

Providing Privacy While Being Connected

Natalia Romero, Panos Markopoulos,
Eindhoven University of Technology
Den Dolech 2, 5600MB Eindhoven
The Netherlands
n.a.romero@tue.nl

INTRODUCTION

Privacy is typically studied as conflicts of information and data security or human rights issues. However a broader view of privacy focuses on how people choose to share as well as to keep for themselves personal information.

This research examine this later view, studying what people want to share, when, how and to whom in the context of Awareness Systems.

SUPPORTING INFORMAL SOCIAL COMMUNICATION

We describe research into supporting the leisure (non work related) use of communication media and more specifically of Awareness Systems. Awareness Systems are meant to provide a low effort, background communication channel that occupies the periphery of the attention of the user, and which helps this person stay aware of the activity of another person or group. Awareness Systems do not aim directly to support information exchange tasks, as for example e-mail and telephone calls do. Rather, the awareness they aim to create is similar to the awareness of people in surrounding offices at work or of one's neighbours at home. Such awareness is built by tacitly synthesizing cues of people's presence and activities, e.g., footsteps on the corridor, and discussions in the street outside. In many cases, these cues have very low accuracy, e.g., we can notice that there are people talking but not what they say, but this low accuracy is sufficient for providing this awareness [4, 8].

Awareness Systems have been studied in the work environment, starting from the Media Spaces work [3], at Xerox. Research into leisure and especially domestic use of Awareness Systems is more recent. In our research, we study and envision the use of such systems to support the communication between people with an existing and close social relationship. A solution to providing an awareness system for helping family members stay in touch through the day is the ASTRA system described in [6]. Here we are concerned mostly with the privacy issues arising in the context of Awareness Systems and more specifically in the context of ASTRA.

The ASTRA System

The operation of the ASTRA prototype described in [6, 11], is shown in figure 1. The system helps to communicate asynchronously family members who do not live in the same household. An individual takes a picture of a

situation she would like to share right away with a specific person or to all person at another household. She composes a message with the picture and a personal note and sends it. A person at home can at, any moment, check the messages sent.

The technology used consists of a mobile device (a mobile phone with camera on and GPRS functionality) that captures and sends pictures and notes to a home device (a portable display with touch screen capabilities) that continuously shows the collection of messages that have been sent by members of the other household. For more details of the implementation please refer to [6, 11].

The homebound device uses a spiral visualization to place the messages in a timeline structure where the user at home can navigate between previous and more recent messages. The display offers a shared space where all members of the family can see the messages that have been sent to the family. It also offers a personal space where each member can view the messages that has been sent only to her/him.



Figure 1: Connecting mobile user with the household through the ASTRA prototype

Pictures plus notes may be used to trigger communication or as conversation props during other communication activities.

A field test [6] was executed as part of the ASTRA project, which confirmed (also with quantitative evidence) that the system indeed helps related distributed households to stay in touch and get more involved in each other's life. From the sender side, results show that by taking pictures and writing handwritten notes the system supports mobile individuals to share moments through the day that they

might not feel are sufficiently noteworthy for sharing by means of more intrusive way of communication. From the receiver side, participants indicated that by receiving regularly messages it gives them a lasting sense of awareness about the members of the other household and therefore it makes them feel being much closer to each other's lives.

ADDING PERVASIVE FEATURES TO AWARENESS SYSTEMS

The ASTRA system offers a simple and explicit way of peripheral awareness between family members based on explicit picture-based communication and on manually inputting to the system one's availability status, e.g., by email, telephone, instant messaging, etc. While the field study has shown that ASTRA provides measurable affective benefits to its users, from a research point of view it is interesting to study to which extent adding more flows of communication and some degree of automation to the system will add more benefits without incurring too many costs. Relevant costs that may be experienced are the loss of autonomy because someone feels watched, the feeling of being obliged to return calls, the disappointment of not receiving an expected answer to a message, etc. Other costs relate to the effort of continually updating one's status or taking pictures or being disrupted by the arrival of new messages.

