

Designing for privacy and self-presentation in social awareness

Mika Raento · Antti Oulasvirta

Received: 21 June 2006 / Accepted: 17 January 2007
© Springer-Verlag London Limited 2008

Abstract Social awareness applications are based on the idea of a group sharing real-time context information via personal and ubiquitous terminals. Studies of such applications have shown that users are not only concerned with the preservation privacy through non-disclosure. Instead, disclosure is manipulated for the constant presentation of self to the group in everyday social situations. Basing on 3 years of research with the mobile social awareness system ContextContacts, established findings in social psychology and ubiquitous computing, we propose a number of design principles to support users in this management of privacy and presentation. These principles are to apply even if disclosure is automated, and include support for lightweight permissions, assuming reciprocity, appearing differently to different audiences, providing for feedback on presentation and allowing lying. These principles are applied in interaction design and protocol engineering for the next version of a mobile awareness system called ContextContacts.

Keywords Privacy · Self-disclosure · Self-presentation · Social psychology · Social awareness · User interface design · Presence protocols · Security

M. Raento (✉)
Department of Computer Science, University of Helsinki,
PO Box 68, 00014 Helsinki, Finland
e-mail: mraento@cs.helsinki.fi; mikie@iki.fi

M. Raento · A. Oulasvirta
Helsinki Institute for Information Technology HIIT,
PO Box 9800, 02015 TKK, Finland
e-mail: oulasvir@cs.helsinki.fi; antti.oulasvirta@hiit.fi

1 Introduction

During the past 3 years we have been designing, implementing and field-testing a ubiquitous social awareness service for mobile devices, ContextContacts [1], shown in Fig. 1. Social awareness applications are designed to re-contextualize remote and mediated communication tasks by transmitting, automatically or in a user-controlled manner, *cues* of people's current state or situation. The goal of such systems is to build "an understanding of the activities of others which provides a context of your own activity" [2, p. 107]. With ContextContacts, the user is presented with cues ranging from the location of others to their emotional status (via self-description), all of which are integrated the phonebook that looks and behaves otherwise normally.

Privacy is an ever-present concern in ubiquitous computing [3], and it's role is further emphasized in a social awareness application—the very idea of which is the automatic disclosure of personal data to remote others. Research investigating people's privacy concerns in ubi-comp has convincingly demonstrated that the problem is both real and non-trivial to solve. Studies and experiments have shown the discontinuity between users' stated attitudes and actual behavior [3], their complex willingness to reveal location information to others [4], and enumerated the typical pitfalls in proposed systems [5].

Research in computer systems has often been pre-occupied with privacy *preservation* (witness 420 hits on Google Scholar with the keyword "privacy-preserving", and work like Platform for Privacy Preferences [6]), as if privacy was a state of the world that needs to be stored, saved, or protected. This notion has been recently worked on [7, 8], using the social psychological view of privacy as an ongoing process of boundary negotiation [9–11]. In this



Fig. 1 ContextContacts. Mobile phone Contacts augmented with information on the current and past location, calendar, phone usage activity, phone profile as well as people and other devices nearby. The *second picture* presents a detailed view for an entry selected in the list view

paper we continue this work, aiming to concretize how that notion can be applied to the design of social awareness systems.

The flip side of privacy is, in a way, *self-presentation*: by manipulating what information is related of oneself to another person, people habitually pursue certain effects on that other person [12]. It is clear that in social awareness applications, and in group applications like ContextContacts particularly, self-presentation has a pronounced role due to the fact that the disclosers know each other. We argue that these two aspects, privacy and self-presentation, need to be tackled together to support human interaction.

This paper addresses the problem of support for controlling privacy boundaries on the one hand and self-presentation on the other, in a way that does not place unrealistic burden to the user and thus undermine the social application itself. For this end, the following steps are taken:

1. *Theory*. We review several theoretical contributions in social psychology and human–computer interaction to characterize the processual nature of boundary negotiation, as applied the domain of social awareness applications particularly.
2. *Lessons from field trials*. We present observations from our four long-term field interventions done with a particular social awareness application (ContextContacts). The observations pertain to the use and functions of privacy control and self-presentation mechanisms.
3. *Applied principles*. We discuss several principles that provide a synthesis to theory and the lessons learned in field trials. The principles are meant to be fairly detailed to be of practical use in the domain of social awareness. Moreover, they build on top of and assume fair information practices [3]: informed active consent,

appropriate security, accuracy and the limitation of collection and storage to data needed for the application at hand.

4. *Demonstration of applicability*. To assess the constructive power of these principles, we show several improvements to ContextContacts motivated by them. The principles imply changes mainly at the level of user interface mechanisms and representations, but we will also show how they provide new ideas to existing presence protocols.

Thus, rather than pooling empirical results, or presenting technological innovations without proper evaluation, this paper contributes to the on-going efforts at developing real world implementations of social awareness by proposing a synthesis among several important theoretical, empirical, design, and engineering aspects of privacy.¹

2 Privacy and self-presentation as social processes

Palen and Dourish [7] have been applying Altman's privacy theory [9] to the design of ubiquitous computing systems. Rather than repeat the full argumentation, we pick some of most salient factors here. Altman describes privacy as ongoing negotiation of the self-environment boundary. In this paper we focus on a subset of such boundaries: between the user and others they already know: their friends, colleagues and family. The most important factors of Altman's theory for us are the dynamic and dialectic nature of privacy, and the emphasis on negotiation. "Dynamic" means that privacy is contextual, dependent on circumstances and people; it cannot be fully described by a static set of rules. By "dialectic" Altman means that the actual boundary is determined by conflicting needs within ourselves, as well as between us and others. The conflicting internal needs include autonomy, social acceptance, tasks and goals as well as impression management. Privacy being "negotiated" the limits of disclosure are not dictated by either the discloser or the environment, but the result of a negotiated agreement between them. Negotiation is of course not overt or explicit, but built-in to the give-and-take of conversations and other interactions, as well as into perceived norms and tact.

Participants in such negotiations often engage in *face-work*. Goffman [14] describes face as the "image of self delineated in terms of approved social attributes" and face-work as the actions of interactants which are consistent with face. The implication of this is that it should be possible for technologically mediated negotiation to also be sensitive to face. The system should allow for tact and what

¹ Some of the interaction design ideas were presented in an earlier workshop paper [13], but the analytical structure is completely new.

Aoki and Woodruff [8] (among others [15, 16]) have described as *plausible deniability*: the possibility to assign different interpretations on actions. An example is the ability for an asker to see the denial of an answer as missing or misunderstanding the question.

The revelation of private matters to others has been called *self-disclosure* [17]. Self-disclosure is seen as a necessary component in building and deepening relationships, the revelation of the private indicates trust, facilitates an understanding of the other persons interests, tastes, needs and desires, and through its reciprocal nature also helps the discloser to learn of the other. Empirical studies have shown genuine self-disclosure to correlate strongly with positive emotional affect [18]. Self-disclosure is generally assumed to be strongly reciprocal [17, 18]: there is a strong correlation between how much the different sides of social relationships disclose. The self-disclosure studies have, however, focused on equal status relationships (friends, spouses, dating) [19, p. 440]. There is no indication that the theory of self-disclosure applies to unequal relationships, such as parent-child or boss-worker.

Self-disclosure is described by Goffman as a part of the larger frame of *self-presentation*: the continuous process of impression management [20]. By disclosing certain facts instead of others, by drawing attention to actions, by their appearance and sometimes by outright deception people try to create a controlled impression of themselves. The creation of this impression is dependent on the ability to monitor the reactions of others, so that the success of the current strategy can be evaluated and alternative strategies or alternative goals can be used. Self-presentation is used for many different goals: for example to gain material benefits, such as a raise, to apologize for or justify actions, or as a part of the identity-building of an individual, since identity depends not only on internal states but on feedback from others. Self-presentation is very much target-dependent. People do not want to give the same impression to all others: parents may want to appear stern to their children but relaxed to their friends, workers may stress their individual contributions to their boss but team-orientation to co-workers. Not only is the goal dependent on the target, but so are also the strategies involved.

