Proxies for Privacy in Ambient Systems

Anders Kofod-Petersen
SINTEF ICT
Trondheim, Norway
akof@sintef.no

Jörg Cassens
University of Lübeck
Lübeck, Germany
cassens@imis.uni-luebeck.de

Abstract

The increased use of social-network services for sharing personal information has made it easier to gain awareness of each other. It has also increased the interest in privacy issues, especially since it is not always clear to the provider of information who gains access to personal data and to what end this data is being used. Many interesting ideas and proposals have appeared to address the issue of privacy vs. information sharing. One of the most interesting is perhaps the notion of minimising asymmetry of information flow. It is not obvious how this idea can be applied in the area of ambient assisted living since raising awareness of the situation of the information provider is a core feature for reaching the goal of enabling elderly and disabled people to stay in their own housing. The work described here argues how the asymmetry of information flow can be minimised without compromising on the quality of monitoring and with the added benefit of giving next-of-kin better access to expert evaluation of the situation of their family members. This paper also reports on some initiatives on location-aware systems and ambient assisted living and shows how the combined experiences gained from these projects have led to the development of the proposed model for minimising asymmetry by proxies in an ambient assisted living environment.

1 Introduction

The growth in the number of social-network applications available on the internet, such as Facebook, MySpace and LinkedIn and their increasing use of people's position as important information in the social graph has raised the attention given to location-aware systems. The inclusion of this location specific information has made such applications effectively location-aware. Location can either be explicitly stated by the user in services such as Facebook, set by using the web browser's geolocation API like with Twitter or directly sensed though location-based services such as Google's Latitude. The increasing specificity of location combined with the publicity of social networking raises many concerns about privacy.

The issue of privacy in online social networks is fairly well established and studied, although most of the existing body of research does not have an explicit focus on location specific data. Users who make conscious choices about what information they reveal to whom concerning data typically found on websites like Facebook or twitter follow certain patterns (see Section3), and it is reasonable to assume that such users will take a similar approach to revealing location data.

With the spread of *ubiquitous* [38], *pervasive* [16], and *ambient* [27] computing, the focus on privacy within these areas[1] has also increased. However, within the emerging field of *ambient assisted living* (AAL), the issue of privacy has only been cursorily addressed. Most of the work that has been done within ambient assisted living has proposed the solution of limiting access to data technically. This leaves the core issues of privacy concerns untouched; those of data ownership and control. To address this shortfall, findings on privacy on social networks in general will be correlated with work focusing on ambient systems. The work presented here takes the position that information privacy is a quintessential

[1] Recently the term *everywhere computing* [13] has also been introduced. Although all these terms are often used as synonyms, a particular term typically indicates a particular perspective, such as a physical distributed system perspective vs. a functional-oriented service perspective.

part of any person's privacy and dignity, and should therefore also be a concern for ambient assisted living.

One important approach to privacy is the principle of minimising asymmetry [18], which aims at levelling out the amount of information flowing between users and suppliers of systems. This principle might at first appear not to fit within a context of AAL. However, it is in fact important and can be employed by using a proxy.

Although the use of proxies provides a technical solution to privacy, when decisions about information disclosure are delegated to proxies, three crucial aspects of the relationship between the proxy and the client must be taken into account. First, consideration must be given to whether it might reasonably be expected that the people acting as proxies have a different stance on privacy issues, for example because of age differences or proficiency in new technologies. Second, it is worth looking at whether a trust relation between those whose information is disclosed and those who influence the amount of disclosure alleviates such differences. And last, the issue of whether those who act as proxies themselves have something to gain in doing so and the potential impact of this on their decision making must be considered.

2 Demographic Trends

The need for solutions in ambient assisted living and the relation between different stakeholders can be better understood in relation to developments in the population structure of industrial countries. Given the projected demographic trends, it can be argued that connectedness between family members is going to be important for families in the near future. Muenz states that the demographic process in Europe "can be characterized as a gradual shift from a society with quantitatively dominant younger cohorts to a society in which the elderly form a solid majority" [32]. A likely scenario will see the median age of the population in the European Union to have risen to 48 years, up from 38.5 in 2005 [32]. The author expects the ratio between the older and the younger population to change from 100 people in the working age range 15–65 to 25 people of age 65 and up in 2005 towards 100 younger people to 51 older in 2050 [32].

Gaymu et al. examine issues of care needs of dependent older adults for nine European countries based on projections for future development until 2030 [11]. They expect that the proportion in the ageing population requiring professional care will grow slower than those with at least the potential of being supported by family. These trends will make the need for children to care for their parents more pronounced. Consolvo et al. classify caretakers based on the impact that carers allow care giving to have on their own lives: the drastic life changer will often sacrifice career or hobbies, the significant contributor will see a profound impact, but with his own life still in focus, and the peripherally involved will provide sporadic care [5].

To support the caregivers and at the same time make it possible for the elderly to live a life they feel they are in charge of, ambient assisted living technologies should cater for the social needs for connectedness, support medical supervision, especially if and when mental or bodily conditions deteriorate, and protect the privacy of all people involved.

