Department of Computer Science
Series of Publications A
Report A-2007-2

Exploring privacy for ubiquitous computing: Tools, methods and experiments

Mika Raento

To be presented, with the permission of the Faculty of Science of the University of Helsinki, for public criticism in Auditorium XII, University Main Building, on May 29, 2007, at 12 o'clock.

University of Helsinki
Finland

Contact information

Postal address:
Department of Computer Science
P.O. Box 68 (Gustaf Hällströmin katu 2b)
FI-00014 University of Helsinki
Finland

Email address: postmaster@cs.Helsinki.FI (Internet)

URL: http://www.cs.Helsinki.FI/

Telephone: +358 9 1911

Telefax: +358 9 191 51120

ISSN 1238-8645
ISBN 978-952-10-3986-7 (paperback)
ISBN 978-952-10-3987-4 (PDF)
Computing Reviews (1998) Classification: D.2.6, H.4.3, H.5.3, I.5.3, J.4, K.4.1
Helsinki 2007
Helsinki University Printing House

Exploring privacy for ubiquitous computing: Tools, methods and experiments

Mika Raento

Department of Computer Science
P.O. Box 68, FI-00014 University of Helsinki, Finland
mikie@iki.fi

PhD Thesis, Series of Publications A, Report A-2007-2
Helsinki, May 2007, 211 pages
ISSN 1238-8645
ISBN 978-952-10-3986-7 (paperback)
ISBN 978-952-10-3987-4 (PDF)

Abstract

Ubiquitous computing is about making computers and computerized artefacts a pervasive part of our everyday lifes, bringing more and more activities into the realm of information. The computationalization, informationalization of everyday activities increases not only our reach, efficiency and capabilities but also the amount and kinds of data gathered about us and our activities. In this thesis, I explore how information systems can be constructed so that they handle this personal data in a reasonable manner.

The thesis provides two kinds of results: on one hand, tools and methods for both the construction as well as the evaluation of ubiquitous and mobile systems—on the other hand an evaluation of the privacy aspects of a ubiquitous *social awareness* system. The work emphasises real-world experiments as the most important way to study privacy. Additionally, the state of current information systems as regards data protection is studied.

The tools and methods in this thesis consist of three distinct contributions. An algorithm for locationing in cellular networks is proposed that does not require the location information to be revealed beyond the user's terminal. A prototyping platform for the creation of context-aware ubiquitous applications called ContextPhone is described and released as open source. Finally, a set of methodological findings for the use of smartphones in social scientific field research is reported. A central contribution of this thesis are the pragmatic tools that allow other researchers to carry out experiments.

The evaluation of the ubiquitous social awareness application ContextContacts covers both the usage of the system in general as well as an analysis of privacy implications. The usage of the system is analyzed in the light of how users make inferences of others based on real-time contextual cues mediated by the system, based on several long-term field studies. The analysis of privacy implications draws together the social psychological theory of self-presentation and research in privacy for ubiquitous computing, deriving a set of design guidelines for such systems.

The main findings from these studies can be summarized as follows: The fact that ubiquitous computing systems gather more data about users can be used to not only study the use of such systems in an effort to create better systems but in general to study phenomena previously unstudied, such as the dynamic change of social networks. Systems that let people create new ways of presenting themselves to others can be *fun* for the users—but the self-presentation requires several thoughtful design decisions that allow the manipulation of the image mediated by the system. Finally, the growing amount of computational resources available to the users can be used to allow them to use the data themselves, rather than just being passive subjects of data gathering.

Computing Reviews (1998) Categories and Subject Descriptors:

D.2.6 Software Engineering: Reusable software—Reusable Libraries
H.4.3 Information Systems Applications: Communications Applications
H.5.3 Information Interfaces and Presentation: Group and Organization Interfaces—Asynchronous interaction, Collaborative computing, Computer-supported cooperative work, Evaluation/methodology
I.5.3 Pattern Recognition: Clustering—Algorithms
J.4 Social and Behavioral Sciences: Sociology, Psychology
K.4.1 Computers and Society: Public Policy Issues—Privacy, Regulation, Transborder data flow

General Terms:

Algorithms, Experimentation, Human Factors, Legal Aspects

Additional Key Words and Phrases:

Data Protection, Social Awareness, Ubiquitous and Mobile Computing

Acknowledgements

The fact that this thesis is now complete owes to the encouragement and support of my advisor, Hannu Toivonen. When I thought that hardly anything had been done yet he managed to help me see how the work that had been done could be gathered together to form this thesis. The Context project he helped to create and run provided the freedom for me to find out what kind of research I liked and to pursue it in my own way.

During these years the people who have helped create this thesis through their work in the Context project have been Kari Laasonen, Renaud Petit and Antti Oulasvirta (and Hannu, of course). Whatever I have been pondering, whether reasonable or not, whether related to our work or not, Kari has always had something insightful to say about my problem. Without Renaud there would most likely not have been any applications on top of ContextPhone and much of the experiments would have been poorer. And without Antti, I think we would not have got much sense out of the experiments. But the work of Context would have been much less vibrant and diverse if it hadn't been for John Evans and Andrew Patterson of the Aware project and the people I met through them: Ben Russell and Theo Humphries.

At the Department the people I went to when I needed an interesting conversation, a break from my current rut, were Evimaria Terzi, Greger Linden, Oskari Heinonen, Floris Geerts and Teemu Kurppa. They would let me talk about my ideas and thought me worth telling me theirs. More communally, both the old 3rd floor and the new 3rd floor coffee rooms would have been much less enticing without Helena Ahonen-Myka, Lili Aunimo, Marko Salmenkivi, Juha Makkonen and Saara Hyvönen.

The Department not only provides great collegues for research, but also excellent facilities for working with computers. I would wager that people who have not worked outside its walls do not realize how competently the systems are run—it is due to the fact that they run so well that we don't have to pay attention to them. Especially I'd like to thank Pekka Niklander for patiently getting all the hardware that I broke in my travels fixed.

Through the Context project, before and after it, I have received financial support from the Academy of Finland, the Helsinki Graduate School in Computer Science and Engineering and the Helsinki Institute for Information Technology, Basic Research Unit. I thank these funders: I have never had to give up an interesting idea or trip for the lack of fiscal resources.

Finally, this thesis would not have been possible without the support of my fiance Niina, who has (with varying patience) put up with the late nights and many trips that accompany work that, in the end, mostly consists of coding. I would also like to thank my parents, who have always both believed that I am capable of any task I care to undertake and let me choose those tasks myself.

Contents

1 Introduction **1**

2 Research questions **7**

3 Constructing the field of privacy in ubiquitous computing **9**

4 On social awareness **13**
4.1 Social awareness in CSCW and the concept of Media Spaces 14
4.2 Real-time Computer-mediated communication 16
4.3 Context-aware and mobile social awareness 18
4.4 ContextContacts 21

5 Privacy research traditions **27**
5.1 Law 27
5.2 Cryptography and computer security 29
5.3 Social Psychology 31
5.3.1 Boundary negotiation 32
5.3.2 Self-disclosure 33
5.3.3 Impression management 34
5.3.4 Entangled in other practices and concerns 35
5.4 Notes on some other related fields 35

6 Contributions of this thesis **37**
6.1 The articles 37
6.2 Answers to research questions 41

7 Outlook **43**

References **47**

Articles **62**

Chapter 1

Introduction

This thesis is about the use of personal data in the emerging age of ubiquitous computing. Specifically, the aim of this thesis is to explore how ubiquitous computing systems should be constructed so that they allow people to manage their privacy—to make their own, informed, decisions about who knows what about their activities. Ubiquitous computer systems have been envisioned as being used for new activities and to know much more about the user, creating a qualitative shift in the gathering, use and dissemination of data about human beings. For such a shift to be acceptable to these humans, the systems should treat that data in a sensible manner. This thesis is both about figuring out what a sensible manner is, and how to construct systems that actually behave in that manner.

Discussion on privacy has often been linked to advances in technology. Warren and Brandeis's 1890 essay "The Right to Privacy" [132], which has been seen as the introduction of privacy as a concept to the legal system of the United States, was sparked by developments in photography and printing. Portable, short-exposure cameras made it much easier for photographers to capture private moments and the newspapers could print these snapshots with less effort and cost than before. In the 1970's Adam Westin [13] began to write about the effects of databases on privacy through much more efficient collection, searching and combination of private data. The mobile phone, taking off in Europe by mid 1990's, has been universally seen as intruding on the individual's control over time and space as well as redefining public and private time and space [82, 84, 85, 106].

So threats to privacy by technology, often claimed to be serious, are nothing new, and we obviously can still conduct affairs in private. This does not mean that the threats resolve themselves. The use of the camera and printing press to publish private facts is carefully legislated in most countries. Finland, for example, prohibits the telling of falsehoods about

others to anyone, and the publishing of damaging information, whether factual or false, unless there is a balancing societal need for the information to be public. The growing use of databases was the direct cause for the Organisation for Economic Co-operation and Development (OECD) to create its "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" [95], influenced strongly by Westin, from which the European Community data protection legislation [124] is descended. The use of mobile phones has evolved rapidly, with the privacy issues becoming questions about social norms, expectations and conventions. The important common factors in all of these have been that the balance between privacy and other concerns has been the result of long deliberation, and that the process of maintaining that balance is ongoing.