Negotiations, face-work and self-presentation may involve deception—lying. DePaulo et al. [21] describe a study in which adults told one to two untruths a day that they consciously recognized as lies. Computer systems have often been designed with the idea that reality can be sensed and described objectively [22], whereas the reality of human interactions has been described as *socially constructed* by Berger and Luckman [23]. All of us may recognize the jointly constructed, and negotiated, reality of concepts like “an appropriate gift” or “a friendship”. In such situations a technical system should not presuppose

certain versions of reality to be more truthful than others, but to leave the decision to users. Goffman also argues [12, p. 222–227] that the audience is quite willing to disregard untruths to maintain a jointly agreed-to situation.

Self-disclosure and self-presentation in human discourse are tangled with other concerns [24]. This makes experiments with privacy hard to analyze. Consolve et al. [25] have argued that location-disclosure is fine-tuned by situation and audience to maintain privacy boundaries. Such tuning is, however, not necessarily disclosure control: it is a well-known theorem of human–human communication (Grice’s maxims [26, 27]) that participants in a dialog will try to convey just the right amount of information, too much is wasteful, too little unhelpful and both will provoke suspicion. So if the person gets to answer, “Where are you?” as a human, *of course* their answer will depend on what they think the “real” question is or what they think relevant to the person asking; e.g., if they are abroad, they will most likely just say “I’m in England” to persons from the States. Also irritation at being asked can genuinely stem from the inability to infer the “real question”. Such conversational rules do not necessarily apply to answers from a computer.

3 Lessons from the field

We have conducted four long-term field trials with ContextContacts. Contrary to our initial expectations, the general finding has been that users are not worried not so much about losing their privacy rather about presenting themselves appropriately according to situationally arising demands. The factors behind these results are analyzed below, after a more detailed description of the system.²

3.1 The current version of ContextContacts

ContextContacts is built on top of the ContextPhone platform running on Nokia Series 60 smart phones [29]. It overrides the standard Contacts application of Series 60 smart phones but looks and behaves very similarly. It can be triggered from the application menu and from the stand-by screen by the same means as in the standard version. Integration into the communication environment of the smart phone, including Short Message Service (SMS) messages and recent calls list, have been implemented.

Our approach to cue design has been to integrate them to contact book, because call placement and answering is still

² The first three studies have been reported in detail in Oulasvirta et al. [28]. The latest study has not been fully analyzed, but we will give preliminary results based on interview data. The existing reports have mostly skimmed the privacy aspects, which we will focus on here.

by far its most commonly used functionality of a phone (see also [30, 31]). The contact book is also an indicator of a person's social networks and a source for finding opportunities for communication and interaction [32, 33]. Most cues are represented as icons to save space and to support visual search and attentional pop-up necessary for spotting changes (see Fig. 1). In icon design, we relied on well-known usability principles: utilizing clear, communicative, concrete, and familiar metaphors. Therefore, the icons rely mostly on conventions in instant messaging (IM) and Nokia's products. Among the cues, there is also textual information to express location and duration of stay in that location. ContextContacts automatically fetches in the background a place name for Global System for Mobile communication (GSM) cell ID from the tele-operators (Elisa and TeliaSonera in Finland) positioning services. However, because ordering the positioning information is costly, the names for only those IDs where the user spends a significant amount of times, called Bases, as determined by a data mining algorithm [34] are fetched. The algorithm also overcomes the frequent cell-switching problem in the GSM network. Thus, a familiar district name is represented in the district cue most of the time.

A detailed view of a contact is provided upon a joystick press (Fig. 1). There, all cues are expanded to a table where the cue type is presented on the left and the corresponding explanation in text on the right. To support the understanding of veridicality and timeliness of the cues, all cue information grays out gradually (in four intervals) if the user is disconnected. To support self-awareness, there is a view accessible from the options menu showing how others see the user at the moment. Finally, the contacts using the ContextContacts service are grouped at the beginning of the contact list. This decision has been made with the aim of supporting understanding of the relative situations of others with as little interruptive scrolling as possible. The reciprocity of self-disclosure [9, 35, 36] is supported only at a very rudimentary level: if the user decides to switch the application off, he/she receives no information on friends' situations either. Therefore, others cannot monitor a user without that user being able to monitor them back.

3.2 The studies

During the past 2 years we have carried out four field-studies with slightly varying versions of ContextContacts:

Family A family of four used the system for about 7 weeks. The family consisted of the mother and three children, aged 13, 15 and 17. They used a version that did not include the free-text description.

The young entrepreneurs Five teenagers running their own business, aged between 16 and 18, four males and one

female. The study lasted for 8 weeks, and was run without the free-text description.

Schoolmates A group of six teenage friends used the system for 6 weeks. There were five females and one male, aged 16–17. They had the free-text description field and used it extensively as a chat-medium.

Office Two intersecting groups of office-workers used the system between 3 and 6 weeks. There were altogether 10 users, 5 female and 5 male, between 30 and 45 years of age. The participants used a version of ContextContacts that had the free-text description as well as indicators of their other personal devices nearby (laptops, desktops).

All of the participants were living in Finland, and apart from two in the Office study, in the Greater Helsinki area. Most were also native Finns. The participants were volunteers found through personal connections of the researchers.

A general introduction included transferring information from the participants' old phones, explanation of data gathering (including phone recording), instructions to use the phone "naturally", explanation of reimbursement of costs and of the subsequent anonymized analysis and publication of data, filling in forms of background information, and fixing schedules for interviews. At the beginning the study, a version of ContextContacts was installed on the participants' phones. The participants were told that ContextContacts replaces the phone's original phone book. All cues were briefly explained, as well as the use of the related mechanisms (details and self-awareness). An interview was held two times during each study: in the middle and in the end. Interviews were semi-structured and focused on collecting concrete, real episodes of using the system.

These studies provide a solid basis for claims on the privacy issues in social awareness. The users represent different ages, life stages, genders and social structures. The system has been used for extended periods, allowing both a variety of situations and evolving practices of use. The automatic collection of data has been as unobtrusive as pragmatically possible [29], and the two interviews per subject should impact the results minimally. The size of the samples of course precludes statistical inferences for any target population. Instead we focused on the interaction of the technology and known social psychological processes.

3.3 Three functions of awareness cues: coordination, expression, companionship

We saw many interpersonal uses of the cues that partly explain why the participants experienced the system as overcoming the threat of losing one's privacy (see

Sect. 3.4). We summarize the functions under three functions of the system (this section is abbreviated from [28]).

Firstly, Coordinations involved mainly of what are called “productions of near space-time”, like meetings and invitations. These actions were based on utilizing the cues for inferences of place, proximity, movement, and activity of the other person. Interviews also revealed that automatic cues were of decisive importance because they could be relied on as being updated and timely, qualities that are known to be important for social inference [37]. Through automatic cues, several of our participants also opportunistically initiated face-to-face meetings when others were seen to be close by and knew when not to do so. Cues were not only used in a compensatory manner (e.g., to explain why a person is late after this event has unfolded) but used to generate anticipations of future events of what the other will do in a given situation and they were taken into account when planning ones own actions. Participants also told of monitoring the progress of others in agreed-upon group coordinations.

On the other hand, *communication-related coordinations*, particularly of phone calls and SMSs, were mostly relying on the hand, location, and alarm profile cues; the key inferences were availability for communication, interruptability, and responsiveness to asynchronous messages. While some of these coordinations were compensatory, for example, looking at cues in order to understand why a recent call attempt was rejected or not answered, a significant part was anticipatory. Participants for example told of using them to postpone calling when the other person is attending a class. From interaction logs recorded during the trials, we learned that cues were systematically looked just before placing a call, and one group indeed did have a small improvement (approximately 12%) on success rates in call attempts.

The second role for mobile awareness exists in its use as a medium for expression; a medium to the extent it is used as channel for actively expressing ideas and emotions and for communicating. This type, that emphasizes impression management, was accentuated in the Schoolmates group who appropriated the free-text cue for chatting, discussions, opinion formations etc. The logs showed over 5,000 short messages sent during a period of 6 weeks. Our analysis of the contents of the messages showed that a good part chatting was emotional instead of rational. As extreme examples, the cues were used to reproduce poetry and to play a word game.