3 Related Work

Ambient systems deliver the technological base for realising awareness systems, that is systems which make information about for example ones status, location, or health available to others. Such systems are useful for keeping in touch with other people in ones social network, giving the user the feeling of being connected. Both industry and research have explored the options to fulfil the need to stay in touch using mobile and ambient devices [8, 34, 37].

What constitutes awareness is depending on the application domain. One area where the issue of awareness has been in the focus is computer supported cooperative work (CSCW), looking at the information one user of a CSCW-system has about other users of the same system. Dourish and Bellotti define awareness as an "understanding of the activities of others, which provides a context for your own activity" [9]. Gutwin at al. distinguish between (1) Informal Awareness, (2) Social Awareness, (3) Group-Structural Awareness and (4) Workspace Awareness [15].

While these definitions already include aspects, which later became important in Ambient Assisted Living, they are still very much targeted at more efficient and effective workplace environments. Targeting a different application domain, Keller et al. developed a "gustbowl" [20], two bowls at the homes of different family members that were interconnected. If one person threw something in one of the flexible bowls, the other would mimic the movement of the first and display a picture of the action which led to the movement. This created an awareness of each other's activities in order to create an emotional bond between family members. Dey and de Guzman call this effect connectedness [8]. The authors consider that giving somebody more information about ones state, thus creating awareness, is a means to an end: they use peripheral awareness displays of information, thereby supporting the feeling of being connected to a remote friend whose activity is being displayed.

Dadlani et al. target the peripheral awareness with their Aurama system, a photo frame displaying awareness information about other people [7]. They conducted extensive user studies when designing their system. Two interesting observations they report on are: (1) that the children did like to have information about their parents status, but not in the form of full traces or logs since they regarded that as an invasion of privacy, and (2) that they recognised the importance of monitoring vital signs, but would prefer to have access to aggregated information reviewed by an expert, like a medical doctor.

A proposed solution to the problem of balancing the wish for sharing information with the need for control of the information flow can be found in the focus-nimbus model, originally described by Benford et al. [3]. The authors use room metaphors as the foundation for a spatial model to support communication between participants in virtual rooms. The basic idea is that people cannot only visit different virtual rooms, but they can move around in these different rooms, and the (modelled) spatial characteristics of the rooms mediate the communication between different persons in the room. Two concepts are introduced: (1) the focus represents a space in the room where a person targets his attention. People are more aware of objects in the focus than those outside. (2) The nimbus is the counterpart, representing where the person locates himself in the room. Objects are more aware of a person if the object is located in the person's nimbus than when it is located outside [17, p. 220].

Awareness of people is defined through the interaction of focus and nimbus, and can be mathematically expressed through the spatial relation of a focus and a nimbus. This model has been generalised by Rodden [36]. He extends the notions of focus and nimbus towards application areas without an explicit notion of spatial relations. Basically, he introduces a graph model for a domain, and awareness becomes a property of this graph. In its simplest form, the awareness measure is the length of the path between two users. Metaxas and Markopoulos have later presented a formal model which concentrates on the communication aspects of the focus-nimbus model [30]. Their model addresses issues of privacy for example by allowing deception, e.g. not telling the truth about ones status or blurring the information relayed. Such an approach is problematic for the ambient assisted living setting, where correct information is crucial for assessing the status of the person being assisted.

The question remains whether users feel a need for privacy, or whether the introduction of privacy measures is mostly due to government regulation. It is an often held belief that users of online social networks do not care about privacy. This is supported by the fact that most users do not change the privacy settings on sites like Facebook, even when the defaults for these are changed in a way that reveals more information about the site's users [14]. Recent research, however, has focused on elements that refute these claims. Madden and Smith, for example, conducted a survey where they assessed that "more than two-thirds (71 %) of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online" [28].

This finding that young users are indeed concerned with privacy is supported by other work. Marwick et al. have published an extensive literature review on quantitative and qualitative empirical studies of children, teenagers, and younger college students [29]. They observe that many studies focus on online risk without taking into account the need of younger people for private space "where they can socialize away from the watching eyes of parents, teachers or marketers" [29]. For the authors, the distinction of public and private spheres seem outdated in the perception of young users, which influences their way of choosing privacy setting. The authors conclude that their review of the literature suggests that young people care especially deeply about privacy when it comes to groups like parents or teachers. Publication of private information, however, to members of their social graph is a way to express themselves, increase their reputation and bond with their peers.

Boyd and Hargittai come to a similar conclusion when they compare surveys on the use of Facebook's privacy settings in 2009 and 2010, covering a period of time when Facebook's attitude towards privacy was actively debated in the media. The authors assess an increase in the percentage of users who have actively changed the privacy setting during this year [4]. Boyd and Hargittai also found a correlation between expertise and frequency of use and willingness to change privacy settings.