To a large extent improvements to ASTRA can help alleviate some of the costs mentioned above. Possible extensions include:

- Automatic notification to the sender when a picture has been viewed by the receiver(s).
- Peripheral awareness of the history of use of the home device by a user.
- Automatic presence capturing when a user is using/looking at the home device.
- Machine perception (e.g. sensors) to support users to manage their reachability information could help family members to control the disclosing and access of information while avoiding excessive interaction workload.

However, besides these benefits automation also incurs costs. For example, there is a tension between providing the desired level of control of what it is captured, shared and displayed and the convenience level of interaction a user wants to engage.

Automatic capture can help users to effortlessly maintain sense of each other's context and activities. For example, an Awareness System can provide cues of the type of situation in which users find themselves (e.g. private or public context). This information can help users to adapt their behaviours between different situations [2]. For example, in an elderly care situation a daughter who is concerned of how her elderly father is doing can refrain

from phone calls that resemble a 'doctor interview' conversation, because she will be able to answer those questions directly from an Awareness System, and therefore concentrate on more nice and meaningful talks.

Automatic capture offers a good variety of techniques to support these goals. Sensors and logs activities are some of the techniques we want to explore.

By adding automation the question is how to deal with the balance of convenience and control when interacting with Awareness Systems. On the one hand it may relieve the user of undesired tasks and therefore support her to focus on the meaningful tasks. On the other hand it may easily become a surveillance system, where the user is unable to control what information about him has been captured and delivered to others.

PRIVACY IN AWARENESS SYSTEMS

Awareness Systems technologies provide access to an increase amount of information that is captured by sensing context in physical environment and social situation. This capability is potentially valuable for the consumer who has access to increasing volumes of content, through numerous media, places and times of the day. Critical for ensuring user acceptance is to find a balance between the amount of personal information captured, how it is captured, the way it will be use, etc., and protection of user's privacy.

Typically questions of privacy are interpreted by people to refer to: (a) undue continuous surveillance by third party (what is known as the 'Big Brother'); (b) unauthorised access to private information.

These views are rather restricted, as we can see by a simple consideration of privacy issues in the ASTRA system.

In the ASTRA system every user of the home device has their own "area". This is where they can see postcards sent only to them instead of the household. In the design phase, we decided not to use any authorization process for accessing this area (e.g. login/password). Within a family we can rely on social norms. Family members will normally respect each other's privacy and refrain from opening doors that they should not [1] or peeping into drawers or personal objects (e.g. a teenager's diary). Protective and security mechanisms seemed an unnecessary interaction cost inconsistent with the idea of having a low cost/effort communication medium.

During the field tests, mobile individuals did not send at all to persons direct. They indicated that nothing was too personal in nature as they appreciated communicating at once to the whole household and not just one member.

In conclusion privacy issues emerge already without introducing surveillance; however a feeling of being under surveillance can arise when a constantly on communication channel is open and when a feeling of obligation to interact is felt. Also, privacy and information security are not synonymous. Privacy management can be achieved by

social interactions and social rules within a group of people and may concern equally well the will to share information instead of protecting it only.

Awareness Systems can lead to us knowing more than we want about friends and family, breaching their privacy or creating embarrassment. For example, the parents may unintentionally obtain an overview of their teenage daughters' social network, or grandma may find out that the grandchild who said she couldn't visit because of a school trip, is at home listening to music.

Besides providing inappropriate amount of information another privacy aspect of Awareness Systems concerns the failure to establish appropriate interaction/communication patterns. E.g., an always-on channel for communication between a mother and her son who is far from home, tells her lots about his daily routine and activities when at home. This can give her a sense of connectedness but may also give rise to an undesired level of engagement whenever the son is at home, even if he just wants to stay there without having to interact with anyone.

Looking at these two kinds of privacy failures in Awareness Systems, it seems crucial to enable users to regulate the process of privacy management. Our aim is to design a "Privacy Profile Interface" (PPI) for Awareness Systems that helps the user determine their own balance between their needs for communication and privacy.

PRIVACY IN SOCIAL PSYCHOLOGY

Early works like Westin's [14] and Altman's [1] theory study privacy from a social perspective, i.e. pertaining to human-human unmediated social interactions. Both these works conceptualise privacy as a dynamic process between the desire of being alone and the desire of interacting with others.