We believe that two features of ContextContacts contributed to the phenomenon which could also be characterized as its emergence as a locale, a digital place that offers a group the site and means for maintaining awareness of another and for rapidly moving into interaction [38]. Firstly, grouping of the cue-augmented contacts

to the beginning of the contact book allowed for accessing situations and messages of the group quickly. Self-disclosure and self-presentation were reciprocal in the sense that whenever a user was able to see other users, he/she was also visible to those others. Secondly, the hand cue allowed for presence, availability, and responsiveness inferences, which have been observed to be important in IM and other on-line messaging systems [16]. Here, interviews revealed that the hand cue was in effect appropriated for understanding and negotiating [39] when to send a message so that others will see it, to infer conversational availability [16], to check to see who is online, to estimate the rapidity of response to ones own turn, to infer if others had received the message after it was sent, and to signal one’s own availability to others. Continuous and situational negotiation of boundary is not possible unless the status of the potential audience is known.

The third role is the role of cues as a proxy for companionship; a proxy in the way they can act and be used in the place of a distant person, having that someone somehow with you. The need of companionship and relatedness is among the fundamental human needs [40]. In this pursuit, the content of the cues is secondary to the outcome of their processing: the feelings and experiences of closeness and companionship. In addition to several participants expressing that companionship was important, there are instances of the users tracking others and looking at the cues in ContextContacts for long periods of time. Moreover, there were few reports evidencing that extraneous effort was put into keeping the phone close to oneself just to maintain connection to others. The importance of free-text cue particularly in this role lies in the fact that it provides a more controlled mean for expression, and is thus a better resource for reciprocally deepening companionship [9].

3.4 Little concern for privacy

We were surprised by the fact that users had no expressed concerns about the automated disclosure, nor felt uncomfortable with it *within the study group*. This is in contrast to many findings based on interviews regarding potential systems [4, 25] as well as reactions to some deployed systems [41, 42]. On the other hand there are other studies, such as on the ActiveCampus location disclosure [43] and Barkhuus and Dey’s questionnaires [44], with similar results.

The perceived lack of concern was clear in the interviews, which were held both during and after the use of the system. Users did not bring up any discomfort related to disclosure spontaneously, nor did they express concerns when explicitly asked. The behavioral data closely reflects the interviews: ContextContacts has an easily accessible

(two interaction steps from the phone idle screen), coarse [5] control mechanism: the turning off of the system. In all of the studies the limitation imposed by the GSM data transmission channel (data cannot be sent when the phone is used for calling) and instability of the networking caused enough disconnections that purposeful disconnections would not have been noticed as such (providing plausible deniability [8]). In all the three first studies the participants also demonstrated the ability to use that option when they went on trips abroad or played with the system. Nevertheless, only one of the participants in all three studies used the disconnection, and he only on two occasions (even these may be better explained as experimentation with the system). So it seems that in addition to not being initially concerned, the users did not become concerned during the study or encounter situations where they would have needed to control their disclosure. In addition to the three functions that the cues were successfully used for, there are other factors partly explaining this finding, detailed below.

Especially in the The Young Entrepreneurs and Schoolmates studies one can argue that self-sampling biased the studies: since volunteers were recruited specifically to use such a system, people concerned about such disclosure were not included. That is not fully the case with the Family and Office studies: for the family, only the mother volunteered spontaneously, the children only had to give consent. In the Office study some initially skeptical participants were convinced by our contact person. The two groups that actively volunteered for the study used the system significantly more and expressed more enthusiasm for it in the interviews, than the Family and Office groups. The enthusiasm can be seen as a verification of the self-disclosure theory, which states that disclosure is linked to strengthening of relationships (which was also reported by the participants in the Schoolmates study) and positive affect.

Another factor contributing to lack of concerns about disclosure was the coarse level of cues. For the Office study, the location disclosure was felt to be safe due to its coarse and geographically oriented nature: all you could see which district and city the others were in. Since the participants were not very intimate, the only kinds of inferences they could draw from this were “work”, “home”, “neither”, with the addition of being able to distinguish between the two different offices of the company. The tracking of somebody’s working hours could not be done through this due to extensive telecommuting. In the other three studies more detailed inferences could definitely be made based on the information. The mother would know whether the children were at school, at home, with friends, in town etc. In the The Young Entrepreneurs and Schoolmates studies the participants came to recognize visiting specific friends or carrying out specific activities.

So the lack of detailed and semantic location information cannot fully account for willingness to disclose, although it surely plays a role. The ambiguity of the information also allowed for socially acceptable interpretations. It seems that situations where location information at the district level would genuinely need to be hidden are rare. We think also that the real-time nature of the system helped the users to feel safe: none of the information was logged for the users to be perused later. It would not have been possible to build up pattern knowledge of others without a large manual effort.

The Schoolmates did express a concern in the interviews: they were concerned about that they would be considered “peepers” that they were *looking* too much at others. They were very aware that others could interpret the activity cue as an indication of monitoring. This means that they were quite aware that the system was stretching inwards some of previously negotiated privacy boundaries. It did not, however, stop them from using the system. We do not know how this should affect the design of the system.

Although all the participants were comfortable with this kind of disclosure within the group, most of them did say in the interviews that they would not want to use it with everyone in the same way. Teenagers would not necessarily have liked their parents to see them all the time, and some of the Office workers named that there had been bosses who would use such a system to monitor their underlings in an uncomfortable manner.

3.5 Self-presentation

The ability to add a free-form textual description to the presence display was added for the Schoolmates study. Since the Office study has not been fully analyzed, we will focus on the Schoolmates one. The analysis relies purely on the actual messages sent by the participants.

The Schoolmates participants realized within a day that the textual description could be used as a group instant messaging system. As an instant-messaging tool, the description was very limited. It was rate-throttled to allow at most one message per minute, the text was limited to 50 characters, no history of past messages was kept, and no alerts were played when receiving such “messages”. Nevertheless, the six participants sent over 5,000 messages with it in the course of 6 weeks. This gives us ample opportunity to see how the combination of automated disclosure and free-form messages are used for self-presentation.

The free-text field was regularly (15% of the messages) used to comment on the automatic cues of the message sender or somebody else in the group. Such comments could be used to draw attention to one’s current situation at

a certain point in time, to frame the location (“Yeah, I’m still at school” at 19:30, implying self-deprecation), or to give additional information (“with friends”). Comments by others (“Is S with his ex there?”) allowed for the monitoring of the impression received by others.

Of course self-presentation unrelated to the automated disclosure was observed as well. The Schoolmates expressed emotional support (“*Hug*”) to somebody expressing doubts about a relationship (“What if he’s right now with some cute French girl?”). The users would present their language skills by writing messages in foreign languages (Swedish, English, Italian). Since the study was conducted during final exams time, they would write many messages on whether they were studying, who was studying, and what were acceptable levels of academic effort. And finally, the Schoolmates were very concerned with whether others were reading their messages, adding questions directed to others (“Is anybody there?”, “Answer me”).

As stated in the previous section, the Schoolmates also expressed that they would not want to share this information with their parents. In this case this should not be read as non-disclosure of the automated cues, but as wanting to give different impressions to different targets. Definitely the kind of social and emotional presentation given through the system (e.g., commenting on the looks and desirability of classmates) would not have been desirable to share with their parents as well.

3.6 In favor of automatic disclosure

Smith et al. [4] have argued that designers of location-based systems should not focus on automatic disclosure. Instead they have advocated a system that allows lightweight manual disclosure of location, often as answers to requests for that information. Such a system is of course implicitly more suitable to controlled self-presentation, since the image is under complete manual control. They base the recommendation on the results of a study where people had been using a manual disclosure system and were given the option to let it automatically make some of those disclosures. The subjects of their study did not want to enable such automation. We refute the universality of this view.

From our field study results described above and in [28] it is clear that:

- There are users who are quite happy to automatically disclose their location and other facts with people they feel close to, as well as people who are more peripheral. This is supported by our studies in that the users (especially in the three latter groups) almost never switched off the system, did not volunteer any concerns

and systematically denied discomfort when explicitly probed while identifying possible other relationships where they would not like to use such a system (see Sect. 3.4 and [28, Chap. 4.5]).