Privacy is an ambiguous term, therefore, when talking about privacy in the context of information disclosure, the meaning of the concept has to be made clear. Westin defines privacy "as the claim of an individual to determine what information about himself or herself should be known to others" [39, 40]. The author explicitly acknowledges that privacy can be achieved in a group setting, pointing at the possibility of intimacy in a small group while at the same time withdrawing from society at large. In the light of technological advances, Nissenbaum identifies three concerns towards privacy: (1) monitoring and tracking, (2) dissemination and publication, and (3) aggregation and analysis [33]. All of these challenges have to be considered when talking about privacy in AAL settings.

Langheinrich [24] describes why privacy is particularly important in ubiquitous computing by pointing out four built-in properties of ubiquitous computing, which differentiate them from traditional systems: *ubiquity*, the computer is everywhere; *invisibility*, the computer disappears; *sensing*, the sensors are becoming more accurate and plentiful; and *memory amplification*, which is the ability to store large amount of data.

When using ambient systems, the hidden nature of the computer will also work as an implicit communication channel. That is, the user's environment will be communicating with any number of potentially unknown entities. In this sense the disappearing computer works as a mediator for communication between humans. Something which will lead to a loss of mutual awareness [2] by breaking down the intuitive principle of: "if I cannot see you then you cannot see me". Bellotti and Sellen [2] argue that to counteract this loss of awareness and potential loss of privacy, control and feedback are the two main concepts that should be employed.

The idea of control and feedback has been, in some sense, formalised by Jiang et al. [18], who define the principle of minimal asymmetry, which states that (original emphasis):

> "A privacy-aware system should minimize the asymmetry of information between **data owners** and **data collectors and data users**, by:
>
> **Decreasing** the flow of information from data owners to data collectors and users.
> **Increasing** the flow of information from data collectors and users back to the data owners."
> [18, p. 7]

Minimising asymmetry in information flow is based on assumptions that are not necessarily met in other models addressing privacy issues. For example, systems following the focus-nimbus model might allow an information flow where the originator of the information is not even aware that private information is being sent [30], it is enough that the receiver of the information is in proximity of the sender with regard to the distance measure chosen.

A model focusing on the symmetry between sender and receiver assumes that by decreasing the information flow from the data owners the user gains better control over the systems. By contrast, increasing the flow of information from the data collector provides a feedback mechanism.

Lederer et al. [25] even argue that control and feedback are essential to the design of systems. Using the combination of control and feedback is a way of inspiring understanding and action. The authors also define five pitfalls in design, which should be avoided:

1. Obscuring potential information flow, systems must make clear what possible disclosures they can make, such as what types of disclosures are possible, who can receive it.

2. Obscuring actual information flow, systems must make clear what is actually disclosed.

3. Emphasising configuration over action, privacy management should follow as a consequence of the user's ordinary use.

4. Lacking coarse-grained control, configuration should allow for typically binary choices and not force the user to micro-manage all configurations.

5. Inhibiting existing practice, computer systems should try to adapt to existing practices in social interaction.

Privacy is achieved through introducing several methods of selectively making awareness states available. Work by Lederer et al. shows that the "identity of the information inquirer is a stronger determinant of privacy preferences than is the situation in which the information is collected" without completely ignoring the influence of the situation [26].

This is supported by results from a study by Consolvo et al. who conclude that users wanted to "determine whether and what to disclose about their location to requests from social relations: *i.e.*, *who* is requesting, *why* do they need to know, *what* would be most useful to them, and *am I willing* to share that?" [6]. The authors describe a study with 16 non-technical participants at Intel Research, Seattle. The study concluded that who is this recipient is the most important factor when people decide what information to disclose. People were willing to share their location with their significant other (disclosed location for 93 % of the requests); followed by friends (85 %); and family (85 %). People were much less inclined to share their location with co-workers (54 %) and manages (34 %). Users rarely disclosed location data on a coarser level of detail to protect their privacy. Participants either disclosed their location in the level of detail most useful for the requester, or not at all.

Jones and Grandhi [19] present a survey conducted at various places on Manhattan, where more than 500 participants were asked about their willingness to disclose location data. Of the respondents, 84 % were willing to (anonymously) share their location data to get information about crowding and occupancy in public places; 77 % were willing to let others know their current location in public and semi-public places; 69 % to family and friends; 32 % to colleagues and 17 % to strangers. The authors concluded that a large portion of the population perceives location-aware systems as sufficiently beneficial to share position data.

4 Privacy in Location-aware Social-networks

Systems that link people to people and people to geographical locations have been called P3 systems [19]. According to Jones and Grandhi [19], P3 systems can be split into two groups: people-centred and place-centred. People-centred systems use absolute position, co-location or proximity to convey information about peoples' whereabouts. Place-centred systems link virtual places to physical locations.

Recent research into P3 systems in the form of location-aware social-networks by researchers in Trondheim has focused on implementing place-centred applications to be used either indoors or in limited geographical areas. Three main systems have been developed and used to investigate privacy concerns. The following three paragraphs briefly describe these systems and the main conclusions that they draw with respect to privacy.