Ubiquitous computing was envisioned by Mark Weiser in his seminal article "The Computer for the Twenty-First Century" in 1991 [133]. One of the defining ideas in the article was the "disappearing computer": computers would no longer be boxes sitting somewhere, but we would interact directly with computerized objects and spaces. Inherent in Weiser's vision has also been the idea that *all* objects and spaces will be computerized to some extent — hence *ubiquitous* computing. In this thesis I will use ubiquitous computing in a very wide sense: it is the computationalization of activities previously not computationalized. This includes not only novel sensor technologies (such as smart floors [97]) or interaction modalities (such as interactive tables [115]) but also the use of Internet for group communication and noticeboards, mobile and smart phones, digital media archives and web logs. Parts of the thesis, however, will focus on programmable mobile phones—smartphones—as the first real ubiquitous platform.

Ubiquitous computing is inherently privacy-sensitive, and has been criticized because of that from the beginning [116]. Any computer that a person interacts with knows where that person is (close to the computer) and what they are doing (to the extent the activities are carried out through the computer), and even catches hints of what the person is feeling (as both our interaction style as well as the content of communications reflect emotions). The aim of ubiquitous computing is to expand both the variety of activities that are carried out through computers as well as the computers' spatial reach. Not only will computers know whether you are at work or at home, and what you are working on or who you are sending e-mail to, but they will have constant knowledge of your movements and daily activities. A somewhat facile example is the automated fridge which knows when you are out of milk: it also knows when you wake up in the night, and how much milk you drink. The change is not purely quantitative, but also qualitative:

the kinds of actions known to computers are changing.

Thus, the aim of this thesis is to explore how people use ubiquitous systems that handle personal data, how they would like these systems to behave, how they can make informed decisions about the systems' behaviour, and how the systems should be constructed that they allow these decisions. The goal has been to construct real-world experiments in how people use technologies that gather and disclose personal data, and the practical tools and methods needed for such experiments make up half of the thesis. Since the whole field of ubiquitous computing would be infeasible to study through actual use, the user trials focus on a single application field: social awareness.

The body of the thesis consists of five peer-reviewed articles and one manuscript. The articles fall into several subfields of Computer Science: Data-analysis, Human-Computer Interaction and Information Systems. Some of them have been published in non-Computer Science fora. These articles describe a process of exploring privacy issues, rather than ready-made answers to questions on how systems should be constructed. New tools and methods were developed during the exploration, which are applicable to the study of human-computer interaction and human behaviour in general. Some tentative answers to the question on mechanisms and design guidelines are given for social awareness. These articles have not been included in any other theses.

Article I Adaptive On-device Location Recognition, Kari Laasonen, Mika Raento, Hannu Toivonen. In *Proceedings of Pervasive Computing: Second International Conference, PERVASIVE 2004*, LNCS 3001, Springer Verlag (2004), pp. 287-304. Berlin, Heidelberg, 2004. Springer Verlag.

In the article we describe a novel feature extraction and prediction algorithm for GSM-cell -based location data. The algorithm provides a necessary building block for location-based services without the need for operator support, enabling experiments on currently available smartphones. The off-line mathematical model was constructed jointly, Laasonen designed the on-line algorithm. I implemented the off-line algorithm, Laasonen the on-line one. I wrote the software that gathered the data needed for the evaluation. Two thirds of the article was written by me, one third by Laasonen. Toivonen provided comments and corrections.

Article II ContextPhone—A prototyping platform for context-aware mobile applications, Mika Raento, Antti Oulasvirta, Renaud Petit, Hannu

Toivonen. *IEEE Pervasive Computing*, 4(2): 51-59, 2005.

The article describes a software platform for prototyping mobile applications, especially context-aware applications: applications that gather and use data about the user. The platform was developed by myself and Renaud Petit. The description of the technology was written by me and Renaud Petit, while Antti Oulasvirta described the user-centered design process. Oulasvirta and I described how the platform can be used in research. Hannu Toivonen contributed parts of the introduction and conclusions, and gave feedback on the text.

Article III Data subject's right of access and to be informed in Finland—An experimental Study, Mika Raento. *International Journal of Law and Information Technology*, 14(3): 390–409, 2006.

The study described explores how well data controllers in Finland can fulfill the subject's requests for data concerning them and the processing of that data. It motivates the study of privacy-related issues in information technology by showing that organizations are ill-equipped to deal even with the privacy demands posed by current-day technology and legislation, and that inability is at least partially due to the qualities of the systems in use. The article is written for the specific framework of the European Community Data Protection directives, and thus largely for a European audience.

Article IV How mobile awareness cues are inferred and acted upon, Antti Oulasvirta, Renaud Petit, Mika Raento, and Sauli Tiitta. *Human-Computer Interaction*, 22(1–2), 2007 (In press).

In this article we describe the results from three long-term field studies with the ContextContacts mobile social awareness service. The results show that that especially young users are capable of confidently using a system that gathers and transmits highly personal data, and find multiple uses for such a system. The study was designed by the authors jointly, the software used constructed by I and Renaud Petit and the analysis carried out jointly. In the analysis I focused specifically on self-presentation and the use of messaging. Oulasvirta had the strongest influence on the actual text.

Article V Designing for privacy and self-presentation in social awareness, Mika Raento and Antti Oulasvirta. *Personal and Ubiquitous Computing*. Accepted for publication.

The article describes a number of design guidelines for supporting privacy management and self-presentation in ubiquitous social aware-

ness applications, based on a number of field studies. The majority of the ideas and text were contributed by me, with Oulasvirta providing comments and feedback throughout the text. The field studies referred to in the text were jointly run by me, Antti Oulasvirta, Renaud Petit and Sauli Tiitta, with the privacy-related analysis done by me and usage analysis by Oulasvirta. The software used in the studies was implemented by me and Renaud Petit.

Article VI Smartphones: an emerging tool for social scientists, Mika Raento, Antti Oulasvirta and Nathan Eagle. Manuscript submitted to *Sociological Methods and Research*.

In this article we analyze how smartphones in general and ContextPhone in particular can be used for social scientific field studies. I led the work on this article, with major contributions from Oulasvirta and Eagle. Of the field studies referenced, Eagle carried out one; I, Oulasvirta, Sauli Tiitta and Renaud Petit one and the third one is a review of work by third parties. We evaluated the importance, validity and reliability of the proposed methods jointly. The data-gathering software used in two of the studies was designed by me and implemented by me and Renaud Petit.

The aim of this introduction is to build a frame of reference, a viewpoint for the main body of work—the viewpoint of privacy. Due to the central role of social awareness in the exploration, the history of that field is included. This introduction will continue with the thesis's research questions, followed by a look at how to define privacy: the idea of spheres of privacy. I will introduce the field of social awareness through its inception in Computer Supported Co-operative Work through to our work on ContextContacts, a mobile context-aware social awareness system, noting the field's relationship to privacy issues. I will describe how the concept of privacy in computing has been influenced by different research traditions: legal, social psychological and computer science, that I have found useful in the work, followed by a short introduction to the application area under focus: social awareness. The spheres of privacy model is original work, whereas the descriptions of social awareness and of the findings from different fields concerned with privacy are purely literature reviews. I will not attempt to provide a detailed introduction to ubiquitous computing. For those unfamiliar with it, Yvonne Rogers provides a critical look at the current state of the art [109], while Adam Greenfield describes well the broader implications of such technologies in "Everyware" [60]. The introduction concludes with the main findings from the individual articles.

Chapter 2

Research questions

The original aim of this work was to provide guidance to builders of ubiquitous information systems, guidance on the kinds of mechanisms such systems should provide, so that the users are in actual control of information about themselves, so that they may make informed decisions about disclosing information to organizations, and give different impressions to different people. During the work, it became obvious that we would not be able to answer the question yet. One of the central ideas in the work has been that privacy cannot be studied in the abstract, it can only be studied through real-world human behaviour [34, 118, 81]. This leads to the first research question:

1 How can we study real-world privacy issues in ubiquitous computing? What tools and methods do we need?

Since I wanted to study real-world behaviour with application prototypes, the scope of the first question had to be narrowed—there was no way to study all kinds of ubiquitous applications. Our research project Context came to focus on *social awareness*, or presence, services: the provision of cues of remote others to the user, for example telling them where their friends are, are they available for communication and who they are with. This led to the second research question:

2 What kind of mechanisms should ubiquitous social awareness systems provide to the user, so that they can carry out impression management?

The next section will elaborate on what privacy means for ubiquitous computing, and will thus concretize the research questions.

Chapter 3

Constructing the field of privacy in ubiquitous computing

When looking at privacy-related research in computer science, the first feeling is that there is no consensus on what privacy is. The data mining community seems to focus on privacy-preservation [7, 83, 6, 121]: the ability to draw interesting facts from the combination of data from multiple sources without having to reveal the original data from one source to the other sources, or to allow mining of datasets by third parties without revealing individual items. From the security researchers' point of view privacy can be achieved via access controls [111, 128] and communications secrecy. For example, Diffie and Hellman's introduction of public-key cryptography claimed to solve the "cryptographic problem [...] of privacy: preventing the unauthorized extraction of information from communications over an insecure channel" [40]. The human-computer interaction field has looked at the interactional, processual nature of privacy in human communications and how it should be supported by technology [102, 134]. These very different approaches stem from focusing on different *spheres* of privacy: Individual–State (what information the nation-state has about citizens), Individual–Organizations (what we disclose to different organizations and what we get in return), Public (what anybody may know), and Groups (how we present ourselves to different reference groups).

The aim of this chapter is not to build an analytical framework to be used *within* this thesis. Rather, the spheres situate this thesis and its contributions within the larger frame of privacy as studied in different subfields of computer science as well as in other disciplines.