- The automatic disclosure allows for deepening of relationships in situations where it might not be clear how to bootstrap manual self-disclosure. Two of the users in the Schoolmates group related that they had “grown closer” even though they had previously been friends-of-friends and felt uncomfortable taking direct contact with each other.
- Automatically disclosed facts are used for the topicalization of lively discussions (see [28, Chap. 6]: users would make questions related to cues in phone calls, and discuss the meaning of cues in the Schoolmates group via the free-text-cue. We have interpreted the way the users described the incidents of “noticing” that somebody was at an interesting location or with certain others as an indication that this information would not have been otherwise available, and that they would not have necessarily been prompted to get that information through other means.
- By not requiring asking for information lightweight, opportunistic uses are made possible (e.g., noting that somebody is also in town and asking them for a cup of coffee or joint shopping, whereas constantly asking somebody’s location just in case they would be nearby would not be productive or acceptable; several cases of opportunistic meetings were related in the interviews [28, Chap. 8.1]).
- Even more task-oriented uses, such as availability inference, are often made in such situations where the discloser is *not* available for communication at that time (especially in the use of the free-text cue for messaging, the non-response of another was rationalized by the the activity cue, as related in the interviews of the Schoolmates).

Based on these findings we argue that providing for privacy-management and self-presentation within automated disclosure is a useful and important topic of research.

4 Design principles

Based on the social psychological findings, our field studies and taking into account the boundary conditions of ubiquitous computing we enumerate nine design principles. We build on previous work in ubiquitous computing as well [3, 5, 7, 8], with the major contribution in providing *positive* design principles (what to do, rather than what not to do) specifically for a mobile, ubiquitous social

awareness application (rather than for ubicomp in general) meant to be used by people who already know each other. While the field studies have been conducted in homogeneous groups, the social psychological literature gives a large body of work to derive principles for heterogeneous groups from.

The principles are:

Support lightweight permissions Different dyads and groups have different rules of disclosure [11]. Some are permissive by default, some more restrictive. Support both, allowing also redress for misuse of permissions. Due to lack of resources in the use of the system [45], permission management must not rely on extensive actions, or simultaneous use of the system by both parties. Our studies show that explicit control mechanisms are rarely used (see Sect. 3.4) within the homogeneous group, whereas the users have in several cases (Schoolmates and Office) stated that they would require control mechanisms with different others.

Assume reciprocity The users in our studies that have liked the system most have been in equal relationships. Disclosure in equal relationships is strongly reciprocal [17]. Treat unequal relationships as a special case. Provide for other mechanisms for unequal relationships [19].

Make it possible to appear differently to different people The social psychological literature provides extensive proof that people maintain different impressions towards different reference groups [12, 14, 20]. In our studies the system itself has not provided means for such impression management directly, and while this has not been disabling for the use of the system within the homogeneous group, we assume that a realistic ubiquitous system will involve different reference groups. Such impression management does not necessarily mean forging information, but for example commenting on different things to different audiences, or broadcasting different availability to different groups. The kinds of self-presentation carried out by our users have would have been fully inappropriate for other audiences (see Sect. 3.5).

Allow for commenting, modifying and framing automatic disclosure You cannot manage impressions through purely automatic disclosure. Allow users to attach different meanings to the automatic cues. If such mechanisms are available, they are used extensively (see Sect. 3.5).

Provide for feedback Self-presentation relies on being able to monitor how others perceive you [12]. Disclosure management requires you to know what is actually being disclosed [9, 17]. The system should provide the opportunity to learn what others are doing with the information and what they think of it. This may mean explicit confirmations

of when cues are looked at or messages read, or the ability to easily comment on cues about others, providing for acknowledgements and joint construction of impressions.

Allow the user to lie Denying disclosure can both be socially unacceptable and make others assume you are doing something bad. Faking an answer instead allows for control of disclosure while preserving face [14]. Lying is often seen as morally reprehensible, and some system designers aim to disallow it [22], although most systems of course allow for it. We want to emphasize the ability as humane [21].

Do not take control away from the user Since users do not exercise control, it may be tempting to downplay its importance, considering the implementation effort. You may not. Autonomy is a basic human need [40], and removing even unused controls leads to irritation [46, p. 22].

Allow opportunistic use Automatic disclosure is useful. Do not assume all monitoring is intruding on others' privacy. In our studies, opportunistic knowledge of others has been central to the use of the system (see Sect. 3.6). Note, however, that not all groups and relationships are equally amenable to opportunistic use.

Do not try to do everything within the system People have other mechanisms for agreeing on rules, negotiating permissions, modifying impressions and seeking redress [24]. Examples of blending the boundaries of social accountability and system-level permissions include the cycle of group creation and invitation in [47], the integration of other communication means (voice calls and SMS) in ContextContacts, the use of killfiles [48] and reproaches [49] on Usenet to control discussion and the collective reading of text messages and answering of voice calls with mobile phones [50].

The design principles enumerated above are not enough for actually building systems. They rest on top of a number of basis assumptions about the system. These assumptions are necessary but not sufficient conditions for actual systems.

We assume that the system is build according to Langheinrich's "Principles of Privacy-Aware Ubiquitous Systems" [3], which he derives from the fair information practices reflected in legislation [51]. We assume that the users are notified of disclosure, they give and may withdraw consent, data are not collected or used in the system other than for the dissemination which is the central function of it, the data are as accurate as technically possible and not stored anywhere for future reference. Security is returned to in Sect. 7.

The principles given here, and their elaboration in the next section can be very well seen as a concrete example of

how to avoid the privacy-management pitfalls enumerated by Lederer et al. [5]: obscuring potential or actual information flow, emphasizing configuration over action, lacking coarse-grained control and inhibiting social nuance. Lederer et al. argue that a privacy-management system works well when the behavior of the system is a result of actions taken by the users. We try to show how this can be achieved while maintaining the benefits gained from automated disclosure.

5 Implementing privacy and self-presentation in ContextContacts

To concretize the design principles developed above, we show how they can be applied to an example application, our ContextContacts. This section is not organized along the principles. Instead we show the features in the next version of ContextContacts and how they implement the principles. This is because the same feature may well implement several principles.

Not all of the principles are free of contradictions. The features here show partly how they can be balanced, but more importantly they show how enough leeway can be left for the user to decide that balance.

5.1 Integrated into the phone book

Principles applied: do not try to do everything within the system; support opportunistic use.

Figure 1 shows the main user interface of ContextContacts. The defining idea of ContextContacts has been to integrate it fully into the built-in phonebook, which we will keep in the upcoming version. The reasoning is that by integrating a view of others into the mobile communication, we integrate the information both to the actual person associated with a phone book entry as well as to the practices of communication with that person. The boundary between ContextContacts and the established practice of calling and texting is weak, allowing the user to see the one as an extension of the other—weaknesses and strengths of the one can be augmented or augmenting the other.

Since using the phonebook is so central to the use of a mobile phone, information in the book is constantly available. This mimics ambient displays on a desktop screen, without actually having one. The information shown here can be used opportunistically, catching interesting tidbits of others (the user might think “Hey, he’s here as well”, “Hmm, wonder what she’s doing over there?”) from the corner of your eye.

The user can see them-self in the phonebook as well, supporting a constant awareness of what is being disclosed and how the user’s situation is reflected in the situation of

others and the communication from them. This also allows the user to build a coherent picture of the status of the whole group.

5.2 Freezing

Principles applied: allow the user to lie

Faking information in automated disclosure can be hard: the faked data must be plausible, and transitions from real data to faked and back must be plausible as well. The user must also be completely aware of what the faked data is, so that they can maintain the lie in other disclosure.

In the next version of ContextContacts the user can *freeze* their current state. When the information is frozen, the effect is as if they had left the phone at that point: the location stays the same, it looks like they are not using the phone and changes in profile are not transmitted. To maintain the illusion that data is updated, however, the calendar events are updated according to current time.

Freezing supports a plausible transition *to* faked information, plausible faked information and easy understanding of what is being transmitted to others. Transitions *from* the frozen state are more difficult. The most plausible view is generated if the user returns to the same location where they froze the data. This allows for example the user to pop out of the office for a while without letting the system reveal that. If the user unfreezes the data in some other location, the location history is zeroed but the current location will be shown, resulting in a jump in position. Such jumps may be attributed to a failure in the locationing system, but may also reveal the lying.

5.3 Free-text description

Principles applied: allow for commenting, modifying and framing automatic disclosure; allow the user to lie; provide for feedback.