FindMyFriends is a place-centred location-aware social network system that was installed during a three week student festival in Trondheim, Norway [21]. In brief, this system offered the potential of keeping track of your friends in the main venue of the festival. It consisted of a physical ultra-sound tag used for positioning, one web-based interface for on-site terminals, and another one for off-site access. Beside allowing users to see each others' position it was also possible to send icons to each other (see [23] for an analysis of the usage).

The only privacy mechanism implemented was the ability to block a user. However, the implicit option of plausible deniability was also possible since obscuring the tag would hinder the system's ability to locate a user.

FindMyFriends had 2769 registered users, 1661 of theses had a registered tag. Of these 207 chose to respond to the questionnaire. The main finding regarding privacy is that the students did not perceive a location-aware system as an invasion of their privacy. Actually, only 1.4 % felt that their privacy had been disturbed. Only 4 % did report on using the blocking feature. In addition, only 9.7 % would use a functionality to lie about one's position if it had been implemented. Finally, 55 % reported that they would use a similar system on a city-wide scale (for a more thorough analysis see [21]). Taken together, these findings suggest that users find that the benefits of such a system outweigh any negative aspects.

The FriendRadar [12] is a positioning systems that allows users to maintain a list of friends and be able to see their location within the city of Trondheim. The system was implemented as a server side solution accessible by a web-browser. The client used was iPod touch and the system was implemented within the Wireless Trondheim environment [1].

The system approached the principle of minimum asymmetry by implementing the following rules:

1. Three privacy levels are available
   (a) *Map privacy level* allows a friend to locate the user on the map.
   (b) *Nearby privacy level* allows friends to know if they are nearby (within 200 m).
   (c) *Blocked privacy level* shows no location information.
2. The strictest level of privacy chosen by one of two friends applies symmetrically.
3. A friend's location can only be seen if the system can localise the user.
4. *Plausible deniability* was facilitated by allowing for positioning to be turned on and off.

FriendRadar was tested among 24 pupils at an upper secondary school in Trondheim for a three week period. Data was gathered by data-log analysis and questionnaire.

The main finding here was that users were not really concerned with privacy issues. Neither were they overly concerned with future systems that could locate them everywhere. The pupils were more interested in the “coolness” of the application than in any privacy issues. There is, however, quite a lot of uncertainty in these results. Due to some technical problems during the test period the usage was not high. Thus, the results of this project are only indicative. However, the findings are in line with results from Jones and Grandhi [19] and Consolvo et al. [6] (see above).

The Find Peer Anton application mimics the Friend Radar system, with the notable exception that it utilises the underlying TCP/IP-network capabilities (realised via GRPS, UMTS and Wi-Fi) of a mobile phone. The application gives the user the opportunity to sort friends in groups, locate one’s friend or a whole group on the map and also to be able to send messages to contacts or whole groups. The application provides feedback about the locations of the peers of a user by indicating their proximity using colours ranging from red to green and by showing their position on a map [22]. Managing friends and their information is done through subscribing to each user’s information.

The system minimises the asymmetry by implementing the following features:

1. Subscribing to another’s presence or location information is only possible by mutual sharing.
2. Being invisible stops the user from receiving other users’ information.
3. Cancelling a subscription removes the cancelled user form the list and marks the cancelling user as offline in other users’ list.

Find Peer Anton is implemented as a server-client solution, where each mobile phone runs a small footprint application. The system has unfortunately not been evaluated besides simple functionality-testing.

The main observation made in the three works described above is that usefulness, or coolness, outweighs users’ need for privacy. These three examples all dealt with systems where people are sharing their location information with peers. Thus, following Consolvo et al. [6], Jones and Grandhi [19], and Marwick et al. [29], it is expected that people were willing to share location information with their friends. What is not clear is how people would respond to sharing information to others than their friends and family.

5 Privacy in ambient assisted living

The findings from the P3 systems and the issues of minimal asymmetry investigated in the above research raised some interesting questions for domains such as assisted living for the elderly. One interesting problem arises in the context of ambient assisted living (AAL), where the users, typically elderly people, are to be expected to share a considerable amount of personal information. This is not restricted to location information but does also include biometric data, such as blood pressure. From the literature referred to in the related work section and, to some degree, in the three experiments described above, the questions of benefit vs. privacy, and sharing with non-peers are still unanswered.

Work conducted in the health informatics group at SINTEF on the M·Power project [35] deals with an ambient assisted living environment where privacy is of utmost importance. The project, which has ended recently, has been conducted under the 6^{th} framework programme financed by the EU. The main objectives were: to construct a collaborative environment for distributed and shared care, providing requirements for information security, information models, context awareness, usability and interoperability; and a smart house environment, providing requirements for information security, information models and usability. Part of the M·Power project is currently continued in the *universAAL*[2] project under the 7^{th} framework programme.

