graphical, and of user-friendly methods of presenting more detailed information about application functionality and how such functionality can be configured. Furthermore, we suggest development of ways to escape from being tracked by Ubicomp applications, so that such escape is not perceived as offensive or as a sign that someone has something to hide.

Since intelligent reasoning algorithms currently are less advanced than storage and transmission capabilities, technologies that are highly privacy-threatening should be limited to domains where they are justified by both domain requirements and existing personal data protection regulations, as in health care. In other domains, usage of such technologies should be under strict personal control, and applications should switch off automatically after a certain period of user inactivity. We also suggest

avoidance of highly privacy-threatening technologies in applications where the goal should be to increase the user's comfort (such as personalisation of TV), and use of less dangerous technology instead.

This paper is based on work done in the context of the SWAMI project [23].

References

1. Aschmoneit, P.; Höbig, M.,eds. (2002). Context-Aware Collaborative Environments for Next Generation Business Networks: Scenario Document, COCONET deliverable D 2.2.
2. Palmas, G.; Tsapatsoulis, N.; Apolloni, B. et al. (2001). Generic Artefacts Specification and Acceptance Criteria. Oresteia Deliverable D01. Milan: STMicroelectronics s.r.l
3. Savidis, A. et al. (2001). Report on Key Reference Scenarios. 2WEAR Deliverable D1.
4. Åkesson, K.-P.; Humble, J.; Crabtree, A.; Bullock, A. (2001). Usage and Development Scenarios for the Tangible Toolbox. ACCORD Deliverable D1.3.
5. Amigo scenarios: http://www.ctit.utwente.nl/research/projects/telematics/other/amigo.doc/
6. Kim, S. W.; Kim, M. C.; Park, S. H. et al. (2004): Gate reminder: a design case of a smart reminder. In: Benyon, D.; Moody, P. et al. (Eds.): Proceedings of the Conference on Designing Interactive Systems, Cambridge, MA, USA, August 1-4, 2004. ACM, pp. 81-90
7. Orr, R. J.; Raymond, R.; Berman, J.; Seay, F. (1999). A System for Finding Frequently Lost Objects in the Home, Technical Report 99-24, Georgia Tech.
8. Gemmel, J., Williams, L., Wood, K., Lueder, R., Bell, G., (2004) Passive Capture and Ensuing Issues for a Personal Lifetime Store, CAPRE 04
9. Langheinrich, M. (2001): Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In: Abowd, G. D.; Brumitt, B. et al. (Hrsg.): Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001). Berlin und Heidelberg,: Springer-Verlag (Lecture Notes in Computer Science, 2201), pp. 273-291.
10. Langheinrich, M. (2003): The DC-Privacy Troubadour – Assessing Privacy Implications of DC-Projects. In: Designing for Privacy Workshop. DC Tales Conference, Santorini, Greece.
11. Bohn, J., Coroama, V., Langheinrich, M., Mattern, F., Rohs, M., (2005) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing, In: W. Weber, J. Rabaey, E. Aarts (Eds.): Ambient Intelligence. Springer-Verlag, pp. 5-29.
12. Friedewald, M., Vildjiounaite, E., Punie, Y., Wright, D., Privacy, identity and security in ambient intelligence: A scenario analysis, Telematics and Informatics, In Press
13. Hong, J., Ng, J, Lederer, S., Landay, J., Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems, in DIS 2004
14. Lahlou, S.; Jegou, F. (2003). European Disappearing Computer Privacy Design Guideslines v1. Ambient Agora Deliverable D15.4. Electricité de France.
15. Nissenbaum, H. (2004), Privacy as Contextual Integrity, Washington Law Review 79, No.1
16. Camenisch, J., ed.,. PRIME Deliverable D16.1, 2005.
17. Bellotti, V., Sellen, A., Design for Privacy in Ubiquitous Comp. Environments, ECSCW'93
18. Nasoz, F., Alvarez, K., Lisetti, C., Finkelstein, N., (2003), Emotion Recognition from Physiological Signals for User Modelling of Affect, In Proceedings of the 3rd Workshop on Affective and Attitude User Modelling (Pittsburgh, PA, USA, June 2003)
19. Nabeth, T., et al., FIDIS Deliverable 2.2: Set of use cases and scenarios.
20. Knospe, H.; Pohl, H. (2004): RFID Security. In: Information Security Technical Report 9, No. 4, pp. 30-41
21. Cranor, L., P3P: Making Privacy Policies More Useful, IEEE Security and Privacy, 2003
22. http://www.aclu.org/safefree/nsaspying/23989res20060131.html
23. http://swami.jrc.es/pages/index.htm