Not only is the awareness display of ContextContacts integrated with calling and texting, but also instant messaging. The free-text description supports a continuum of use from being just another situational cue, to commenting on the other cues to chatting with the others. We will keep this ability in the upcoming version. The free-text can be set both from the explicit self-view as well as from the phonebook. Changing one’s description takes less interaction than, say, sending an SMS.

In previous versions of ContextContacts, changing the free-text description does not alert the receivers in any way. In the next version the user can specify whether an alert should be generated. This will allow for drawing more or less attention to the text, including drawing attention while not drawing attention (e.g., if you think you are doing something cool, but do not want to brag overtly

about it, you might set “Bar-hopping” as a comment to your location, but would not alert the others).

The idea with drawing attention to one’s situation allows both for disclosure management and self-presentation via emphasizing or de-emphasizing aspects of one’s situation or some situations over others. Since no receiver will pay equal amounts of attention at all times, control over attention is in effect control over disclosure. So although the same information is in principle revealed all the time, by controlling at which times it is actually looked at the discloser controls the boundary.

The ability to hold textual conversations in ContextContacts of course allows for a high degree of self-presentation: the user can both state anything they want as well as receive replies to the statements from others. This way the user can monitor how successful their presentation is.

5.4 Naming of places

Principles applied: allow for commenting, modifying and framing automatic disclosure; allow the user to lie; do not try to do everything within the system.

ContextContacts does not show the location of the user on a map. Instead we show the name of the current location (and the previous one). The names come normally from a network location service, which gives the official name for the district the user is in, for example it could be Covent Garden, London.

Previously, the user has not been able to change the automatically retrieved names, with the idea that automatic naming should be more convenient. We are now making it possible for the user to assign a name for the current location them-self. This allows for meaningful names, for example Home or School, but also for free manipulation of the location disclosure. As Palen showed the case to be with calendar events [46]: if the text automatically shown is input by the user with the knowledge it will be shared with others, it is not perceived to be a privacy problem.

The user can fully disguise their location with this facility (name the cafe by their school “School” as well), name something so that only a part of the audience knows its meaning, or give very semantically accurate labels (“Harry’s bar”). If the information is not meaningful to the receiver, this of course reduces the value of that information. We assume that users will be quite capable of balancing disclosure control and utility themselves. It is always also possible to call or SMS the discloser to get more information on the location.

5.5 Activity indicators

Principles applied: provide for feedback.

All versions of ContextContacts have had a phone-use indicator. The reasoning has been that call answering and time-since-last-phone-use are highly correlated, and so the indicator is useful for making availability inferences. The Schoolmates user study showed, however, that the users were very much interested in when *ContextContacts* was being used, not just when the phone was used. They used the existing indicator as a cue of that, but it was of course not fully reliable. They also were keenly aware that the phone use indicator implied that they were monitoring the behavior of others.

The next version of ContextContacts will have an explicit indicator for use of the presence-enhanced phonebook. This will allow users to know whether their information is actually being looked at, not quite in as much detail as the Lookup log, but preserving opportunistic use. Since we assume that self-presentation and disclosure control are done via focusing attention to certain cues or times, feedback on attention are important for successful presentation.

This indicator will of course also be an improved cue as to availability for instant messaging. Many instant messaging clients have typing and activity indicators. To save battery power and communication costs, we cannot have quite the level of real-time indication, but will instead integrate activity over time. The detail-view will for example say that the other person has “used ContextContacts 5 times in last 3 min”, or “not used ContextContacts for 30 min”.

5.6 Lookup log

Principles applied: support lightweight permissions; do not try to do everything within the system; provide for feedback.

The user-interface figures shown so far have all shown the location, bluetooth environment etc. in the phonebook list view. This has always been the case with ContextContacts. It allows for very quick use of the information, but does preclude the application from knowing when the user is looking at somebody’s information.

If we remove all the automatically sensed data (location, buddies, bluetooth devices) from the list view the user will have to go to the detail view to see that information. In that case we know exactly when the user is looking at somebody’s presence information. This can also be then logged and transmitted to the person who is being looked at. Figure 2, the *Lookup log*, shows how this will appear to the looked-at user: all lookups done by others are listed, an indicator shows if they are new lookups, and additionally a tone can be played when a lookup notification is received.

There are several benefits to be gained from this: the looked at person will have an exact idea of what has been



Fig. 2 Lookup Log. Time and date of presence lookups made by others are shown, and by clicking on the log item the information that was revealed is shown

disclosed (compare to Lederer et al.’s idea of not hiding actual disclosure). This reduces at least unnecessary fear that somebody is using the system to monitor or track you. The lookups themselves can act as a communication channel: for example, when on your way to meet somebody you see they have looked at location you know that they now know how far you are and that you are on your way, or lookups may serve as a notice that somebody’s trying to gauge your availability. Self-presentation relies on the ability to monitor the others you are presenting to, this enables at least knowing that somebody saw the information. Lastly, and most importantly, the lookup log allows for *retroactive permissions*.

The idea of retroactive permissions is that you implicitly rely on people to only monitor you according to rules explicitly or implicitly negotiated. Instead of having to manually close and open the disclosure channel, you rely on them only to access it in situations where you would have it open anyway. Now with the lookup log, you can see whether the rules are being respected. If they are not, you can confront the person disobeying and reinforce those rules or to disable access to that person. This way management is only needed if something is wrong, and in the optimal situation no actions are needed.

The removal of information from the list view of course violates the principle of allowing opportunistic use. It is still more lightweight than, say, explicit request-reply [4], but probably limits use to situations where the looker has an a priori motive to look at the information. We suggest that the lookup log is to be used in the unequal-power relationship (boss–employee, parent–child), and further that in such relationships there are very few situations where opportunistic use would be important (When did you last ask your control-freak boss for a coffee just because you met him in town?).

5.7 Groups

Principles applied: make it possible to appear differently to different people; support lightweight permissions.

As both disclosure and self-presentation are inherently target-dependent, all of the features of ContextContacts given above will in the future apply not to everyone at once, but to *groups* of recipients. Turning the service on and off, freezing your state, requiring lookup logs and the content of the free-text description can be set either for all, or for a group at a time. Groups may have as many or as few members as the user wants. The self-view is extended to show how the user appears to the different groups and to allow manipulation of this (see Fig. 3).

We emphatically do not aim for multiple *identities* within ContextContacts. As the users are bound to their real identities coupled to mobile phones, we aim to support multiple *roles* instead. The user will have the same identity, but may look different to different people.

A crucial point in allowing different roles to be specified and manipulated by the discloser is the ability to change the level of access somebody has. Consider the case of a co-worker becoming your boss. You might want to require lookup logging from them. If that was controlled on an identity level, you would need to get the boss to agree to start using a new identity for you. At role level, you just assume a new role in relation to the boss, assigning them to the “Boss” group. The problem with identity-based control has been reported with mobile phone use, where to disallow control to an ex-friend may require changing your number and getting *all* of your current friends to use the new number [8].

We have observed that people do not use contact groups on their mobile phones. Why should they use the group functionality in ContextContacts? The idea is that since instant messaging and presence are integrated, there are

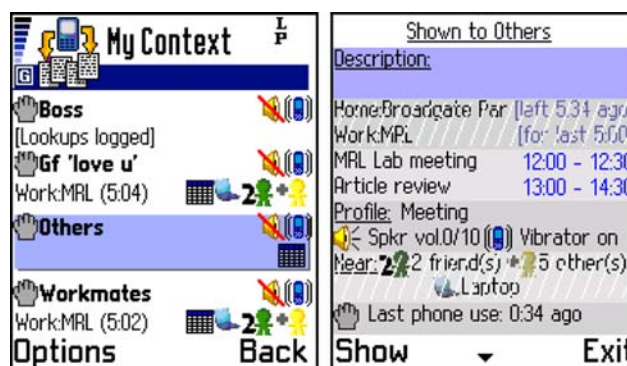


Fig. 3 Groups and visibility control. The user can quickly both see what they are disclosing to different others as well as manipulate that information. One click from the main view activates the details, where clicking on items enables/disables the disclosure of that item. Description is always sent, but may be empty

multiple motivations for grouping people. The user will want to chat about certain topics with their friends, and some other topics with their parents. This means that creating two groups supports not only disclosure management, but also other communicational needs.