Individual–State The privacy between the state and an individual is best captured by the idea of civil liberties. Traditionally civil liberties

were defined only for citizens, but the current European thinking has extended them to all individuals, reflected for example in the new Finnish Constitution from 1995. The individual should be protected from unwarranted intrusions into the private life by the state (privacy of the home, privacy of communication, physical privacy of the body). The state does have non-negotiable powers over the individual, but the use of these powers is strictly regulated (e.g., legislation over personal searches, wiretapping). The individual may take precautions beyond the guarantees of the regulation, such as encryption of communications, but may be legally required to reveal the contents of such communication if deemed necessary for the public good. Critique of unnecessary surveillance by the state can most robustly be grounded in the idea that the collection of personal data is inherently *risky*: once such data has been collected, it may fall into the wrong hands, even if in theory "if you have nothing to hide, you have nothing to fear".

Individual–Organizations An individual enters into relationships with organizations for varying reasons: employment, hobbies, consuming or producing goods. The transactions they have with the organization create personal data, which may be valuable for the organization for profiling, business development or process optimization. These goals may not coincide with the interests of the individual (e.g., loyalty cards may be used to identify unprofitable customers and the information used to discourage their visits or to raise the price of items they tend to buy). Often the individual has a choice in whether to enter into the relationship and what transactions to make, although it would be naïve to think that the choice exists in all cases: there are many service monopolies or oligopolies, the threat of unemployment and social pressures. The data collection and processing by organizations is primarily regulated in the European Community with the 1995 directive "on the protection of individuals with regard to the processing of personal data and on the free movement of such data" [124] through member state implementations. The data protection legislation is comparable to other areas of consumer protection. Collection of personal data by organizations is of course no less risky than collection by the state, and often more risky due to less oversight and more actors.

Public An individual has an interest in maintaining control over their public image. Concrete harm may be done if they for example, engage

in activities that are deemed unacceptable by a portion of the public (for example communism) and public knowledge of such lessens their status or employment prospects. Concretely, the individual's privacy in relation to the general public could be defined as the ability to control the spread of information about oneself to others. Intrusions on private spaces, communications and the body by others are protected by legislation with very little leeway for interpretation. The publishing of information that has come to the knowledge of others may or may not be regulated, although defamation (publishing or relating false information) is almost universally legislated against. In practice, both intrusions and publishing may happen and a-priori protection against them plays a central role (locks on doors, access controls on information systems).

Groups An individual acts in many roles: as a parent, a spouse, a friend, a workmate, a boss or an official. Groups can be defined as people who see the individual in the same role, thus they may often be just dyads, and do overlap (for example the dyad formed by spouses overlaps the group of the immediate family). Privacy for the individual's participation in groups means the real ability to appear differently to different others. The appearance is a social construct, and thus does not necessarily mean keeping anything secret (although it may), but the opportunity through different emphases, interactions and actions, agree on different appearances. Although the legislation in force for the Public is of course in force for the Groups, it is mostly of no interest: the privacy is defined through balancing of the participants' needs and wants, through social norms and conventions.

This thesis is focused on the Groups and Individual–Organizations spheres, with some implications on the Public sphere. To an extent that information processing reveals or stores no personal data, it reflects on the Individual–State sphere, but I will not try to bring any specifics of that sphere into the discussion. The included articles cover these spheres as follows:

- Article I provides algorithmic methods that allow sidestepping the Individual–Organizations and Public spheres.
- Article II provides prototyping and data-gathering tools for studying the Groups sphere.
- Article III focuses solely on legal aspects of the Individual–Organizations sphere.

- Article IV describes the use a social awareness service, including self-disclosure and self-presentation, within the Groups sphere
- Article V applies social-psychological findings to create design guidelines for the Groups sphere.
- Article VI introduces new methods for research in the Groups sphere.

This introduction deals almost solely with issues in the Groups sphere, with the next chapter on social awareness touching on Individual–Organization and the Public spheres, on how the idea of social awareness has been found to be ill-suited to these spheres of activity.

Chapter 4

On social awareness

The main application field within which I discuss privacy in this thesis is Social Awareness or, more specifically, ubiquitous and mobile social awareness. This chapter will provide a historical overview of the development of social awareness, concluding with an analysis of how our work on ContextContacts builds upon previous work. I will start from the field's beginnings in Computer Supported Co-operative Work and Media Spaces, continuing through real-time computer-mediated communication (primarily instant messaging), on to context-aware systems through to the emerging integration of these application areas. The discussion will focus on the conceptual development of social awareness as well as how different understandings of technological systems reflect views on communication, social structures, context and privacy.

An oft-used definition of social awareness comes from the field of Computer Supported Co-operative Work (CSCW) and is due to Dourish and Bellotti [42]: "awareness is an *understanding of the activities of others*, which provides a *context for your own activity*". This definition of awareness is very broad (and as such suits even this thesis, which mostly deals in non-work situations). In effect any and all CSCW work can be seen as "awareness": access to shared artefacts and communication channels build awareness. *Awareness* is thus an emphasis, or an analytical stance, not a well-defined set of functions or goals (see also Schmidt's critical view on the concept [76]).

A social awareness system, thus, is a system whose goal is the creation of awareness of the activities of others. In more functional terms, awareness systems *record, interpret, transmit and represent* data about people and their activities. The pertinent system-level questions for studies of awareness are then: what and when to record, to what extent and how to interpret the recorded data, which of it to transmit to whom and how to

represent it. On a more processual level, the purpose of the system plays an important role: of whom the data is gathered, what it is to be used for and by whom—the sphere of the activity. Our work on ContextContacts (Article Vand Article IV, and [100, 107]) has been about *recording, interpretation* and *representation* on the functional level. On the processual level we have made the decision about who the data is gathered about as well as to whom it has been transmitted (and these have always been the same people), and our main interest has been in *what the data is used for and how*, and how that relates to what data is gathered and how it is represented. In this review of related work, I will focus on these issues. Especially, I will not discuss issues related to the real-time distribution of the data: the selection of what events or media streams are to be routed where, nor the detailed development of sensing technologies.

4.1 Social awareness in Computer Supported Co-operative Work and the concept of Media Spaces

Prinz [105] distinguishes two different kinds of awareness in CSCW: *task-oriented awareness* and *social awareness*. Task-oriented awareness is about *tasks* and *artefacts*: the data being gathered and represented is strongly bound to certain artefacts within the CSCW system and to the task of producing those artefacts. This work is exemplified by the ShrEdit shared editor with audiovisual links presented by Dourish and Bellotti [42], the GroupDesk system described by Fuchs et al. [54], and Ackerman and Starr's work on Social Activity Indicators [3]. The idea of awareness of others' actions through shared artefacts is grounded in formative ethnographic reports of real-time task co-ordination: Heath and Luff's study from a London Underground Control room [68] and Harper et al.'s study of Air traffic controllers [66]. However, these are settings with highly formalized artefacts, skilled work and repeated processes.

Work in other environments has a larger role for informal and opportunistic interaction, as argued by Isaacs [73] and Bly et al. [25]. *Social* awareness (a concept close to Nardi et al.'s "outeraction" [94]) is about producing knowledge of the others' actions even if they are not directly related to the task at hand or artefacts under manipulation. This kind of information can no longer be gathered only from interactions with the "shared workspace"—Moran and Anderson argue in 1990 [93] for two new paradigms for CSCW: co-ordinated communication and informal interaction. The move beyond the shared workspace and towards informal interaction—Social awareness, results in two distinct branches of research: Media spaces

[25] and what later becomes called Context-awareness.

The early work on Media spaces: long-term, reconfigurable video and audio links between locations, was carried out at Xerox PARC and EuroPARC. Dourish and Bly report on Portholes [43], describing low framerate always-on video links between workers, providing more a *sense* of shared context rather than knowledge of the detailed actions of others. Bly et al. [25] describe always-on real-time video and audio links. The idea spread quickly to other institutions. The Montage system at Sun reported on by Tang et al. [122] provided video links integrated with electronic sticky notes for use when the other person was not available. They found the system to support lightweight interaction similar to face-to-face meetings. Tollmar et al. [125] elaborate further the role social awareness to be the knowledge of the *social* situation of others, their current availability, relationships and interactions with other people, in their study on the design process of a system similar to Portholes and Montage, but with web-based access added. This emphasis on the social situation also defines a new goal for awareness: in addition to supporting impromptu interactions by letting the potential participants know of the opportunity, social awareness can also support the creation and maintenance of relationships, groups and social structures.

Work on Media spaces for social awareness was motivated by key factors inherent to video links: richness of the media, technical feasibility, and the availability of non-verbal cues. Richness of media: the high bandwidth, multiple cues and multiple media inherent audio and video links was assumed to support peripheral awareness, shifting attention between local and remote events [86] and intuitive negotiation of attention and availability [73]. Video and audio links are obviously technically feasible, in ways that context-aware systems are not necessarily. The ability to see gestures and facial expressions alleviates the problem of judging tone and emotional content compared to pure audio or textual communication [43]. The imitation of co-location, however, falls short in many ways: flatness of video, asymmetric viewpoints and lack of directional audio reduce the ability to interact over media links the same way we interact in physical space [55, 16].

Privacy was seen as a central problem for Media spaces from the beginning [87, 86, 41]: Although Media space mimics real space, it does not limit observability in the same way. Making control flexible and intuitive, providing feedback on whether a video feed was used by anybody and making access reciprocal emerged as design guidelines, Bellotti and Sellen drawing them together into a design framework [19]: users should have actual control and get actual feedback on the capture, construction, accessibility

and purposes of the media link. Another approach has been to add noise or to remove information from the media, for example by blurring video [27, 117] or by only indicating where there is activity within the field of view without displaying the activity as such [71]. Although filtering techniques were perceived by users to provide less information, and thus afford more privacy—as in revealing less to the other, computer manipulation of audio and video drastically lessen the ability of the observed person to manage the impression they are giving (I will return to the relationship between control over information and impression management in the next chapter). Lee at al. report of severe difficulties in spreading the Portholes system outside the research laboratory [81], including the users' lack of interest in controlling access by blurring the video. In general, Media spaces have been very influential in the emergence of Social awareness as a goal for systems and a topic for study, but the technology as such has not seen widespread adoption [76, 96]. The early assumption that non-verbal cues are essential for relational and emotional communication [33], based on communications theory and laboratory experiments, was later, after field studies in the use of Computer-mediated communication, dismissed as too narrow and pessimistic [129].