Westin's theory of privacy states and functions [14] has been an influential discussion on the ways people might want to achieve privacy, focusing on different ways and reasons for individuals to be alone or to be left alone. He identifies four different types of privacy (solitude, anonymity, intimacy and reserve) used as mechanisms to achieve four purposes or ends of privacy (personal autonomy, emotional release, self-evaluation and limited and protected communication). Without getting into the details of his theory we can clearly see that privacy may refer to groups as well as individuals level, can be affected through physical separation or behavioural mechanisms of people.

Altman takes a broader view than Westin consider privacy as a dialectic process by which people manage the extent to which they are accessible to the environment. He defines behavioural mechanisms (verbal and non-verbal behaviour, personal space and territory, and cultural defined norms and practices) for privacy regulation. He includes in his theory both social and environmental psychological concepts and describes how environment use by people is used to

manage privacy (e.g. territory, personal space) and how these mechanisms affect regulation of social interaction looking at both input (e.g. regulating who visits, being observed) and output (e.g. disclosing to another) aspects of privacy.

Although these theories do not cover the high complexity that privacy brings about when trying to study its impact in awareness systems, it gives us a good framework to conceptualize privacy in the context of human social behaviours and human social needs.

Mediated Social Communication

Social communication can be characterized as an interaction need of users to exchange information, and an outeraction [9] need that comprises several conversational processes outside the exchange of information to reach out others for communication.

Following the same idea, privacy concerns can be divided under two perspectives: information and interactional control perspective. An information perspective addresses privacy of the information content communicated: what information users want to exchange? How? When? To whom?. An interactional perspective addresses privacy of the outeraction needs for communication: what behavioural mechanisms users need? In which context? How to support them?. Rather than controlling access to Personal Information (PI) an interaction control perspective encourages users to develop their own social mechanisms to address the problem of interruption undesired communication.

PRIVACY MANAGEMENT

Recent studies [7, 12, 15] mainly focused in the mobile communication domain have developed several techniques to address these conflicts. We vision the state of art of privacy in Awareness Systems in terms of the distinction between information and interaction control perspective.

Information Control Perspective

Most of the works done try to facilitate communication by helping users to control their own PI and to access other's PI. Two examples of such systems are Personal Level Routing and Presence Cues, described below.

The Personal-level Routing [12] is a personal proxy to maintain person-to-person reachability. It is a rule-based engine that by asking users to set their own rules, it offers them a routing service that tracks location, converts message's format and forwards it to the proper communication medium. It protects privacy by hiding location information and by filtering and routing incoming messages according to user's desires. A clear constraint of this solution is that users need to interact with complex interfaces to explicitly set their own rules.

The Presence Cues project [7] offers presence cues for telephone users that display dynamic information of the

recipient's reached number and how available s/he is for the next call, in what they called a "life address book". In this case presence information is based on availability, current reachable number and personalized status messages. It requires users to update explicitly their own presence information when automatically detecting a potential updating situation, offering also a multiple-devices access to actually perform the update. By this means it tries to address the trade-off between overheads vs. control of information. Although this solution provides a good balance between automatic versus manual updating it underestimates the highly dynamic aspect of availability information that needs to be constantly updated. In consequence it was not valued as a reliable and useful social cue in their tests.

Interaction Control Perspective

Interaction control perspective in mediated social communication activities faces two mayor privacy conflicts:

1. Interactional commitment or attentional contract [15] refers to the level of engagement both recipient and initiator are willing to convey in their current communication activity. For example, it could be phrased in terms of desired effort to put: 'a short chat', 'a long talk', 'just a note', or in terms of which mediums is chosen: 'only text', 'only voice', 'only image', 'video', etc. A typical conflict scenario will be how to negotiate the initiator's intention for communication with the recipient's desired level of commitment.
2. There is a natural asymmetry between initiator and recipient refers to the unbalanced power that the initiator has over the recipient mainly when starting a communication activity.

Push-to-talk [15] represents the idea of protection of privacy by an interactive negotiation. Based on cellular radio technology it offers direct and accessible communication channel between small groups of people. It covers several styles of conversation like bursty, intermittent and focused. Instead of relying on automatic management of users' reachability, it relies upon lightweight social interaction mechanisms to avoid undesired levels of engagement when communicating.