Currently, groups in ContextContacts exist on each user's phone separately. This means that building a "real" group, where each user has the same members in it needs some real-world negotiation. The group instant messaging would not really work if the users did not agree on the composition of the group. An in-system representation of groups, like the one in Microsoft's 3 research system [47], would probably be necessary in a deployed system.

5.8 Controlling what gets disclosed or if any

Principles applied: do not take control away from the user; support lightweight permissions.

In previous versions, the user has had the ability to switch the service on or off. In the next version, the user can at control which of the available variables are communicated to others, or to switch off the service fully. The interface for doing that is shown in Fig. 3.

The idea is not only that the control is used dynamically (as it has been shown in the field studies that it may not be). The control has two more aims: making the users feel that they are in control and to set up a certain model of sharing in more institutional settings. The amount of fine-grained settings is to ensure that the machine is under the user's control.

The switching on and off has been made as available as possible, however, requiring only three interaction steps from the phone idle screen. This is so that should there be users who do end up wanting to switch the service on and off it is as convenient as possible (following Lederer's notions on allowing for coarse control).

5.9 Reciprocity

Principles applied: assume reciprocity.

Reciprocity is not a separate feature, but influences the implementation of almost all the other features. All the new features will be augmented to support reciprocity on a group-by-group basis:

- If you close off the service on your end, you will stop receiving updates of others.
- If you do not tell disclose certain variables (e.g., location, buddies) to somebody, you will not see that information for them.
- If you freeze your information, you will get others' information either.

- If you require lookup notifications from somebody else, they will get notifications from you.

This reciprocity does not cover everything: you may name places so that they do not reveal anything, you may not put things in your calendar, you can quickly reconnect and look at others and disconnect again. But these should be enough to for groups of users to build their own social rules around.

The rules here are implemented as "denier-side reciprocity". If you freeze, your client stops showing updates of others even if they are sending them, if you do not disclose your location to somebody, your client will not show their location and so on. The disclosure can be easily re-negotiated as it does not require mutual agreement over starting to disclose something.

6 Implications on social awareness protocols

The principles we have developed have implications beyond interaction design and feature specifications. They give clear guidelines for the design of protocols as well. Here we show how they can be applied to two Internet Engineering Task Force (IETF) social awareness protocols: SIMPLE [52] and XMPP [53].

Let us first assume a typical instant messaging service with some presence information, such as MSN Messenger,³ AIM⁴ or ICQ:⁵ the client gathers data on the user and sends this to all of the members in the user's buddy list. The user may control some or all of this data, for example, appearing off-line. The user has full control over who is on their buddy list, and can add and remove buddies at will. They may also switch off and on the client application.

If we look at the features described in the previous section, are number of requirements emerge on top of the basic model:

- Dynamic control over who gets to see what information
- Appearing differently to different groups of buddies
- Reciprocal disclosure
- Faking some or all of the presence information
- Requiring the receiver of presence to notify the sender when they look at the information.

These requirements can now be contrasted by the capabilities afforded by SIMPLE with GEOPRIV [52, 54] and XMPP (Jabber) [53, 55]. These basically assume that

- Information about the user (e.g., location) is gathered by one or more clients acting on behalf of the user.

³ <http://messenger.msn.com/>.

⁴ <http://www.aim.com/>.

⁵ <http://www.icq.com/>.

- The user may, even dynamically, decide who this information is disclosed to and to what extent. They may for example say that person X only gets to know which city they are in, and person Y also which district.
- Presence information can be either pushed to the receiver, or pulled by the receiver's client when required. The push or pull policy can be set by the sender. The pull may result in a query to the sender as to whether they want to send the information or not.

The access rules are managed on the client-side but applied on the server, so that the server may, for example, get information from several clients and apply the same rule-set to all that information. Additionally both protocols allow the user to send specifically tailored presence information to explicitly named buddies (directed presence). Buddies can be assigned to groups, and access rules can be per-group.

The features of SIMPLE and XMPP do not support all of the requirements given above in an efficient manner. The only way to appear differently to different groups or to lie selectively is to send directed presence to all recipients. We would propose the following extensions:

- Instead of purely filtering out some variables, it should be possible to give fixed (faked) values for those variables to a group of recipients.
- Since mobile clients are often offline, while the last known data may still be of interest to the recipient, the latest directed presence should be kept on the server even if the client becomes unavailable.
- If requested, pulls from the server should be logged and notifications sent to clients when they reappear online.
- It should be possible to set the server to make denials of access (faking and not disclosing) reciprocal, not sending information about others to the denier.

All of these can of course be implemented by client-side mechanisms, together with directed presence. The sending client handles reciprocity, faking and access rules, the receiving client notifications on looking at the information. This is what ContextContacts does when using a standard XMPP server. This is not efficient, since it requires the client to send a separate version of the presence information to each recipient: multiplying the amount of data by the number of recipients. Client-side implementation also requires a trusted client. Although the upcoming smartphones will allow for integrity checks on application [56] they still do not allow the client to prove its identity over the network.

We have constructed a custom proxy for ContextContacts that implements the above-mentioned extensions on top of XMPP. The client sends the proxy the group definitions and has then available the following per-group

operations: freeze, disconnect and require lookup notifications. Reciprocity and the sending of lookup notifications are still implemented on the client (we are assuming a trusted client in the research setting). Additionally the proxy implements a half-duplex optimization: when the phone is not being used, the proxy collects updates from others and stores them. When the user takes the phone into use again, the client requests the queued updates from the proxy. This is fast enough over the GSM data channel to not result in a visible lag to the user.

The next step with the proposed extensions to XMPP and SIMPLE is to formalize them into extension proposals with actual protocol definitions and submit them to the IETF. We will first evaluate the extensions in further field studies. There are two distinct motivations for the extensions: efficiency with mobile communications and privacy management. There are probably more privacy-related issues in both than we have discussed here.

7 Security in ContextContacts

Although we have been focusing on privacy from the perspectives of social interaction between people who know each other, we do need to provide for security as well. We outline here some of the salient design ideas. The treatise is not very rigorous, and assumes a familiarity with private-key security (for a thorough introduction, see [57, Chap. 2.5]).

Anonymity is not quite appropriate for a presence service, but pseudonymity may be. We assume that users of ContextContacts want to bind presence information to people known to them, but real identities are not used in the communication. Instead we use XMPP identifiers, which are effectively pseudonyms. For automatic generation of the identifiers we may use a single server and generate the user-name part by hashing the eight last digits of the phone number. This will allow for easy discovery of somebody whose phone number you know (using eight last digits tends to work whether you are using a local or international form of the number) without disclosing the number.

We can protect the client-server communication from eavesdropping with Secure Socket Layer (SSL), which is supported with most XMPP server implementations. If we use just one server, we can install the server certificate along with the application to verify the server identity. In a more general setting, SSL is of-course vulnerable to man-in-the-middle due to user actions [58]. This seems to be an acceptable risk, since banks for example are willing to use SSL to secure communications with the client.

To protect from SSL man-in-the-middle as well as untrusted servers we can encrypt the presence information.

Since we assume that all clients will also have a phone number, we can use a text-message (SMS)-based side-channel to exchange keys. SMS can of course be spoofed, but mounting a simultaneous attack via SMS and Internet protocol (IP) is probably not the most economical attack vector. In a simple form, we would use a single key-pair for each sender: they would send the other half of the key to all buddies via SMS and encrypt the presence (and IM) data with the other half.

Encrypting the full representation of the presence of course precludes intelligent filtering or modification of that data on the server-side, as proposed in the previous chapter. Instead we can just encrypt the contents of fields and send the field names in plain text.

We have not implemented these security mechanisms in ContextContacts, but they will become necessary for example for sharing corporate calendaring data.