4.2 Real-time Computer-mediated communication

Computer systems have supported real-time text interchange for about 30 years. The combination of `finger` and `talk` enabled users of the Unix system to find out who was online, and to chat with them already in the mid-1970's. Internet Relay Chat (IRC) enabled non-local (`talk` tended to work only within a single system or a smaller number of trusted systems) and topic-oriented, group chat from late 1980's on. The basic availability indicators have been very much the same in most widespread instant messaging systems since: online/offline, active/idle and a textual away message. Widely available, commercial, Internet-based instant messaging systems started to appear in the mid 1990's. However, the relationship between awareness and instant messaging did not become an active interest within the Human-Computer Interaction (HCI) and CSCW fields before late 1990's.

Erickson et al. [50, 49] "call systems which provide perceptually-based social cues which afford awareness and accountability 'Socially Translucent Systems'". Translucency is described as a property of real-world, co-located human activity, where we may gain partial knowledge of the activity of others through windows or open doors, or by being able to hear ongoing

conversations around us. As an example, they present "babble": a real-time, persistent chat structured around freely formed conversations with social activity indicators. In babble, the chat system is enhanced with indicators of not only who is available for communication, but also who is currently active in which conversations, and conversely, which conversations are currently actively participated in. The timestamped, persistent conversation history provides a more detailed view into past and present activity. Through these measures, babble aims to recreate social cues often inhibited by technological mediation: the tempo, formality, attendance and acknowledgments of an ongoing conversation. Many of these proposed features are part of popular current commercial IM systems: IBM's Sametime, Skype, Microsoft's MSN Messenger, ICQ and AOL Instant Messenger do all support a persistent, timestamped conversations, although they have varying support persistent multi-user discussions structured on topics.

Nardi et al. [94] describe an ethnographic study of instant messaging (IM) in a corporate setting, bringing to focus a number of crucial issues that link real-time computer mediated communication and social awareness. They coin the term "outeraction" to describe the uses of IM that fall outside pure information exchange. Considering the goal of social awareness to support opportunistic interaction, IM with availability indicators supports the discovery of who is available for communication. More constructively, however, they note that opportunistic communication is not so much dependent on the ability of one of the communication partners to infer the availability of the other, but on the flexible negotiation of availability (see also Tang et al. [18]). IM supports this negotiation in three ways. First, IM can be used to send a message that does not interrupt or intrude them unless they do want to pay attention to their IM client. Second, asynchronity, in that the other party can wait an unspecified period of time to respond to an initiation of communication. And third, asynchronity, in the way that even if the response arrives much later than the initial request, it may still be utilized by the initiator as soon as they turn their attention to the conversation (cf. compared to purely synchronous media, such as telephony). Two other crucial features of IM use are its perceived informality and ignorability. The users under study clearly felt that it is socially acceptable to use IM for both less formal topics of conversation as well as for less formal style (tone). They also feel that they may ignore IM if they are busy, in a way they may not ignore a phone call. The first is less obviously linked to the technical characteristics of IM as a medium, whereas the second is likely due to the fact that the receiver of an IM message can read the message as it arrives and decide whether it warrants immediate

attention, without committing to a conversation. This study shows how IM *as such* is an awareness technology, even without additional indicators of what activity the others are engaged in or how interruptible they are. However, the "buddy list" with its online/offline indicators is seen as the enabler for the use IM.

Whereas Media Spaces were fairly expensive enterprises, deployed in a work environment, instant messaging is often free and used widely outside work. Grinter and Palen [62] describe the rapid take-up of IM by American teenagers. Here we see very similar creation of awareness as in Nardi et al.: the teens use the online/offline indicators to know when their friends are available, and know for which friends the information is unreliable. IM is used both for group chat as well as one-to-one interchanges, the one-to-one chats providing a back-channel to the group conversation. IM is used at the same time as the teens carry out their home-work, providing peripheral awareness, and friends and class-mates are brought in to help with the work if necessary, the conversation switching fluently between work and other topics. There are even shades of the same goal to recreate co-located activity: as the teens have gotten older, they have less opportunities to be co-located with their classmates, and they use IM to recreate that communication.

Instant messaging is quickly becoming an integrated part of people's experience with desktop computers. According to a commercial report from 2006 [31], 49% of European Internet users, 64% of Latin American Internet users and 37% of North American Internet users use instant messaging at least once a month. Statistics also point that the numbers are heavily skewed towards the younger end of the population [53]. IM is thus becoming ubiquitous in that it is extremely widely used, as well as in that many users are becoming highly skilled in its use [62]. The tool is disappearing from the view, and the users are focusing on the communication happening within it. The corollary is that the awareness cues provided by IM systems are also becoming accepted and their meaning known.

4.3 Context-aware and mobile social awareness

One of the central ideas in Weiser's "The computer for the 21st century" [133] were mobile devices, the *tabs* and *pads*. These would be personal, carried by the user and would be able to talk to local communication infrastructure, thus allowing the carrier to be identified and located. This gave rapidly birth to the idea of *context-aware* computing, beginning with devices that were aware of their carrier as well as their immediate surround-

ings. The goal of context-awareness: computers that react intelligently to the user's situation without explicit interaction, is also tightly linked to Weiser's idea of the "disappearing computer".

The most often used definition of context comes from Dey and Abowd [39]:

> Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.

Should we here change "and an application" to "and another person", we would have something very close to the definition of "social awareness information". I will return in more detail to the similarity and difference of views on context held by the field of context-awareness and the field of CSCW after discussing some context-aware social awareness systems.

The first of Weiser's tabs, Active Badges [130] and pads, ParcTabs [131] were already used to locate people by co-workers, but very little of their use in building awareness was ever reported. The `locations` [120] system was built do display users on a map, but no user experiences were described. The use of contextual information to build awareness seems to have been more accidental than planned, and easily explained by the close link between the definition of context-awareness and the goals of social awareness. Representations of contextual data are inevitable by-products of designing and implementing context-aware systems, so their possibilities are noticed fairly easily, and simple applications are quickly built.

McCarthy and Meidel [91] were among the first to report on the use location-aware devices for social awareness. They describe ActiveMap, a mapped representation of where co-workers are, based on a badge system very similar to Active Badges. The map shows photos of the users overlaid on an office plan. The images are shaded according to how long ago the badge was located, allowing the users to take into account the veridicality of the information. Recent movement was also indicated with a color change, to create an unintrusive notification of changes. The use of the system, however, centered around the locating others when a task required it, rather than opportunistic interaction. The authors feel that there were no significant privacy issues since it was easy not to wear the badge, in comparison to the ambient cameras of media spaces. However, our own experience with prolonged use of ContextContacts[1] indicates that the so-

[1] Unreported internal use of the system at the Helsinki Institute for Information Technology

cial pressure to use such as system can be significant, which has also been found of the original Active Badges [67].

Ranganathan et al.'s article on ConChat [108] and Prinz's on NESSIE [105] are system-oriented descriptions on how different context sensors and inference mechanisms can be used together with instant messaging, physical representations and virtual rooms to create awareness environments that communicate the users' location, activity level, other people nearby, device environment, environmental conditions like temperature, and access to communication tools. These systems are representative of the aims of context-awareness research: the use of physical sensors to infer relevant facts about people's activities. Although this aim is not trivial, there have been indications that at least certain subtasks related to availability are feasible. Fogarty et al.'s [52] show that a limited number of reasonably priced sensors (like a microphone with some signal processing and a switch that indicates use of the office telephone) could be used to make a predictive model of interruptibility that agreed well with subjective judgments of the same. Begole et al. [18] show that availability can be predicted with high confidence from past patterns of communication.

The encouraging results on availability and interruptibility inference were combined in LilSys [17], which produced an estimated availability indicator based on device use, speech detection, a door open/closed sensor and telephone usage. Use of LilSys brought to light three highly salient results for context-aware awareness systems: Firstly, although the there were high statistical correlations between perceived availability and sensor readings, individual differences in behaviour were large. Such individual differences as when a person closes their office door or what kinds of conversations are interruptible are probably known to co-workers, but become quickly obstacles to automatic reasoning. Secondly, the users felt uncomfortable with being represented as "unavailable" automatically, by a computer. "Unavailability" is socially costly, as it is in effect a refusal to collaborate, and people do not want to appear unavailable unless they need to. Thirdly, although the inferences made were often accurate, interruptions did not diminish in number. Instead the availability indicators would make would-be communicators approach people in different modes, probing for a communication channel. Brown and Randell have heavily criticized the automatic inference of availability in favor of providing the necessary cues for people to make inferences themselves [29].

An independent development made possible by the commercial emergence of pads, first hand-held computers (Personal Digital Assistants, PDAs) and later network-enabled mobile phones, are mobile awareness systems.

Systems like Tang et al.'s Awarenex [123] and Isaacs et al.'s Hubbub [74] brought the IM buddy list to PDAs, enabling the use of the system while locally mobile within the workplace. The ActiveCampus Explorer [63] lets students see the location and system usage of their fellows and send them instant messages on a PDA. In their aims and functionality, these systems were not necessarily very different from desktop IM and awareness systems, although creating light-weight, informative and peripherally accessible applications for mobile devices is of course a great interaction design challenge. Reports on user experiences with the systems are sketchy.