[2] http://www.universaal.org/

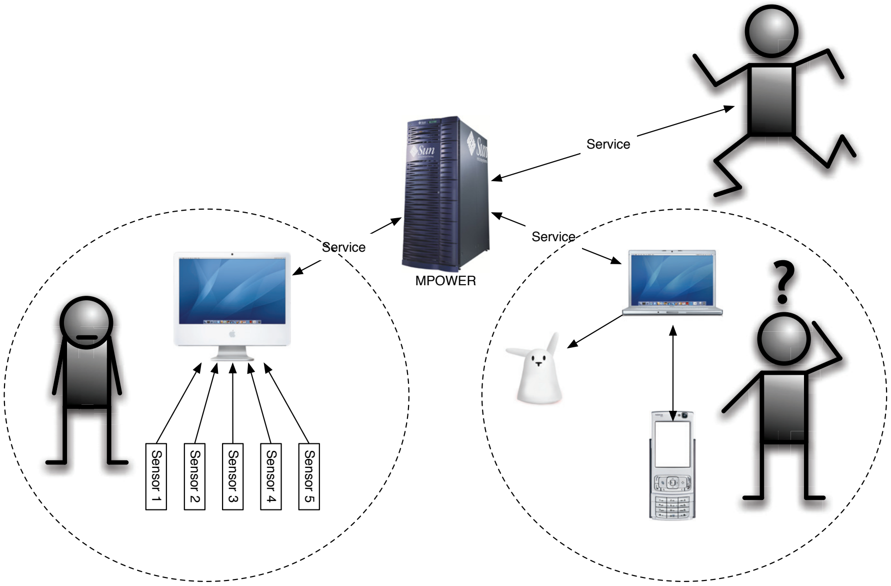

Figure 1: Overview of the M·Power system

A result of this project is an open source SOA-based platform[3] for building web-service based applications, which can be used to implement AAL [31].

One of the demonstrators implemented was a touch-screen based terminal made available to elderly with dementia living at home. This application has been very well received by both the elderly and their next-of-kin, and is recognised as an important tool for allowing people to continue to live at home and maintain a meaningful existence[4]. Interestingly, and in line with the research described in Section4, the usefulness of the application greatly outweighed any privacy concerns both by the users and their family.

Figure 1 depicts a rough sketch of the M·Power setup. The AAL environment is located to the left, where a, typically elderly, user is equipped with the touch-screen terminal as well as one or many sensors. Each of the sensors is available as a service in the SOA world. Any meaningful combination of these sensors can be used as a monitoring tool, primarily for the health care provider, seen at the upper right corner of the figure. The next-of-kin, lower centre, has the option to access information from the system via a number of interfaces. The implementation of the M·Power system showed that it was not only the elderly who regarded the system as useful, but perhaps even more the next-of-kin.

Currently, privacy has only been dealt with on the level of only giving access to those that should have access. However, some issues are still unresolved. Among these the most important issue is perhaps the issue of asymmetry. In an AAL environment the inhabitant is clearly primarily, if not only, a data owner. Whereas the health care service is primarily a data collector and user. This asymmetry is perhaps not obvious, in particular when dealing with elderly with dementia. However, as Jiag et al. [18] point out in their example of Bob and Carol, the service provider knows much more about the use of the data gathered than the owner. This asymmetry might be accepted by weighing the benefits against the lack of control. However, as Duckham and Kulik [10] point out, information privacy goes beyond mere technical feasibility and rather follows the definition by Alan Westin [39], who argues that privacy is the fact that the data owner controls how data collectors and users use the information collected.

The health care sector is typically strictly regulated, in particular with respect to information security.

[3] `http://sourceforge.net/projects/free-mpower/`

[4] The results are currently being prepared for publication.

However, privacy mechanisms in complicated systems should perhaps go beyond current legal boundaries and embrace privacy as a means of usability, e.g. inspiring understanding and action as described by Lederer et al. [25].

6 Minimum Asymmetry by Proxy

Many people, in particular elderly living with dementia, will not benefit from using systems that attempt to minimise information asymmetry. Actually, in the case of dementia, it is likely to be counter productive to supply too much information to the end-user.

If we follow the analysis by Jiag et al. [18] and apply it to the case of AAL we can either decrease the information flow from the AAL environment to the health care service provider or increase the flow of information from the health care service provider to the user of the AAL environment.

Except for a strict access control, decreasing the information from the AAL environment is counter intuitive as the whole point is monitoring of important, if not vital, information about the inhabitant. The same argument holds for anonymising or even pseudonomising, which can be counter productive.

Increasing the information flow from the health care provider to the user of the AAL environment appears to be the option of choice. One example of information that might flow back to the user is access information, that is, information about who accessed what information and when. This is also known from contemporary electronic patient health records. However, as described above, it is likely to be counter productive to inform the user of the AAL environment. Experience gained through the M·Power project shows that even simple actions such as logging in to a system is far outside the scope of what elderly with dementia are capable of. So explicitly giving access to log information is simply not useful, rather quite the opposite.