8 Conclusions and future work

Privacy and self-presentation are best served in a system where the users' explicit actions create the information shown to others, and they can see how others use that information. This article tries to balance this fact with the potential benefits of automated disclosure and opportunistic use, allowing for the negotiation of Altman's privacy boundaries [9] through actions, rather than configuration [5]. This balance expressed in the design principles in Sect. 4 can be summed up into three more general ideas:

1. Even if all cues are transmitted all the time, others do not pay the same amount of attention to all cues and at all times. By manipulating that attention the user can control how others see them. The attention can be gathered as simply as sending messages which alert the receiver in some way: "here I am, look at me". This contrasts strongly with a priori control of disclosure, such as preferences: controlled disclosure has at most the potential to diminish losses—gaining attention through actions may give new positive effects to both parties.
2. Allowing users to label and comment on automatically derived data enables both control of disclosure as well as impression management. Again, this allows for new positive effects. It also allows for self-expression, collaboration, or group cohesion through labels that have different meanings to different audiences: by using a shared name for a location the user both expresses membership in the group as well as potentially masking their location from non-members.
3. Both privacy and self-presentation rely on adequate feedback of what others see and pay attention to, and

what they think. If we do not know whether others read our message, or looked at our situation, we cannot build on that information. Interaction is very poor, if each comment has to make sense on its own. *Unnecessary* feelings of monitoring are also precluded, if the actual amount of attention paid to oneself is known.

The principles we propose build coherently on the existing body of research in privacy within ubiquitous computing. Langheinrich's "Principles of Privacy-Aware Ubiquitous Systems" [3] provide the basis for building systems that handle private data. Palen and Dourish [7] have applied Altman's privacy negotiation theory to the design of computing systems—we continue on this path, but see self-presentation [12] as an equally central concept, and show how they can be applied together. Following Aoki and Woodruff [8] we allow for *ambiguity* in the actions of the system, but add concrete mechanisms for the user to create meaning on top of that ambiguity. We disagree with Consolvo et al. [25] and Smith et al. [4] in that management of disclosure could not coexist with automated disclosure: our field-studies give ample evidence that automated disclosure can be desirable, and the three ideas above show how it can be reconciled with privacy. We do, however, strongly agree with them in that awareness systems should be designed not to facilitate *observation* but to facilitate *disclosure*—they are not created for the audience, but the presenter.

Our user studies give initial support for applying the theory of self-disclosure [17] and Goffman's self-presentation [12] to (partially) automated disclosure: we have observed that such disclosure may facilitate relationship-building and positive affect [18], and that users do have the need to augment the impressions given off by the automated disclosure [12]. We have also seen that users have been highly aware of the audience in the control of disclosure and self-presentation [12]. From related research we hypothesize the need for more control over the automated disclosure in unequal relationships as well as the need for deception [12, 21], and testing these hypotheses will be central to our future research. Two other interesting issues are "peeping" and group management: should the system take into account that people may become uncomfortable when looking at information of others? How should overlapping groups (such as the two groups parents and family) be handled, for example, should there be multiple representations of the discloser for the same recipient?

Social awareness is an expanding area of research. There have been a number of research systems both for mobile and desktop settings [30, 31, 59–63]. Awareness is an emerging area for commercial services as well, with

examples like Plazes,⁶ dodgeball⁷ and Proximating.⁸ From a privacy perspective, the defining quality of social awareness is the *automated collection and disclosure* of personal data, such as location or activities. This characterizes also other application areas, such as automated photo sharing [64, 65] or location-based messaging [66, 67]. The design principles we have described should be relevant to all these areas. The next steps will be in concretely applying them to the design of such related fields, and testing the results.

Acknowledgments This work has been funded by the Academy of Finland under the PROACT research programme, and by the Helsinki Graduate School in Computer Science and Engineering. We thank Antti Salovaara, Sakari Tamminen, Marko Turpeinen, Louise Barkhuus and Markus Bylund for commenting on drafts of the paper and Kliment Yaney for comments on the protocol design section.

References

- Oulasvirta A, Raento M, Tiitta S (2005) ContextContacts: re-designing SmartPhone's Contact Book to Support Mobile Awareness and Collaboration. In: Proceedings of the 7th international conference on human computer interaction with mobile devices and services, MOBILEHCI'05. ACM, pp 167–174
- Dourish P, Bellotti V (1992) Awareness and coordination in shared workspaces. In: CSCW '92: proceedings of the 1992 ACM conference on Computer-supported cooperative work. ACM Press, New York, pp 107–114
- Langheinrich M (2001) Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. In: Abowd GD, Brumitt B, Shafer SA (eds) Proceedings of the third international conference on ubiquitous computing (UbiComp 2001), vol 2201. Lecture Notes in Computer Science. Springer, Atlanta, pp 273–291
- Smith I, Consolvo S, Lamarca A, Hightower J, Scott J, Sohn T, Hughes J, Iachello G, Abowd GD (2005) Social disclosure of place: from location technology to communication practices. In: Gellersen HW, Want R, Schmidt A (eds) Pervasive computing: third international conference, PERVASIVE 2005, Munich, Germany, May 8–13, 2005. Proceedings, vol 3468. Lecture Notes in Computer Science. Springer, Berlin, pp 134–151
- Lederer S, Hong JI, Dey AK, Landay JA (2004) Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput* 8(6):440–454
- W3C (2005) Platform for Privacy Preferences (P3P) Project, online, <http://www.w3.org/P3P/>, referenced Jun 2006
- Palen L, Dourish P (2003) Unpacking “privacy” for a networked world. In: CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems. ACM Press, New York, pp 129–136
- Aoki PA, Woodruff A (2005) Making space for stories: ambiguity in the design of personal communication systems. In: CHI '05: Proceeding of the SIGCHI conference on human factors in computing systems. ACM Press, New York, pp 181–190
- Altman I, Vinsel A, Brown BB (1981) Dialectic conceptions in social psychology: an application to social penetration and privacy regulation. *Adv Exp Soc Psychol* 14:108–161
- Margulis ST (2003) On the status and contribution of Westin's and Altman's Theories of Privacy. *J Soc Issues* 59(2):411–429
- Petronio S (2002) Boundaries of privacy, dialectics of disclosure. State University of New York Press
- Goffman E (1990) The presentation of self in everyday life. Penguin Books, London, Reprinted, original 1959 Anchor Books
- Raento M, Oulasvirta A (2005) Privacy management for social awareness applications. In: Proceedings of the workshop on context awareness for proactive systems, CAPS 2005. Helsinki University Press, pp 105–114
- Goffman E (1967) Interaction Ritual, chapter On Face-Work. Pantheon Books, New York, pp 5–45
- Hong JI, Landay JA (2004) An architecture for privacy-sensitive ubiquitous computing. In: MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services. ACM Press, New York, pp 177–189
- Nardi BA, Whittaker S, Bradner E (2000) Interaction and interaction: instant messaging in action. In: CSCW '00: Proceedings of the 2000 ACM conference on Computer supported cooperative work. ACM Press, New York, pp 79–88
- Berg JH, Derlega VJ (1987) Themes in study of self-disclosure. In: Derlega VJ, Berg JH (eds) Self-disclosure. Theory, Research and Therapy. Plenum Press, New York, pp 1–8
- Vittengl JR, Holt CS (2002) Getting acquainted: the relationship of self-disclosure and social attraction to positive affect. *J Soc Pers Relat* 17(1):53–66
- Miller JB, Stubblefield A (1993) Parental disclosure from the perspective of late adolescent. *J Adolesc* 16:439–455
- Leary MR, Kowalski RM (1990) Impression Management: a literature review and a two-component model. *Psychol Bull* 107(1)
- DePaulo BM, Kashy DA, Kirkendol SE, Wyer MM (1996) Lying in everyday life. *J Personal Soc Psychol* 70(5):979–995
- GEOPRIV Working Group Archives (2003) Geopriv and actively lying. Mailing list exchange, online, <http://ecotroph.net/~anewton/hypermail/geopriv/0309/0846.html>, referenced June 2006
- Berger PL, Luckman T (1966) The social construction of reality: a treatise in the sociology of knowledge. Garden City, New York
- Antaki C, Barnes R, Leudar I (2005) Self-disclosure as a situated interactional practice. *Br J Soc Psychol* 44:181–199
- Consolvo S, Smith IE, Matthews T, LaMarca A, Tabert J, Powledge P (2005) Location disclosure to social relations: why, when, and what people want to share. In: CHI '05: Proceedings of the SIGCHI conference on human factors in computing systems. ACM Press, New York, pp 81–90
- Grice H (1975) Logic and conversation. In: Cole P, Morgan JL (eds) Syntax and semantics, Speech Acts, vol 3. Academic Press, New York, pp 43–58
- Schegloff EA (1972) Notes on a conversational practice: formulating place. In: Sudnow D (ed) Studies in social interaction. The Free Press, New York, pp 75–119
- Oulasvirta A, Petit R, Raento M, Tiitta S (2006) On how users interpret and act upon mobile awareness cues. *Human-Computer interaction* (in press)
- Raento M, Oulasvirta A, Petit R, Toivonen H (2005) Context-Phone, a prototyping platform for context-aware mobile applications. *IEEE Pervasive Comput* 4(2):51–59
- Bardram JE, Hansen TR (2003) The AWARE architecture: supporting context-mediated social awareness in mobile cooperation. In: Proceedings of the CSCW03. ACM Press, New York, pp 192–201
- Milewski AE, Smith TM (2000) Providing presence cues to telephone users. In: CSCW '00: Proceedings of the 2000 ACM conference on Computer supported cooperative work. ACM Press, New York, pp 89–96

⁶ <http://www.plazes.com/>.