Mobile phones, however, are potentially very different from a PDA. The mobile phone is already a real-time communication platform with voice calls and (especially in Europe) one-to-one text messaging. The mobile phone is also already accepted by a very large audience, in stark contrast to Active Badges or even PDAs. And finally, the mobile phone infrastructure is pervasive, which means that there are very few spatial or temporal limits to the use mobile phones (in developed countries).

Schmidt et al.'s Context-Call [9] is tightly bound to the mobile phone as a communications device. Their aim is to improve call success rates, since failed calls thwart the caller's intentions, wasting their time as well as interrupting the callee. This would be accomplished by allowing users to make a visible statement about their current availability that callers can access before making calls, in the manner of "away" lines in IM. Bardram and Hansen's AwarePhone [14] is closer to the more generic idea of social awareness. AwarePhone integrates location, calendar events and manual availability state into a custom smartphone application, aimed at hospital workers. Hospital work is characterized by them as having high local mobility, both scheduled and ad-hoc activities and collaboration between different groups of workers. The AwarePhone is meant to support easily contacting others through the most appropriate media, be it by physically locating them, calling, or leaving a message. Both Context-call and AwarePhone have only been reported in the concept phase with no user experiences from deployed systems.

4.4 ContextContacts

Our work on ContextContacts (Article IV) continues the thread of mobile, context-aware social awareness, exemplified above by Awarenex, Context-call, ConChat and AwarePhone. The application was inspired by the emergence of smartphones: programmable mobile phones (for a brief technological introduction, see Chapter 2 in Article VI). With a smartphone, we

were able to integrate cues about the user's location, calendar, phone usage, other phones nearby, ringing profile and manual availability into the phonebook. The technical steps that make ContextContacts different from previous systems, are thus:

- Running on a device that is already integrated into the users' existing practices. Although the application itself is of course something new, it is less disruptive and more likely to be used than if it requires a new device to be carried around (compared to non-phone based systems, for example Barkhuus and Dourish report real problems with acceptance of PDAs with ActiveCampus purely based on inconvenience [15]). Phones also use a pervasive infrastructure and are already used throughout the daily life. ContextContacts is not limited to specific environments with their specific social situation (again, compared to non-phone based mobile systems or desktop systems).

- Peripheral information and use without additional interaction. The phonebook is something the user already uses on a mobile phone. Augmenting the phonebook means that the users will see the information even if they are not specifically looking for it, allowing opportunate usage (compared to Context-Call or AwarePhone).

- Combination of automatic and manual cues: the system can provide useful information about someone even if they are not motivated to input anything at the moment (compared to Context-Call) but allows the user to augment and manipulate this information (compared to, say, LilSys).

These technical qualities *frame* ContextContacts, but do not define it. There are four defining characteristics that I think are worth discussion: Not only efficiency, Cues instead of inferences, A proxy for companionship and Privacy through self-presentation.

Not only efficiency We started out with the goal of improving the users' ability to choose when and whether to make calls, or whether to use other media, with assumptions about the suitability of automatic inferences to support this, very similar to the aims of the LilSys system [17]. It turned out that this was a very narrow view of how awareness cues may be used. The most interesting aspect of being wrong in this way is that it exposes a deeper analytical flaw. By assuming that a system will only impact the efficiency of existing practices we disallow the potential for new and changed practices introduced by the system. This problem has been present to some extent in social awareness research, as one of the oft-stated goals has been

to re-enable practices of co-located work in non-co-located settings [76], rather than exploring what new kinds of practices it may enable. Article IV gives a detailed account of the different new uses users found for their mobile phones, and how their existing practices changed (especially the teenagers). Our continued field studies and changes to the application were very much in line with the goals of opportunistic interaction expressed by Isaacs [73] and Bly et al. [25] and of creation and maintenance of social relationships that Tollmar [125] describes.

Cues instead of inferences Two extreme approaches can be identified in the work cited in this chapter. The early work on Media Spaces [25] aimed to provide an immediate channel between the users with no machine-interpretation of activity or intention. The LilSys [17] context-aware availability inference system distilled all the data about the user's behaviour into a single variable, "availability", with a symbolic representation. Matthew Chalmers [89] has written that there is a fundamental difference in the way CSCW approaches context and the way context-aware researchers do. CSCW researchers see context as being constructed by living in the interaction, whereas the whole premise of context-awareness is that meaningful interpretations of human activity can be made by machine observation and inference.

Simplistically, ContextContacts belongs in the CSCW camp. Instead of trying to infer availability and interruptibility, we provide *cues* of the situations of the others that the user may interpret, and indeed construct through communication with those others. More realistically, any system that gathers sensor data and creates representations of it is riddled with implicit and explicit interpretations created by the designer, and so is ContextContacts. The idea of constructing context by living it is a design principle. Firstly, we have tried to minimize the amount of interpretation within the system, and secondly, through several iterations of design, we have tried to identify those interpretations that should be removed, improved or made more transparent. The use of cues has an important implication for privacy as well. By letting the users jointly construct the meaning of the cues, we allow for the normal process of co-operative impression management. And by using manipulable cues, the user can exercise control over the impression being given. I will return to this theme in the next chapter.

Chalmers notes that there are also observable social structures and observable human activities. An example of something observable is location, even if the context-awareness research community has lamented the early and continuing use of location as the main contextual variable [113]. Although the meaning of being in a place is not observable as such, people do

not dispute the validity of assigning Cartesian coordinates or even names to the current location of somebody. Interesting but not so externally observable variables include tasks (people multitask constantly), availability (the desire to participate in communication is both negotiable and depends on the content of the communication), interruptibility (the ability to store the current task into long-term memory depends on the skill of the individual in the task, pacing of the work and the interruption [98]) or current social situation (how shared is the situation of 'being in a meeting' for the current presenter, a person dependent on that task and somebody catching up on their e-mail?). This categorisation is of course simplistic: there are many situations where even these variables are codified to an extent to make them observable: the availability of a receptionist at a desk, the interruptibility of a butler, or the task of the air traffic controller. The most important point Chalmers makes is thus not the dichotomy between the two, but the joint use of them to analyse different situations.

A proxy for companionship A repeated finding in awareness studies has been the feeling of companionship. Nardi et al. [94] describe users of the IM system experiencing "awareness moments [that] produced a certain feeling" of not being alone, Dourish and Bly [43] tell of users feeling glad that they were not the only one working during a weekend by seeing somebody else in their office through the low frame-rate video. Similar findings appear in [103, 69, 69, 26]. We similarly found that one of the most evocative uses of ContextContacts was as a *proxy for companionship*: it recreated some of the feeling of being physically close to the other users. Both we and the cited researchers have not dug very deeply into what the users mean when they talk of "not being alone", but it is obvious that this is agreed to on the level of shared everyday language. It seems that purely the knowledge that somebody else is using the same computer system can produce these feelings, even when the other person is not engaging us in any meaningful way. This would seem to be another phenomenon linked to the "emergence of space" [50]: the system becomes a "locale" not only as a way to gather the group and carry out conversations, but also in the sense of co-habitation.

Privacy through self-presentation Although privacy has been a central concern in the work cited in this chapter, there has been a certain limit to how it has been seen. Especially in the work before the 2000's, privacy has been seen mainly as an obstacle for the adoption of the (CSCW) system. The system designers have designed in control and feedback so that the users would accept the proposed system. In the next chapter and in Article V I will describe how the management of impressions and self presentation (cf. Goffman, [79, 58]) can guide the design of awareness systems

in a positive way: by building systems that allow people to present themselves the way they want, and to jointly construct impressions with others of themselves, the others and the groups they participate in, we can create systems that provide more perceived value to the users, systems that are not just acceptable. This line of thought is by no means originated by me, but is present in awareness work by at least Zaner et al. [134], Aoki et al. [12] and Ackerman [2]. What I aim to do is to further that work into concrete and positive guidelines for ubiquitous social awareness systems.

Chapter 5

Privacy research traditions

This chapter gives a review of the current literature on privacy in ubiquitous computing, structured around the different research traditions that touch on privacy. I shall elaborate most on the social psychological basis, as it has been most influential in this work. I also assume that the reader is fairly familiar with the computer science fields, and will only briefly mention some concepts from them. The emerging field of privacy in ubiquitous computing is not discussed separately, instead its current state is discussed through the different research traditions that influence it.

5.1 Law

Data Protection is a fairly mature field, with generally accepted principles within the European Community. The legal basis for European data protection is two-fold: privacy as a human right by the Council of Europe Treaty No 108 / 1981 (ETS 108) "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", and Data protection as a mechanism for establishing the internal market, from directive 95/46/EC. The Council of Europe Treaty covers all of Individual–State, Individual–Organizations and Public spheres, whereas the directive only applies to Individual–Organizations and Public. These two documents share the same five principles. The processor or collector of personal data:

- Must process the data in a lawful and fair manner (ETS 108 Article 5a, 95/46/EC Article 6 1 a)

- Must ensure that the data is accurate and, if appropriate, up-to-date (ETS 108 Article 5d, 95/46/EC Article 6 1 d)

- Must ensure that the data collection is adequate, relevant and not excessive for the *purpose* of the collection (ETS 108 Article 5c, 95/46/EC Article 6 1 c and 9)
- Must inform the subject of the collection and allow access to data collected (ETS 108 Article 8, 95/46/EC Articles 10-12)
- May only process data by informed consent, contractual or legal obligation, for the vital interests of the subject or for legitimate interests of the controller (ETS 108 Section 5 a and b, 95/46/EC Article 8)

A poignant example of how the amplification of human actions in ubiquitous computing clashes with data protection is the case of a parish worker in Sweden [65]. She was organizing a confirmation camp, in which some parents of the participants were also involved. To facilitate the organization, she created a website where she posted the contact details and short profiles of the parents for use by the organizers and participants. She was sued under the Swedish implementation of the data protection directive for unlawful processing of personal data, processing of sensitive data (in one of the profiles she had included the fact the person had broken their leg) and transmission of personal data to countries outside the EC. She was fined by the local court, appealed to the high court and was found guilty but not fined because of the minority of the crime. I argue that this is a clear case of where the amplification exceeded the understanding of the user: she did not realize that by moving information from the parish noticeboard to the Internet, she was actually publishing it (although the complaint against her was made under data protection, it seems that the person raising the issue was miffed by their portrayal at the site, it being public). In this case something that in the user's mind was group communication (Group sphere), was in reality publishing (Public sphere).

