

Minimising Information Asymmetry by Using Proxies

Anders Kofod-Petersen
SINTEF ICT
S. P. Andersens vei 15b
7465 Trondheim, Norway
Email: akof@sintef.no

Abstract—The fast growing number of social-network services utilising location information has also increased the interest in privacy for such systems. Many interesting ideas and proposals have appeared. One of the most interesting is perhaps the notion of minimising asymmetry of information flow. This idea can also be applied in the area of ambient assisted living. The work described here reports on some initiatives on location-aware systems and ambient assisted living. The combined experiences gained from these projects have led to the development of a model for minimising asymmetry by proxies in an ambient assisted living environment.

I. INTRODUCTION

With the spread of *ubiquitous* [1], *pervasive* [2], and *ambient* [3] computing, the focus on privacy within these areas¹ has also increased. The specific sub-group called location-aware systems has received quite a lot of attention. This is in part due to the growing number of social-network applications available on the internet, such as Facebook, MySpace and LinkedIn, and their recent use of people’s position as an important part of these social networks, in effect making them location-aware. Location can either be explicitly stated by the user in services such as Twitter or Facebook, or directly sensed through location-based services such as Google’s Latitude.

However, within the emerging field of *ambient assisted living* (AAL), privacy has only been touched upon briefly. Most of the work that has been done within ambient assisted living has been to limit access to data technically. Not so much work has been done on the underlying issues about data ownership and control. The work presented here takes the position that information privacy is a quintessential part of any person’s privacy, and should therefore also be an underlying issue in ambient assisted living.

One important approach to privacy is the principle of minimising asymmetry [5], 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.

The rest of this paper is organised as follows: initially an overview of work related to privacy in ubiquitous computing

and minimal asymmetry is presented. Section III describes some of the work that has led up to the current work on privacy in ambient assisted living. Section IV describes the ambient assisted living M-Power project. Section V describes the suggested use of proxies. The paper ends with a summary and outlook on future work.

II. RELATED WORK

Recent research into location-awareness and privacy has found that users are very concerned with privacy and will explicitly weigh up the benefits of the new technology against issues of privacy. Further, there seems to be a close coupling between the closeness of users and their wish to disclose location information.

Langheinrich [6] described 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 implicit communication channels. 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 [7] by breaking down the intuitive principle of: “if I cannot see you then you cannot see me”. Bellotti and Sellen [7] 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. [5], who define the principle of minimal asymmetry, which states that ([5, p. 7] (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.

¹Recently the term *everywhere computing* [4] has also been introduced. Although all these terms can be viewed as synonyms, a particular term typically indicates a particular perspective, such as a physical distributed system perspective vs. a functional-oriented service perspective.

Increasing the flow of information from data collectors and users back to the data owners.”

By decreasing the information flow from the data owners the user gets better control over the systems. By contrast, increasing the flow of information from the data collector provides a feedback mechanism.

Lederer et al [8] 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 users 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.

Both Lederer et al. [9] and Consolvo et al. [10] also demonstrated that, with respect to privacy concerns, the identity of the information recipient is of greater importance than the situation which the user is in.

Consolvo et al. [10] 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 managers (34 %). Users rarely disclosed location data in a more coarse 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 [11] 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.

III. PRIVACY IN LOCATION-AWARE SOCIAL-NETWORKS

Systems that link people to people and people to geographical locations have been called P3 systems [11]. According

to Jones and Grandhi (2005), 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 [12]. 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 ultrasound tag used for positioning, a web-based interface for on-site terminals, and one for off-site access. Beside allowing users to see each others' position it was also possible to send icons to each other (see [13] 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 these 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 reported 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 [12]). Taken together, these findings suggest that users find the benefits of such a system outweigh any negative aspects.

The FriendRadar [14] 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 [15].

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 here are only indicative. However, the results are in line with results from Jones and Grandhi [11] and Consolvo et al. [10] (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 (such as 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 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 [16]. Managing friends and their information is done by 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 from 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. [10], and Jones and Grandhi [11], it is expected that people were willing to share with their friends. What is not clear is how people would respond to sharing information to others than their friends and family.