As argued by Westin [39], control of your own information is an essential aspect of privacy. Thus, some way of maintaining privacy is required as well as control and feedback. We argue that a primary carer or next-of-kin might be a natural *proxy* for the elderly. Figure2 depicts the relationship between the elderly, in the top left corner, the next-of-kin, in the middle, and the care facility, at the far right. If we consider an ambient assisted living environment minimising asymmetry by using proxies, monitoring information will flow from the elderly to the health care provider, whereas the increased flow of information from the data collector and user can be achieved by informing the proxy.

Following Dadlani et al. [7], the next-of-kin would appreciate to have access to an awareness system enhancing their feeling of connectedness. At the same time, they do actually prefer to get aggregated, expert-reviewed reports and not raw data. This would increase the information flow towards the proxy since the reports would also state how information acquired by the medical experts was used, such as who uses what, when and why. This type of information will initially give feedback about the system and its information usage, and will lead to a better control over the acquisition of information besides the increased feeling of connectedness.

This approach opens up two main concerns that have to be considered: *i*) the issue of the health care provider acting as a data owner and the proxy as a data user; and *ii*) any relationship as owner, collector or user between the elderly and the next-of-kin.

In the first case, it could be argued that when the health care providers supply information about their states and processes to the proxy an issue of asymmetry might arise. The health care providers can be seen as data owners and the proxy as data user. However, even though the proxy can be seen as a third party, that would by counter productive from the perspective of the end user of the AAL environment. Further, the data supplied by the health care service is a function of the data gathered from the end user and in particular of the service provided. Thus, information flowing to the proxy should be seen as increasing information flow back to the data owner.

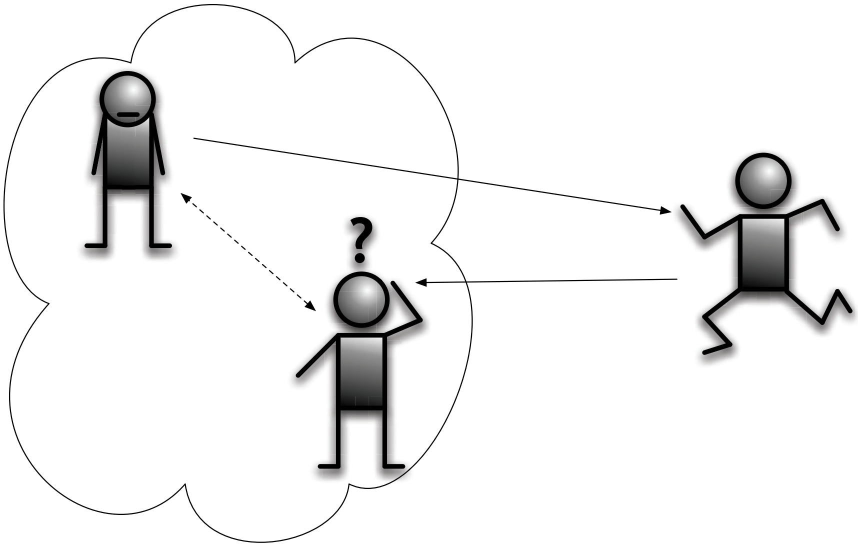

Figure 2: Minimising asymmetry by proxy

The second case of the relationship between the elderly and the next-of-kin is far more complicated. The simplest case is also the most extreme, where the elderly resident has been declared legally incompetent. However, these cases are, luckily, rare. Designers of AAL systems that rely on proxies must assume benign family relationships, and allow the end-user the final saying in whether or not a proxy should be used.

With what we know about the use of online social networking platforms by the tech-savy, younger generation as cited above, we are confident that the next-of-kin will view the information exchange in the light of smaller, intimate, peer-to-peer sub-groups. There is also evidence to support the hypothesis that parents are in principle willing to make personal information available to their children. In any case, the idea of a proxy for information flow should be an integrated part of any AAL system.

7 Summary and Further Work

The main argument presented here is that minimising information asymmetry is an important tool for maintaining privacy in ambient assisted living and other environments. The main tool for minimising asymmetry in AAL systems is to increase the information flow from the data collector and user. However, many current and future users of AAL systems are not capable of using such information. Thus, the notion of a proxy in the form of a next-of-kin is suggested.

Such a notion is easily manageable without introducing anything but engineering issues. It has been argued that using a proxy does not increase any significant complexity to the core idea of symmetric information flow.

The use of proxies is at an early stage. Even though existing AAL systems, such as the M·Power system, already implement some concept of proxies, it is important that the concept is included in the design of any system. Failing to do so will likely lead to falling into many of the well-know pitfalls of AAL system design.

The technical details of how to implement proxies in the AAL setting are currently being investigated through the aforementioned *universAAL* project, as well as the recently started Co-Living[5] project under the Ambient Assisted Living (AAL) Joint Programme. The latter is focusing on the social connectivity of the elderly. The goal is to support and enhance the social life through the use of awareness technologies. This research represents ongoing work and details resulting from this research will be presented as they come to hand.

Acknowledgements

The authors would like to thank the reviewers for their feedback on the paper draft and Rebekah Wegener for her suggestions for and assistance with the final version.