The example above highlights a general problem with the current data protection legislation. Although the legislation has been written to be technology-neutral it fails to take into account the change in the organizational *structure* of data processing triggered by ubiquitous computing. For example, the central concepts of 95/46/EC are the subject (a person the data is about) and the controller (the organization controlling the collection and processing of said data). With new service provision infrastructures like sharing of Wireless LANs[1] or peer-to-peer communication infrastructures[2] all the users are both subjects and controllers. The legislation specifies fairly heavy burdens (see [77, p. 107], [37]) on the controller, based on the

[1] `http://www.fon.com/`
[2] `http://www.skype.com/`

1970's idea that anybody with the resources to run data processing operations will surely have the resources to learn about and comply with the legislation.

Langheinrich has taken these principles and applied them to ubiquitous computing, creating seven fundamental principles of privacy-aware ubiquitous systems [78]: Notice (openly declaring what data is being collected), Choice and Consent (real, informed choice), Anonymity and Pseudonymity (when applicable, systems should not identify individuals), Proximity and Locality (ubiquitous systems should reflect real world limitations in both collection and dissemination of data), Adequate Security, Access and Recourse (collection of and access to data should be limited by both access rights and need, violations should be observable and actionable). These principles have been taken as the basis for work in this thesis, and Article V discusses how they can be built upon. Although focusing on the larger spheres, these principles can be seen as pre-requisites for implementing privacy for the Groups sphere as well.

Iachello and Abowd use the general legal principle of *proportionality* [72]. Proportionality is reflected in EC/95/46 [124] in that "data collection is adequate, relevant and not excessive for the purpose of the collection" and that the "processing is necessary for the purposes of the legitimate interests pursued by the controller". Iachello and Abowd generate a three stage "judgment" process from the idea of proportionality for the evaluation of ubiquitous computing application ideas and designs:

Legitimacy —Establish that the application goals would be useful for the intended user population.

Appropriateness —Recommend the best alternative from a variety of technology (and non-technology) solutions.

Adequacy —Even with a given technology solution, there are many parameters that can be adjusted, and each should be examined to justify proper use.

This process is somewhat orthogonal to the ideas presented in this thesis. The main thrust of my research has been in finding ways to reflect established human disclosure patterns in automated disclosure.

5.2 Cryptography and computer security

In the practical work documented in Article II and Article V we have assumed the existence of reasonable encryption methods for keeping commu-

nications secret from third parties. Communications secrecy is a necessary precondition for working privacy management in all spheres, but doesn't address the harder questions on how the user manages *disclosure*: practical control over what they tell to whom. I would concur with Bruce Schneier [48] that we have reached the point in cryptographic research that we have the technical tools for secrecy, but that security in reality is compromised by the user. Since ubiquitous computing tends to increase the number of devices users interact with, and often removes these devices from central administration, the risk of inappropriate key management or misunderstanding security grows.

Within the European Community, the Commission has argued for the development and use of Privacy Enhancing Technologies [30, p. 25] as a means of data protection, focusing on anonymity and pseudonymity [51]. Anonymity and pseudonymity are important solutions for the Individual–Organizations and Public spheres. Within Groups, pseudonymity has some uses when the group is not based on real-world interactions.

Permanent pseudonyms have limited usefulness: Firstly, if the real identity behind the pseudonym is ever leaked, all data is compromised. In ubiquitous computing, the information system is linked to real-world movements and activities, which Beresford and Stajano have shown to trivially leak real identities [21]. Secondly, publicly used pseudonyms become repositories of status and reputation as much as 'real' identities. More interesting is the use of transient, short-term pseudonyms; but any system that can use pseudonyms instead of real identities should do so, as it still adds a layer of protection (for example the German data protection legislation mandates anonymity or pseudonymity whenever possible).

Bessler and Jorns [24] describe a system for service composition using transient pseudonyms. In their system, two (or more) users who know each others' real identities want to share location information. The location information is provided by a third-party service, and is made pseudonymous. A trusted identity server provides mappings between identities and transient pseudonyms, so that the users can map the pseudonymous location information to each other. This is quite a typical set-up for pseudonymity [8, 21].

The work in Article V uses long-term pseudonyms to provide the presence service. The users of the system are assumed to know the real-world identities linked to the pseudonyms. In the current implementation, however, the service provider does not have to know the contents of the presence data, so it can be encrypted while in transit and only decrypted on the receiver's device. The data is produced fully on the user's own device, and

the service only acts as a transmission channel (there are of course traffic analysis attacks, but they are probably not a realistic threat). Should we want to intelligently produce or combine data in the server, transient pseudonyms should be applicable.

Even anonymous services may obtain personal data if they are location-based: the anonymous location the service receives may identify a person (the trivial case would be position information so accurate that only one person can physically occupy the given co-ordinates). Adding noise to the location information, often called *cloaking*, has been proposed to combat this problem [64, 20, 45]. The addition of noise takes into account identifiability: enough noise is added so that the single user can not be identified (the disclosed area will include multiple users). This kind of location cloaking is problematic to the user, since with automatic addition of noise it may be difficult to predict what the system is disclosing and to understand how the system works.

Models and protocols for access control have been a central topic in computer security [111, 128]. Any privacy-sensitive system will have to include access controls, but the idea that the user's desire and willingness to disclose private facts can be adequately captured by static preferences has been severely criticized. Leysia Palen's study of shared calendars at Sun and Microsoft showed that most users kept the system's default settings although at Sun they were set to share the full calendar and at Microsoft only free/busy information [101]. Spiekermann and Grossklags noticed that users in a realistic online setting were willing to disclose a large amount of private information for very small discounts or no visible gains whatsoever, although they had a-priori expressed concerns about disclosure online [118]. Adams [5], Lederer et al. [80], and Consolvo et al. [32] argue that not only is disclosure dependent on whom information is disclosed to, it is also dependent on the discloser's dynamic situation and what they perceive the recipient's informational need to be. This dynamic nature of disclosure control is elaborated upon in the following sections on social psychology, and Article V describes how a social awareness system may support such dynamic control.

5.3 Social Psychology

The main thrust of our research group's experimental studies [100, 99] has been the development of ContextContacts, a ubiquitous social awareness service: a service aimed at letting users easily disclose their location, availability and activities to their communication partners. Thus the most cen-

tral sphere of privacy for us has been Groups, and the most influential research tradition social psychology. The following describes the most salient social psychological theories and findings as comes to privacy, self-disclosure and self-presentation, as well as their relationship to privacy research in ubiquitous computing.

5.3.1 Boundary negotiation

Leysia Palen and Paul Dourish [102] have been applying Altman's privacy theory [10] to the design of ubiquitous computing systems. Rather than repeat the full argumentation, I pick some of the most salient factors here. Altman describes privacy as the ongoing negotiation of the self–environment boundary. There are several kinds of such boundaries, corresponding to the spheres of privacy discussed in this thesis. I will focus on the Groups sphere.

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 and impression management. Privacy being "negotiated", the limits of disclosure are not dictated by either the discloser or the environment, but are 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 politeness.

Participants in such negotiations often engage in *face-work*. Goffman [57] 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 Aoki and Woodruff [12] (among others [70, 94]) 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.

Altman's theory is seen as a valid base for current social psychological research, and to have been verified experimentally [88]. It has been later extended by Petronio [104]: she has shown that even though disclosure is dynamic, it is mostly based on a set of practical rules, which are followed most of the time. These rules themselves can be individually negotiated,

for example between spouses, but are also shared in groups like families. Following the established rules can be seen as face-work: they are not supposed to lead to embarrassing situations, the rules define what is considered tactful.

The actual rules and norms of disclosure and tact constructed by any real group of users, be they families, friends or workers cannot be—at least not fully—predicted by the system designer. A good example of this is the varying social acceptance of rejecting calls (several participants in our field-studies have related that expressing unavailability by explicitly rejecting the incoming call has become a valid communication mechanism with some of their peers, while being as unacceptable as hanging up for some). So since the social implications of things like disconnection are not known, the designer should leave room for multiple mechanisms and interpretations, for both obvious refusals and masking of reality.

5.3.2 Self-disclosure

The revelation of private matters to others has been called *self-disclosure* [22]. 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 [127]. Self-disclosure is generally assumed to be strongly reciprocal [22, 127]: there is a strong correlation between how much different sides of social relationships disclose.