For example, plausible deniability of presence by the recipient helps to negotiate the intention of the initiator with the desired commitment of the recipient by that time with low social cost. Delaying/omitting responses, provides a more relaxed protocol where expectations or obligations are not strong enough to overrule the personal desire at that time of interacting with another person. Decreased costs for openings/closings makes it easier for both the initiator and the recipient to propose and/or to reject an initiation of a conversation without feeling too much responsibility on that action. While it seems to be a very effective solution to

protect privacy its success is mostly based on supporting only small groups of people where a (high) level of social-knowledge already exists. The design question here is: to which extent can aware systems afford sufficiently numerous and flexible such mechanisms to support users control their social interactions?.

FUTURE WORK

The every day perception of the term privacy is associated with threats, violations, misuse, etc. of personal information. By answering the question of what do individuals NOT want to share will clearly leads us to an unlimited list of issues. Our approach proposes to observe users' attitudes and behaviours when using awareness systems. This can help identify privacy requirements from such systems, answering the question of what information about themselves DO individuals want to share, with whom, at what contexts/times and for what purposes. In this sense, awareness systems provide a sociable way to study privacy requirements. We examine the sharing of information and the negotiation of information communication channels, when a social purpose is pursued and when the social image of a person is concerned. (How their "self" is presented.)

Two major design tradeoffs play a crucial role:

- *Informativeness vs. privacy*, has to deal with how much personal information a user needs and wants to convey without violating his/her own privacy.
- *Overhead vs. control*, has to do with how a user wants to maintain his/her own personal information.

We aim to investigate to which extent does information management become an excessive workload for the user and whether people can and are willing to control over privacy management of awareness systems.

The two perspective to study privacy

As introduced and explained in previous chapters, we propose two different perspectives to study privacy in awareness systems: information and interactional control perspectives. Based on the literature findings previously described and taking advantage of an existing awareness system, the following proposal describes how the ASTRA system could be extended to address privacy from these two different angles.

The ASTRA system will be extended with a PPI (Privacy Profile Interface) to allow for management of a person's privacy using mechanisms that correspond to both these perspective. The extended system will be tested in order to validate and generalize concepts of privacy regulation to help users with the dynamic process of privacy management in awareness systems.

Information Control of PPI

The main objective is to address privacy concerns based on disclosing, control, and access of information depending on the type of information exchanged:

- Information awareness that facilitates communication can be provided by means of personal information (e.g. availability, location, reachability), context cues (e.g. office hours, traffic jam, sport night, holidays, etc.) and social cues (e.g. dinner time, social evening, family meeting, etc.)
- Information content that is exchanged during communication, where factors like sensitivity, relevance, temporality, etc. influences how to deal with privacy.

Interactional Control of PPI

The main objective is to address privacy concerns based on the choice and use by the user of awareness mediated mechanisms:

- From the initiator point of view a major privacy need relates to control over connection failure. This can be supported by “preambles” where the initiator can be informed of the readiness of the recipient for communication, before attempting to make a contact. The chance of easily switching media can be another solution helping the initiator to choose the proper media for a successful connection.
- From the recipient point of view a major privacy need relates to control the timing of a communication. For this purpose several mechanisms can be used: screening of messages so that messages can be easily masked without interrupting other activities of the recipient; plausible deniability of presence by which the recipient decides whether to show to the initiator that she is there or not; delaying/omitting response by which the recipient can decide whether to react or not on a response without incurring in high cost for not answering a message.
- From both recipient and initiator point of view the possibility to collectively control interactional commitment and desired level of engagement are others mechanisms for regulation of privacy. Interesting examples are: (1) lightweight openings and closings with no need of fixed protocols (how are you, I need to hang up now, etc.) that makes it easier for the initiator to propose a contact and easier for the recipient to engage or reject it; (2) lightweight swapping of activities; (3) reduced feedback/accountability where less awareness may lead to less expectations and obligations.