References

[1] Steinar H. Andresen, John Krogstie, and Thomas Jelle. Lab and research activities in wireless trondheim. In *Proceedings of IEEE International Symposium on Wireless Communication Systems*, pages 385–389. IEEE Computer Society, 2007.

[2] Victoria Bellotti and Abigail Sellen. Design for privacy in ubiquitous environments. In Giorgio De Michelis, Carla Simone, and Kjeld Schmidt, editors, *Proceeding of the Third European Conference on Computer-Supported Cooperative Work (ECSCW '93)*, pages 77–92. Kluwer Academic Publishers, 1993.

[3] Steve Benford, Adrian Bullock, Neil Cook, Paul Harvey, Rob Ingram, and Ok-Ki Lee. From rooms to cyberspace: models of interaction in large virtual computer spaces. *Interacting with Computers*, 5(2):217–237, 1993.

[4] Danah Boyd and Eszter Hargittai. Facebook privacy settings: Who cares? *First Monday*, 15(8), August 2010.

[5] Sunny Consolvo, Peter Roessler, and Brett E. Shelton. The carenet display: Lessons learned from an in home evaluation of an ambient display. In Nigel Davies, Elizabeth D. Mynatt, and Itiro Siio, editors, *Ubicomp*, volume 3205 of *Lecture Notes in Computer Science*, pages 1–17. Springer, 2004.

[6] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 81–90, Oregon, USA, 2005. ACM.

[7] Pavan Dadlani, Alexander Sinitsyn, Willem Fontijn, and Panos Markopoulos. Aurama: caregiver awareness for living independently with an augmented picture frame display. *AI & Society*, 25(2):233–245, 2010.

[8] Anind K. Dey and Ed de Guzman. From awareness to connectedness: the design and deployment of presence displays. In Rebecca Grinter, Thomas Rodden, Paul Aoki, Ed Cutrell, Robin Jeffries, and Gary Olson, editors, *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 899–908. ACM Press, 2006.

[9] Paul Dourish and Victoria Bellotti. Awareness and coordination in shared workspaces. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work - CSCW '92*, pages 107–114, New York, New York, USA, 1992. ACM Press.

[10] Matt Duckham and Lars Kulik. Location privacy and location-aware computing. In Jane Drummond, Roland Billen, Elsa João, and David Forrest, editors, *Dynamic & Mobile GIS: Investigating Change in Space and Time*, pages 34–51. CRC Press, 2006.

[11] Joëlle Gaymu, Peter Ekamper, and Gijs Beets. Who will be caring for europe's dependent elders in 2030? *Population (english edition)*, 62(4):675–706, 2007.

[12] Per Anton Gransæther. Privacy in location-aware systems for social interaction. Master's thesis, Department of Computer and Information Science, Norwegian University of Science and Technology (NTNU), 2008.

[13] Adam Greenfield. *Everyware: The Dawning Age of Ubiquitous Computing (Voices That Matter)*. New Riders Publishing, 2006.

[5] `http://www.project-coliving.eu/`

[14] Ralph Gross and Alessandro Acquisti. Information revelation and privacy in online social networks. In *WPES '05: Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, pages 71–80, New York, NY, USA, 2005. ACM.

[15] Carl Gutwin, Saul Greenberg, and Mark Roseman. Workspace awareness in real-time distributed groupware: Framework, widgets, and evaluation. In *HCI '96: Proceedings of HCI on People and Computers XI*, pages 281–298, London, UK, 1996. Springer-Verlag.

[16] Uwe Hansmann, Lothar Merk, Martin S. Nicklous, and Thomas Stober. *Pervasive Computing: The Mobile World*. Springer Professional Computing, 2003.

[17] Steven Harrison and Paul Dourish. Re-place-ing space: The roles of place and space in collaborative system. In Gary Olson, Judy Olson, and Marks S. Ackerman, editors, *Proceedings of the 1996 ACM Conference on Computer Supported Cooperative work*, pages 67–76. ACM Press, 1996.

[18] Xiaodong Jiang, Jason I. Hong, and James A. Landay. Approximate information flows: Socially-based modeling of privacy in ubiquitous computing. In Gaetano Borriello and Lars Erik Holmquist, editors, *Proceedings of the 4th International Conference on Ubiquitous Computing (UbiComp 2002)*, volume 2498 of *Lecture Notes in Computer Science*, pages 176–193. Springer Verlag, 2002.

[19] Quentin Jones and Sukeshini A. Grandhi. P3 systems: Putting the place back into social networks. *IEEE Internet Computing*, 9(5):38–46, 2005.

[20] Ianus Keller, Wouter van der Hoog, and Pieter Jan Stappers. Gust of me: Reconnecting mother and son. *IEEE Pervasive Computing*, 3(1):22–27, 2004.

[21] Anders Kofod-Petersen, Per Anton Gransæther, and John Krogstie. An empirical investigation of attitude towards location-aware social network service. *Int. J. Mobile Communications*, 8(1):55–70, 2010.