The self-disclosure studies have, however, focused on equal status relationships (friends, spouses, dating) [92, p. 440]. There is no indication that the theory of self-disclosure applies to unequal relationships, such as parent–child or boss–worker. Of course power inequality is not a black-and-white matter, most social groups will have some power structure. Although traditional work in self-disclosure has been in relation to facts disclosed through actions, I assume that the framework can be applied to automated disclosure as well, as long as there are aspects in the automated system which imply voluntary disclosure and allow the participants to control how they appear through the system. One way to control appearance is of course communication *outside* the automated system: the information in the system can be framed and manipulated by non-automated actions: face-to-face conversations, messages and calls.

5.3.3 Impression management

Self-disclosure can be seen as a part of the larger frame of *self-presentation*: the ongoing process of impression management [79]. People engage in self-presentation continuously. By disclosing certain facts instead of others, by drawing attention to actions, by their appearance and sometimes by outright deception they 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 the strategies involved.

One way to avoid disclosure, to save face of the self or others, or to avoid unwanted intrusions or obligations is lying: from white lies ("I'm just on my way") to outright lies ("I did not have sexual relations with that woman"). DePaulo et al. [38] show that in their study adults told 1–2 untruths a day that they consciously recognized as lies. Many of these lies were made to foster certain expressions of the lier. Although they show that interactions where you lie are more distressful, they also show that many small lies are routine-like and do not affect the lier.

Computer systems have often been designed with the idea that reality can be sensed and described objectively, an excellent example being the unwillingness of the GEOPRIV working group to allow users to modify their location information, since it would mean endorsing lying—unfitting for a professional society, such as the IETF [56]. The reality of human acts is often *socially constructed* (see for example Berger and Luckman [23]). A good example is a person's location. "Leaving work" may take tens of minute, but communicating the intention and starting the necessary preparations can make it so for somebody waiting for you. My current address may have very little meaning, but to say I'm in the city's best restaurant (maybe even if I'm not) gives off a certain impression. In these 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 [58, p. 222–227] that the audience is quite willing to disregard untruths to maintain a jointly agreed-to situation.

5.3.4 Entangled in other practices and concerns

Self-disclosure and self-presentation in human discourse are tangled with other concerns [11]. This makes experiments with privacy hard to analyze. For example, Consolvo et al. [32] argue that people apply highly dynamic control in mediated location disclosure. We agree with their factual findings, but disagree about their analysis of the motivation. They use experience-sampling to probe users' willingness to share their current location with their peers in real-life situations. They show that although the most important factor in disclosure is the identity of the asker or observer, there are no static rules that can decide what is revealed but that is instead completely situation-dependent.

It is not, however, necessary to see situationally dependent tuning of disclosure only as *control*: it is a well-known theorem of human-human communication (Grice's maxims [61], [112]) 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. For example, 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".

Conversation analysts have also noted that people tend to rather give a bit higher-level descriptions of their doings, because less accurate updating is then expected for. For example, telling that you are in your office sitting in your chair implies more pressure to tell when this position changes [112]. Automatic disclosure does not have to obey the same rules, as users will not ascribe all human qualities to a computer system: they will not assume that the system answers with only the necessary information, and the system may give a higher frequency of updates than a human.

5.4 Notes on some other related fields

The previous sections describe the development of privacy within ubiquitous computing from the point of view of this thesis and what I have found useful in the work. There are some related fields that should be mentioned, even though they have not been as influential in this work. They have often influenced the papers referenced above.

- The definition, justification and implications of privacy have been a topic of study within philosophy for a long time. Adam Westin's work [13] has been very influential for the development of legal guidelines. For an introduction, see Judith DeCew's "In Pursuit of Privacy" [36], and for a modern overview, Number 2, 2000 of Social Philosophy and Policy [47]. Langheinrich provides a brief description of how philosophical concepts of privacy relate to ubiquitous computing in [78].

- Computational modeling of trust has become an active area of research in the past fifteen years. Lea Viljanen provides a unified view of current attempts to model trust in [126]. Trust models as a basis for security and privacy in ubiquitous computing have been described for example in [75, 114].

- Secure multi-party computation: It has been shown that any efficiently computable function with n inputs can also be efficiently computed by n participants, each providing one of the inputs, and everyone learning only the output [44]. This can be used to gain the advantages of sharing data, for example to generate recommendations, without revealing private data.

- Economics and game theory. Jens Grossklags [118, 4] has been studying people's economical behaviour in relation to privacy. He has summed his findings as "Traditional theory suggests consumers should be able to manage their privacy. Yet, empirical and theoretical research suggests that consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term benefits."

Chapter 6

Contributions of this thesis

The articles in this thesis describe a process of exploring privacy issues, rather than ready-made answers to questions on how systems should be constructed. New tools and methods were developed during the exploration, which are generally applicable to the study of human-computer interaction and human behaviour in general. Some tentative answers to the question on mechanisms and design guidelines are given within a limited application field. The research questions the thesis was set out to answer were:

1 How can we study real-world privacy issues in ubiquitous computing? What tools and methods do we need?

2 What kind of mechanisms should ubiquitous social awareness systems provide to the user, so that they can carry out impression management?

6.1 The articles

Article I describes an adaptive, on-line algorithm for extracting location features (important places and routes between them) from GSM cell data. Cell data is sequential data describing which base station a mobile phone is currently communicating with. Cells vary in size from some hundreds of meters to some kilometers in diameter, are irregularly shaped (with holes caused by radio propagation shadows from buildings and land-forms) and always overlap; but the information is available on the mobile device without extra hardware or infrastructure support. The article shows how meaningful, smoothed features can be extracted from such sequences with an algorithm that can be run on the mobile device itself. These features have been used in the ContectContacts (Article IV), and have been crucial to its

development. Thus the algorithm is both an answer to the second research question as well as a part of the practical answer to the first.

The privacy implications of this algorithm is that the user does not have to communicate the original data to any outside party to extract the features nor disclose the derived location to service providers, thus removing the need to consider the Individual–Organizations sphere. Location systems with these features have been proposed for specialized devices (e.g., PARCTAB location agents [119]), but our algorithm works on off-the-shelf devices operating within widely deployed infrastructure. Commercially available location systems for GSM networks have supposed that the location information is generated by the operator (the Organization) and distributed to service providers or other users by that operator, which is much more open to abuse than a system running on the user's own device (see for example Ben Goldacre's "How I stalked my girlfriend" [59])[1]. The only other widely available alternative to GSM locationing is GPS, but it suffers from poor coverage in cities and battery consumption that is unacceptable for continuously running mobile applications.

Article II describes the ContextPhone platform for developing mobile context-aware applications running on Nokia's S60 smartphones. The smartphone is the first platform for pervasive computing [1] available for long-term, outside-the-laboratory studies. The platform we developed has been made publicly available under an open-source license, and this article describes its functionality and uses. The platform includes a number of software sensors, including location, user activity, communications and phone internal state. The data from the sensors is made available through a uniform blackboard architecture (under development when the article went to press, but now available). A number of Internet-standard communication protocols are included in the platform, as well as three major example applications.

ContextPhone supports the general goal of real-world studies of ubiquitous systems, expressed as the first research question of this thesis. It also specifically supports experimenting with different awareness cues. Previous studies in social awareness indicate that different cues give very different possibilities for the use of the system [125, 42, 43]. Thus what sensors and representations are used in a system, play a large role in defining the kinds of use as well as patterns of use, the expectations users have of each others' use of the system, and the perceived value of the system. On the other

[1]We have also heard from several commercial service providers that building of location-aware systems has been hindered greatly by the need to have a separate contractual relationship between the application provider and the consumer.

hand, different cues are perceived a-priori to have different privacy implications, for example location and the granularity of location [14, 56, 32, 67]. These two factors justify the claim in the article, that experimental studies of privacy in ubiquitous computing are facilitated by a platform that provides flexible configuration of sensors, reasoning and representations.

ContextPhone has been the major vehicle for our studies of privacy issues in the Groups sphere: it provides both the application through which privacy issues can be revealed as well as the data gathering mechanism for learning about the issues, thus giving a partial, practical answer to the first research question. It is the technological basis for Article IV and Article V.

Article III is based on an experimental study on data controllers' compliance with the Finnish implementation of the EC data protection directive [124], specifically as it comes to the subjects right to be informed and to access to the data. It had been thought before that compliance might be low, and my own experience with working in the industry also suggested that typical information systems do not help organizations in complying with the regulations. There existed, however, no studies testing this experimentally. The study explores the Individual–Organizations sphere.

The results of the experiment show that while the public sector in general is able to both inform and to give access to data to the subject, the private sector, including listed companies, is not. For example, only 16% of non-profit organizations and companies provided complete data from the subject access request. The responses that I did receive further indicate that the information systems in use in the organizations did not support the subject access, but that the required data had been manually extracted via different reporting mechanisms. This link between the technical properties of the system and ability to comply with Data protection give direct guidance for systems design, as an answer to the second research question. These results are most likely directly applicable to commercial ubiquitous computing systems as well. The same economic realities are in force: there is no market force that pushes adoption of Data protection compliant information systems for ubiquitous computing any more than there is for more traditional systems.

Article IV describes in detail how several groups of users have used the ContextContacts ubiquitous social awareness service. It shows that the cues provided of the others in the system served three main uses: First, the system is used in the coordination of mobility and communication, typically between two users. The cues also facilitate various ad hoc opportunities and informal encounters. Second, when a user-controlled text field was introduced as an additional cue, the use of the system evolved from coor-

dination toward discussion, chatting, and expressions of emotions. The use of automatic cues evolved in parallel, emphasizing those cues that support availability and the presence inferences needed in the coordination of conversations. Third, the cues support companionship among group members: feelings of mediated connectedness, closeness, and communality.