CONCLUSION

This project looks forward to define a set of policies that will ensure a proper balance between the communication benefits and privacy costs that are experienced by users of

awareness systems. These policies should support different levels of automation when sharing information based on content shared, the circumstances and the audience involved. This might guide us on the creation of a proper design interaction framework to offer a build-up privacy model when designing awareness systems.

Expectations from the Workshop

The focus of attention of this research can be described in the following list of research questions:

Information perspective

- What information do people want to be captured implicitly by automatic capturing technique and explicitly by input devices? How to represent information of one’s actions with respect to a specific receiver?
- What information is temporality sensitive (becomes history) when log applications are provided? How to provide the proper interpretation of past, present and future actions?

Interaction perspective

- What are the desired levels of feedback (accountability) user want when sensor capturing occurs? How to provide understanding and anticipation of how one’s actions appear to others?
- What are the desired levels of control for the receiver over the information displayed? Decision of what to view, when and how to view it.

REFERENCES

- [1] Altman, I. *The environment and social behaviour*. Brooks/Cole., Monterey, CA, 1975.
- [2] Anne Adams, M.A.S., Privacy Issues in Ubiquitous Multimedia Environments: Wake Sleeping Dogs, or Let Them Lie? *Proceedings of Interact '99, International Conference on Human-Computer Interaction*, Edinburgh, UK, 1999, IOS Press, IFIP TC.13, 214-221.
- [3] Bly, S., Harrison, S.R. and Irwin, S., Media Spaces: Bringing People Together in a Video, Audio and Computing Environment. in *Communications of the ACM*, (1993), 28-47.
- [4] Eggen, B., Hollemans, G. and Sluis, R.v.d. Exploring and enhancing the home experience. *Journal of Cognition Technology and Work*, 5. 44-54 , 2001.
- [5] Langheinrich, M., Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. *Proceedings of International Conference on Ubiquitous Computing - Ubicomp*, Atlanta, Georgia, 2001, Springer
- [6] Markopoulos, P., Romero, N., Baren, J.v., IJsselsteijn, W., de Ruyter, B. and Farshchian, B., Keeping in Touch with the Family: Home and Away

with the ASTRA Awareness System. *To appear in Proceedings CHI 2004*, Extended Abstracts, Vienna, 2004, ACM Press.

- [7] Milewski, A.E. and Smith, T.M., Providing presence cues to telephone users. *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, Philadelphia, Pennsylvania, United States, 2000, ACM Press, 89-96.
- [8] Mynatt, E.D., Back, M. and Want, R., Designing Audio Aura. *Proceedings of CHI 98*, Los Angeles, CA, USA, 1998, 556-573.
- [9] Nardi, B.A., Whittaker, S. and Bradner, E., Interaction and Outeraction: Instant Messaging in Action. *Proceedings of the 2000 ACM conference on Computer supported cooperative work*, Philadelphia, Pennsylvania, United States, 2000, ACM Press, 79-88.
- [10] Palen, L. and Dourish, P., Unpacking privacy for a networked world. *Proceedings of CHI'03*, Ft. Lauderdale, Florida, USA, 2003, ACM Press.
- [11] Romero, N., van Baren, J., Markopoulos, P., de Ruyter, B. and IJsselsteijn, W., Addressing interpersonal communication needs through ubiquitous connectivity: Home and away. *Proceedings of Ambient Intelligence*, 2003, Springer-Verlag, 419-431.
- [12] Roussopoulos, M., Maniatis, P., Swierk, E., Lai, K., Appenzeller, G. and Baker, M., Person-level Routing in the Mobile People Architecture. *Proceedings of 2nd USENIX Symposium on Internet Technologies and Systems*, Boulder, Colorado, USA, 1999.
- [13] Sven Meyer, A.R., A survey of research on context-aware homes. *Proceedings of Australasian information security workshop conference on ACSW frontiers*, (Adelaide, Australia, 2003), Australian Computer Society, Inc, 159 - 168.
- [14] Westin, A.F. *Privacy and Freedom*. Atheneum, New York NY, 1967.
- [15] Woodruff, A. and Aoki, P.M., How push-to-talk makes talk less pushy. *Proceedings of the 2003 international ACM SIGGROUP conference on Supporting group work*, Sanibel Island, Florida, USA, 2003, ACM Press, 170 - 179.