[22] Anders Kofod-Petersen, Espen Klæboe, Jørgen Jervidalo, Kjetil Aaltvedt, Magnus Romnes, and Trond Martin Nyhus. Implementing privacy as symmetry in location-aware systems. In Gabriele Lenzini, Bob Hulsebosch, Santtu Toivonen, and Jean-Marc Seigneur, editors, *Proceedings of the International Workshop on Combining Context with Trust, Privacy and Security (CAT 2008)*, volume 371, pages 1–10, Trondheim, Norway, June 2008. CEUR Workshop Proceedings.

[23] Anders Kofod-Petersen and Rebekah Wegener. Like a poke on facebook emergent semantics in location-aware social network services. In Rotimi Taiwo, editor, *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction*, chapter 32. IGI Global, 2010.

[24] Marc Langheinrich. Privacy by design – principles of privacy-aware ubiquitous systems. In G. D. Abowd, B. Brumitt, and S. Shafer, editors, *Ubicomp 2001: Ubiquitous Comp*, volume 2201 of *Lecture Notes in Computer Science*, pages 273–291. Springer, 2001.

[25] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and action: five pitfalls for designers. *Personal and Ubiquitous Computing*, 8(6):440–454, 2004.

[26] Scott Lederer, Jennifer Manko, and Anind K. Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03: CHI '03 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2003.

[27] Artur Lugmayr. The future is 'ambient'. In Reiner Creutzburg, Jarmo H. Takala, and Chang Wen Chen, editors, *Proceedings of SPIE*, volume 6074 of *Multimedia on Mobile Devices II*. SPIE, 2006.

[28] Mary Madden and Aaron Smith. Reputation management and social media. Technical report, Pew Internet & American Life Project, 2010.

[29] Alice E. Marwick, Diego Murgia-Diaz, and John G. Palfrey Jr. Youth, Privacy and Reputation (Literature Review). *Berkman Center Research Publication No. 2010-5*.

[30] Georgios Metaxas and Panos Markopoulos. 'aware of what?' a formal model of awareness systems that extends the focus-nimbus model. In *Proceedings of the IFIP conference EHCI 2007*. Springer, 2007.

[31] Marius Mikalsen, Sten Hanke, Thomas Fuxreiter, Ståle Walderhaug, and Leendert Wienhofen. Interoperability services in the M·POWER ambient assisted living platform. In *Proceedings of the Medical Informatics Europe (MIE) Conference 2009*, Sarajevo, Bosnia and Herzegovina, August 2009.

[32] Rainer Muenz. *Aging and Demographic Change in European Societies: Main Trends and Alternative Policy Options*. Number 0703 in SP Discussion Paper. Social Protection Advisory Service– The World Bank, Washington, DC, USA, 2007.

[33] Helen Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2009.

[34] Sobah A. Petersen, Monica Divitini, and George Chabert. Identity, sense of community and connectedness in a community of mobile language learners. *ReCALL Journal on Mobile Assisted Language Learning (MALL)*, 20, 2008.

[35] Andreas Pitsillides, Eleni Themistokleous, George Samaras, Ståle Walderhaug, and Ole Martin Winnem. Overview of M·POWER: Middleware platform for the cognitively impaired and elderly. In *Proceedings of IST-Africa 2007 Conference & Exhibition*, Maputo, Mosambique, May 2007.

[36] Tom Rodden. Populating the application: A model of awareness for cooperative applications. In *CSCW '96: Proceedings of the 1996 ACM conference on Computer Supported Cooperative Work*, pages 87–96, New York, NY, USA, 1996. ACM Press.

[37] Natalia Romero, Panos Markopoulos, Joy van Baren, Boris de Ruyter, Wijnand Ijsselsteijn, and Babak Farshchian. Connecting the family with awareness systems. *Personal and Ubiquitous Computing*, 11(4):299–312, 2006.

[38] Mark Weiser. The computer for the 21st century. *Scientific American*, pages 94–104, September 1991.

[39] Alan F. Westin. *Privacy and freedom*. Atheneum, 1967.

[40] Alan F. Westin. Social and political dimensions of privacy. *Journal of Social Issues*, pages 431–453, 2003.

Anders Kofod-Petersen holds a Doctorate in Computer Science from the Norwegian University of Science and Technology (NTNU). He is currently employed as a Senior Research Scientist at the research foundation SINTEF and as an associated professor at NTNU. His research interests include knowledge-intensive case-based reasoning, cognitive science and explanation-aware computing. His recent research has been focused on using socio-technical theories in modelling and representation of knowledge in mobile and ambient intelligent systems.

Jörg Cassens is a lecturer and senior researcher at the University of Lübeck, Germany. He works in artificial intelligence and human-computer interaction on issues of integrating intelligent systems into human work processes with a focus on ambient intelligence, awareness systems, and knowledge-intensive case-based reasoning. His main research interests are the applicability of socio-technical theories for the design of intelligent systems and the role of explanations for the user and for the system. He has worked on the development of psychologically sound context models and on requirements engineering methodologies for intelligent systems.