IV. 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 issues for situations such as assisted living for

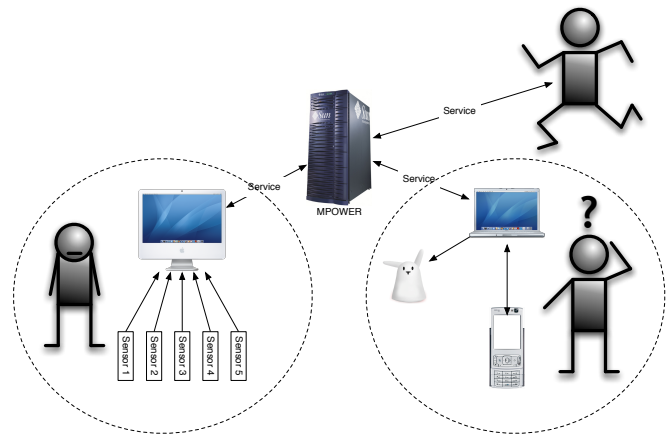


Figure 1. Overview of the M-Power system

the elderly. One interesting problem arises in the context of ambient assisted living (AAL), where, typically elderly, are to be expected to share, not only location information but also biometric data, such as blood pressure. From the literature described in the related work section and, to some degree, in the three experiments described, the question of benefit vs. privacy, and sharing with non-peers is yet unanswered. Recent work conducted in the health informatics group at SINTEF on the M-Power project [17] deals with an ambient assisted living environment where privacy is of utmost importance.

The M-Power project is a recently ended project conducted under the 6th frame programme financed by the EU [17]. 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.

A result of this project is an open source SOA-based platform² for building web-service based applications, which can be used to implement AAL [18].

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 live at home while maintaining a meaningful existence³. Interestingly, and in line with the research described in Section III, 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 are available as a service in the SOA world. Any meaningful combination of these sensors can be used as a monitoring tool, primarily

²<http://sourceforge.net/projects/free-mpower/>

³The results are currently being prepared for publication.

for the health care provider, seen at the upper right corner of the figure. The next-of-kin, lower centre, has the possibility 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 is perhaps the most important 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. [5] point out in their example on 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 [19] point out, information privacy goes beyond mere technical feasibility and rather follows the definition by Alan Westin [20], 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. 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. [8].

V. MINIMUM ASYMMETRY BY PROXY

As aforementioned, many people, in particular elderly 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.

If we follow the analysis by Jiag et al., [5] 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 access what and when. This is also know 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. Experienced 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

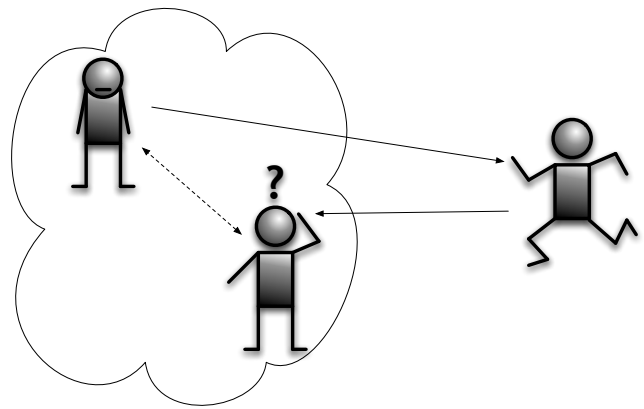


Figure 2. Minimising asymmetry by proxy

with dementia are capable of. So explicitly giving access to log information is simply not useful, rather quite the opposite.

As argued by Westin [20], 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 primary carer or next-of-kin might be a natural *proxy* for the elderly. Figure 2 depicts the relationship between the elderly, in the top left corner, the next-of-kin and the care facility, at the far right.

If we again investigate an ambient assisted living environment in the context of minimising asymmetry and by using proxies and consult Figure 2, 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.

Examples of increasing the information flow includes giving access to information about the usage of the information acquired, 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.

This approach opens up two main concerns, which again can be seen as problems of asymmetry: *i*) the issue of the health care provider as a data owner and the proxy as a data user; and *ii*) any owner, collector, user relationship between the elderly and the next-of-kin.

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 be 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 particular to the service provided. Thus, information flowing to the proxy should be seen as increasing information flow back to the data owner.

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 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. However, the idea of a proxy for information flow should be an integrated part of any AAL system.

VI. SUMMARY AND FUTURE WORK

The main argument presented here is that minimising information asymmetry is an important tool for maintaining privacy, also in ambient assisted living 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.

The notion of a proxy 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 systems, 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 inevitably lead to falling into many of the well-known pitfalls of AAL system design.

The health informatics group at SINTEF is currently planning the *universAAL* project, which in many ways can be seen as an extension of the M-Power project. This project will consolidate the use of SOA systems for AAL services. Part of this ongoing work focus on privacy and the application of the principle of minimising asymmetry.