⁷ <http://www.dodgeball.com/>.

⁸ <http://www.proximating.com/>.

32. Katz J, Aakhus M (eds) (2002) *Perpetual contact: mobile communication, private talk, public performance*. Cambridge University Press, Cambridge
33. Ling R (2004) *The mobile connection: the cell phones impact on society*. Morgan Kaufmann, San Francisco
34. Laasonen K, Raento M, Toivonen H (2004) Adaptive on-device location recognition. In: *Proceedings of the 2nd international conference on pervasive computing (Pervasive 2004)*, vol 3001, Lecture Notes in Computer Science. Springer, Berlin, pp 287–304
35. Prinz W (1999) NESSIE: an awareness environment for cooperative settings. In: *Proceedings of the sixth European conference on computer supported cooperative work—ECSCW99*. Kluwer, Dordrecht, pp 391–410
36. Rubin Z (1975) Disclosing oneself to a stranger: reciprocity and its limits. *J Exp Soc Psychol* 11(3):233–260
37. Ambady N, Bernieri F, Richeson JA (2000) Toward a history of social behavior: judgmental accuracy from thin slices of the behavioral stream. *Adv Exp Soc Psychol* 32:201–271
38. McEwan G, Greenberg S (2005) Supporting social worlds with the community bar. In: *GROUP '05 Proceedings of the 2005 international ACM SIGGROUP conference on supporting group work*. ACM Press, New York, pp 21–30
39. Wiberg M, Whittaker S (2005) Managing availability: supporting lightweight negotiations to handle interruptions. *ACM Trans Comput Hum Interact* 12(4):356–387
40. Deci EL, Ryan RM (2000) The “What” and “Why” of goal pursuits: Human needs and the self-determination of behavior. *Psychol Inq* 11(4):227–268
41. Sloane L (1992) Orwellian dream come true: a badge that pinpoints you. *The New York Times*, September 12
42. Lee A, Girgensohn A, Schlueter K (1997) Nynex portholes: initial user reactions and redesign implications. In: *GROUP '97 Proceedings of the international ACM SIGGROUP conference on supporting group work*. ACM Press, New York, pp 385–394
43. Griswold WG, Shanahan P, Brown SW, Boyer R, Ratto M, Shapiro RB, Truong TM (2004) ActiveCampus: experiments in community-oriented ubiquitous computing. *Computer* 37:73–81
44. Barkhuus L, Dey AK (2003) Location-based services for mobile telephony: a study of users' privacy concerns. In: *Interact 2003*. ACM Press, Zurich, pp 709–712
45. Oulasvirta A, Tamminen S, Roto V, Kuorelahti J (2005) Interaction in 4-s bursts: the fragmented nature of attention in mobile HCI. In: *Proceedings of the 2005 conference on human factors in computing systems (CHI 2005)*. ACM Press, New York, pp 919–928
46. Palen L (1999) Social, individual and technological issues for groupware calendar systems. In: *Proceedings of the SIGCHI conference on Human factors in computing systems* ACM Press, New York, pp 17–24
47. Zaner M, Chung EK, Savage T (2003) 3 and the Net Generation: Designing for Inner Circles of Friends. In: *Proceedings of the workshop on intimate ubiquitous computing at UbiComp 2003*. Intel Corporation, online, <http://berkeley.intel-research.net/paulos/lab/ubicomp03/Workshop/index.html>, referenced June 2006
48. Phillips DJ (1996) Defending the boundaries: identifying and countering threats in a usenet newsgroup. *Inf Soc* 12(1):39–62
49. Smith CB (1997) Conduct control on usenet. *J Comput Mediat Commun* 2(4)
50. Weilenmann A, Larsson C (2001) Local use and sharing of mobile phones. In: Brown B, Green N, Harper R (eds) *Wireless world: social, cultural and interactional aspects of wireless technology*. Springer, London, pp 99–115
51. The European Commission (1995) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Off J Eur Commun (L 281)*:31–50
52. IETF Secretariat (2005) SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE), online <http://www.ietf.org/html.charters/simple-charter.html>, referenced May 2005
53. Saint-Andre P (ed) (2004) IETF. RFC 3920. Extensible messaging and presence protocol (XMPP): Core, October
54. Peterson J (2004) A presence architecture for the distribution of GEOPRIV Location Objects
55. Saint-Andre P (ed) (2004) IETF. RFC 3921. Extensible messaging and presence protocol (XMPP): instant messaging and presence
56. Symbian Ltd (2006) How has Symbian Signed evolved with Symbian OS v9? online, https://www.symbiansigned.com/How_has_Symbian_Signed_evolved_with_Symbian_OS_v9.pdf, referenced June 2006
57. Schneier B (1995) *Applied cryptography*, 2nd edn. Wiley, London
58. Burkholder P (2002) SSL Man-in-the-Middle Attacks. Technical report, February 2002. online, <http://www.sans.org/rr/whitepapers/threats/480.php>, referenced Jun 2006
59. Tang JC, Yankelovich N, Begole J, Van Kleek M, Li F, Bhalodia J (2001) ConNexus to awarenex: extending awareness to mobile users. In: *CHI '01: Proceedings of the SIGCHI conference on human factors in computing systems*. ACM Press, New York, pp 221–228
60. Holmquist LE, Falk J, Wigström J (1999) Supporting group collaboration with interpersonal awareness devices. *Pers Technol* 3(1–2):13–21
61. Marmasse N, Schmandt C, Spectre D (2004) WatchMe: Communication and Awareness Between Members of a Closely-Knit Group. In: Davies N, Mynatt E, Siio I (eds) *UbiComp 2004: Ubiquitous Computing: 6th International Conference Nottingham, UK, September 7–10, 2004 Proceedings*, vol 3205. Springer, Berlin, pp 214–231
62. Burak A, Sharon T (2004) Usage patterns of FriendZone: mobile location-based community services. In: *MUM '04: Proceedings of the 3rd international conference on Mobile and ubiquitous multimedia*. ACM Press, New York, pp 93–100
63. Isaacs EA, Tang JC, Morris T (1996) Piazza: a desktop environment supporting impromptu and planned interactions. In: *CSCW '96: Proceedings of the 1996 ACM conference on Computer supported cooperative work*. ACM Press, New York, pp 315–324
64. Davis M, Van House N, Towle J, King S, Ahern S, Burgener C, Perkel D, Finn M, Viswanathan V, Rothenberg M (2005) MMM2: mobile media metadata for media sharing. In: *CHI '05: CHI '05 extended abstracts on Human factors in computing systems*. ACM Press, New York, pp 1335–1338
65. Counts S, Fellheimer E (2004) Supporting social presence through lightweight photo sharing on and off the desktop. In: *CHI '04: Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM Press, New York, pp 599–606
66. Rantanen M, Oulasvirta A, Blom J, Tiitta S, Mäntylä M (2004) InfoRadar: Group and public messaging in mobile context. In: *Proceedings of NordiCHI04*. ACM Press, New York, pp 131–140
67. Persson P, Espinoza F, Fagerberg P, Sandin A, Cöster R (2003) GeoNotes: a location-based information system for public spaces. In: *Designing information spaces: the social navigation approach*. Springer, London, pp 151–173