ACKNOWLEDGMENT

The author would like to thank Jörg Cassens and Rebekah Wegener for their suggestions and assistance.

REFERENCES

- [1] M. Weiser, "The computer for the 21st century," *Scientific American*, pp. 94–104, September 1991.
- [2] U. Hansmann, L. Merk, M. S. Nicklous, and T. Stober, *Pervasive Computing: The Mobile World*. Springer Professional Computing, 2003.
- [3] A. Lugmayr, "The future is 'ambient'," in *Proceedings of SPIE*, ser. Multimedia on Mobile Devices II, R. Creutzburg, J. H. Takala, and C. W. Chen, Eds., vol. 6074, no. 1. SPIE, 2006.
- [4] A. Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing (Voices That Matter)*. New Riders Publishing, 2006.
- [5] X. Jiang, J. I. Hong, and J. A. Landay, "Approximate information flows: Socially-based modeling of privacy in ubiquitous computing," in *Proceedings of the 4th International Conference on Ubiquitous Computing (UbiComp 2002)*, ser. Lecture Notes in Computer Science, G. Borriello and L. E. Holmquist, Eds., vol. 2498. Springer Verlag, 2002, pp. 176–193.
- [6] M. Langheinrich, "Privacy by design – principles of privacy-aware ubiquitous systems," in *UbiComp 2001: Ubiquitous Comp*, ser. Lecture Notes in Computer Science, G. D. Abowd, B. Brumitt, and S. Shafer, Eds., vol. 2201. Springer, 2001, pp. 273–291.
- [7] V. Bellotti and A. Sellen, "Design for privacy in ubiquitous environments," in *Proceeding of the Third European Conference on Computer-Supported Cooperative Work (ECSCW '93)*, G. D. Michelis, C. Simone, and K. Schmidt, Eds. Kluwer Academic Publishers, 1993, pp. 77–92.

- [8] S. Ledere, J. I. Hong, A. K. Dey, and J. A. Landay, "Personal privacy through understanding and action: five pitfalls for designers," *Personal and Ubiquitous Computing*, vol. 8, no. 6, pp. 440–454, 2004.
- [9] S. Lederer, J. Manko, and A. 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.
- [10] S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. 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*. Oregon, USA: ACM, 2005, pp. 81–90.
- [11] Q. Jones and S. A. Grandhi, "P3 systems: Putting the place back into social networks," *IEEE Internet Computing*, vol. 9, no. 5, pp. 38–46, 2005.
- [12] A. Kofod-Petersen, P. A. Gransæther, and J. Krogstie, "An empirical investigation of attitude towards location-aware social network service," *International Journal of Mobile Communications*, 2010, to appear.
- [13] A. Kofod-Petersen and R. Wegener, "Like a poke on facebook emergent semantics in location-aware social network services," in *Handbook of Research on Discourse Behavior and Digital Communication: Language Structures and Social Interaction*, R. Taiwo, Ed. IGI Global, 2010, to appear.
- [14] P. A. 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.
- [15] S. Andresen, J. Krogstie, and T. Jelle, "Lab and research activities in wireless trondheim," in *Proceedings of IEEE International Symposium on Wireless Communication Systems*. IEEE Computer Society, 2007, pp. 385–389.
- [16] A. Kofod-Petersen, E. Klæboe, J. Jervidalo, K. Aaltvedt, M. Romnes, and T. M. Nyhus, "Implementing privacy as symmetry in location-aware systems," in *Proceedings of the International Workshop on Combining Context with Trust, Privacy and Security (CAT 2008)*, G. Lenzi, B. Hulsebosch, S. Toivonen, and J.-M. Seigneur, Eds., vol. 371. Trondheim, Norway: CEUR Workshop Proceedings, June 2008, pp. 1–10.
- [17] A. Pitsillides, E. Themistokleous, G. Samaras, S. Walderhaug, and O. M. 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.
- [18] M. Mikalsen, S. Hanke, T. Fuxreiter, S. Walderhaug, and L. 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.
- [19] M. Duckham and L. Kulik, "Location privacy and location-aware computing," in *Dynamic & Mobile GIS: Investigating Change in Space and Time*, J. Drummond, R. Billen, D. Forrest, and D. & E. Joao, Eds. CRC Press, 2006, pp. 34–51.
- [20] A. Westin, *Privacy and freedom*. Atheneum, 1967.