This article serves the thesis in three ways. It gives a basic existence proof of positive effects from automatic distribution of highly personal data, motivating the line of research (otherwise we could always take the safe road of not building such systems). Secondly, it gives the background for Article V, allowing the claims specific to privacy in it to be judged in light of the actual use of the system. And finally, it already provides some answers to the question of how such systems should be constructed, which are further developed in Article V.

Article V is the most developed answer to the question of "What kind of mechanisms should ubiquitous social awareness systems provide to the user, so that they can carry out impression management?" we have been able to provide so far. It is based on two years of field studies with five long-term (over 6 weeks) studies with different groups of users. The results from the field studies are integrated with existing findings in ubiquitous computing as well as social psychology to provide a number of design guidelines. These guidelines are tested by applying them to the ContextContacts application, and thus deriving a design specification for its next version.

One of the major findings from our field studies was that the users were almost universally unconcerned with automated sensing and disclosure of location, phone usage, physical environment and availability. They did, however, when possible manipulate and re-frame the automatically sensed information by renaming profiles and places and commenting on their own activities as well as the activities of others. The guidelines we derived include supporting light-weight access controls, assuming reciprocity, making it possible to appear differently to different audiences, allowing commenting and manipulation of automatically sensed data as well as providing mechanisms for lying. The major limitations in these claims comes from the fact that our field studies have been almost solely with groups where the users only had to appear in one role in the system. The design guidelines and the new features of ContextContacts will have to be verified in settings where there are multiple, overlapping groups using the system.

Article VI is aimed at the social sciences audience. In it we draw together methodological advances in the study of human behaviour made possible by the smartphone technology. The general possibilities of smartphones and ContextPhone are explained in enough detail to allow the reader

to evaluate the suitability of the methods, and the discussion is concretized by describing three major field studies done using smartphones. Two of the field studies have been carried out by the authors, and one is a review of an external study.

The major benefits from using smartphones to study human behaviour stem from two qualities: Firstly, the smartphone is capable of automatically observing and logging behavioural data, including physical encounters between people. Secondly, the smartphone is from the user's point of view just a mobile phone, which is accepted as an unintrusive and normal part of most westerners' life. These combine to make it possible to observe variables previously only available via self-reports, which are known to have granularity, accuracy and reliability problems. The limitations of using smartphones for behavioural study include the lack of verified analysis methods for the data thus gathered.

Although we present Smartphones as a generic tool for social scientific research, there is no reason to assume that it would not be equally suitable for specifically privacy-related research. Thus it provides a methodological answer to the first research question.

6.2 Answers to research questions

This section summarizes purely the novel contributions of this thesis, in relation to the stated research questions.

1 *How can we study real-world privacy issues in ubiquitous computing?*

The answer to this question is not a result from a study, it is a set of tools and methods for studies. ContextPhone provides a ready-made platform for research into how ubiquitous services are used, although it still requires non-trivial effort to build new applications. To the extent ubiquitous computing gathers data about human behaviour, it can also be used to *study* human behaviour. The "invisibility" can be used to gather data less influenced by observation, and the automated collection of behavioural data allows the researcher to access to data from longer periods of time and for larger populations than previously feasible. Our experiences with such studies have been reported in detail so that the methods can be applied by others. (The algorithms and software described in Article I and Article II give concrete tools for practitioners; Article III, Article VI describe novel or under-used methods)

2 *What kind of mechanisms should ubiquitous social awareness systems provide to the user?*

An information system that handles private data should provide explicit support for fair information processing: they should be able to distinguish between personal data and other data, provide reporting facilities for subject access requests and allow, if not require, expiration of personal data. Otherwise organizations, especially small organizations, have trouble complying with legislative requirements and thus basic guarantees of privacy. (Article III provides a quantitative criticism of the current state of information systems and organizational practices with suggestions on improvements).

The fair information processing guidelines are a necessary but not sufficient condition for successful impression management: control over what is disclosed to whom and when is needed for the user to feel that they are in control, but is rarely used as-such. We have found that automated disclosure is found acceptable and useful, and can become a part of impression management if augmented with the ability to comment on and manipulate the automatically gathered information, at least with certain groups of users. Commenting and activity cues allow disclosers to get feedback on how others perceive them. We propose that users are willing to address such comments and manipulations to different reference groups separately, but do not have conclusive empirical support for the claim. (Article V)

Chapter 7

Outlook

This thesis does not provide general and conclusive answers on how to construct ubiquitous computing systems so that they support privacy management. What it does provide is a set of guidelines on privacy management for social awareness services that I feel are practical and useful, as well as being based on solid empirical work. The findings will serve as the basis for commercializing the proposed social awareness service ContextContacts[1].

The tools, methods and data described in this thesis are a major contribution to work in this area, and have already been proven useful to others in related fields [46, 35, 110, 90, 28]. The methods should have a contribution to make in sociological and social psychological studies as well, and I hope that Article VI will reach researchers in these fields. The validity and reliability of smartphones as tools for gathering real-world data on dynamic social networks, movements, activities and interaction is yet poorly understood. Carrying out experiments where the reliability and validity can be robustly estimated would greatly aid in the use of these tools. Since such data has not been practically available previously, analysis of the data is also still in its infancy.

Article III shows there is cause to concern with the private sector's compliance with EC Data protection regulation. It also provides strong arguments that this concern is linked to the information systems in use, and some concrete proposals for improving the situation. In the case of traditional information systems, the improvements are somewhat straightforward: comprehensive tagging of personal data, reporting functionality and special purging and access rules for the data. I would claim that if we are incapable of providing privacy-aware traditional information systems, we will have serious trouble doing that within ubiquitous computing. The

[1] `http://www.jaiku.com`

article is based on a limited sample, only studying those controllers who hold information about me. As stated in the article, the same experiment should be repeated with a larger number of controllers—meaning recruiting several people to request access to their data and information on processing.

We have found that at least certain groups of users not only can cope with automated disclosure in a social awareness application, but find it useful and *fun* (Article IV): it provides topicalization for discussions, a pretext for communication and a proxy for companionship, helping users establish and deepen relationships. Although such feelings of companionship have been reported by others as well [43, 94] neither we nor the others have dug into what the users mean when they talk about "closeness" and "not feeling alone". This re-creation of feelings of physical proximity and connectedness from very thin cues should prove an interesting topic of further study.

By commenting and manipulating the automatically disclosed information users can carry out impression management (Article V). By looking at how people use technological systems to manipulate and construct impressions, we get *positive* guidelines for privacy-respecting design, rather than building systems that just avoid the pitfalls. We have not yet carried out a field study where the same system would be used with several reference groups at the same time. Whether users can cope with automated disclosure in such a situation, and what kinds of features they need from the system to do that is a crucial future research topic.

There are two possible enabling, one could even say *empowering*, shifts in how we handle personal data in ubiquitous computing. The first is the ability for the users to keep the data: instead of relying on a service provider to do something useful with their data, they in principle provide the service themselves—sidestepping the Individual–Organization sphere. This approach is reflected in Article I, which shows how a device can be made aware of its location with no location-oriented service infrastructure, and the ContextContacts application discussed in Article V and Article II, in which the users disclose their location from their own personal devices, rather than from a third-party service. This shift alleviates concerns over legal and factual control as well as transparency: the user can be made aware exactly of what data is disclosed to outsiders, as it all originates from their personal device. The enabler of this shift is the emergence of personal, always-on networked computing devices, replacing "ambient" intelligence.

The second shift is not technologically driven (although it, too, requires technological support), but more a change in the way the data is seen by a service provider, the Individual–Organization sphere. The EC data protection directive already stipulates that the subject must have access

to data about themselves, but only in principle at a rate of once-a-year, and only in a human-readable format. If instead the service provider would allow the subject—the user—continuous real-time access to their own data, the user could use it with other services. For example, a smart-card based payment system for public traffic would be able to provide the traveler partial traces of their movements, enabling them to tag media they create with their location. If both the controller and the subject can use the data, its potential value can increase—and this increase in utility can of course be split between the two. There are indications that this kind of shift may happen, for example some banks already allow individual users to download their itemized credit card bills as spreadsheets, and Flickr[2] allows anybody, including users themselves, to build new applications on top of the photos people upload. This shift is also a defining factor in our efforts to commercialize ContextContacts.

[2] `http://www.flickr.com/`

References

[1] Gregory D. Abowd, Liviu Iftode, and Helena Mitchell. Guest Editors' Introduction: The Smart Phone–A First Platform for Pervasive Computing. *IEEE Pervasive Computing*, 04(2):18–19, 2005.

[2] Mark S. Ackerman. The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility. *Human-Computer Interaction*, 15(2&3):179–203, 2000.

[3] Mark S. Ackerman and Brian Starr. Social activity indicators: interface components for CSCW systems. In *UIST '95: Proceedings of the 8th annual ACM symposium on User interface and software technology*, pages 159–168, New York, NY, USA, 1995. ACM Press.

[4] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26–33, January/February 2005.

[5] Anne Adams. Multimedia information changes the whole privacy ballgame. In *CFP '00: Proceedings of the tenth conference on Computers, freedom and privacy*, pages 25–32, New York, NY, USA, 2000. ACM Press.

[6] Dakshi Agrawal and Charu C. Aggarwal. On the design and quantification of privacy preserving data mining algorithms. In *PODS '01: Proceedings of the twentieth ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, pages 247–255, New York, NY, USA, 2001. ACM Press.

[7] Rakesh Agrawal and Ramakrishnan Srikant. Privacy-preserving data mining. *SIGMOD Rec.*, 29(2):439–450, 2000.

[8] J. Al-Muhtadi, A. Ranganathan, R. Campbell, and M. D. Mickunas. Flexible, privacy-preserving authentication framework for ubiquitous

computing environments. In *Distributed Computing Systems Workshops, 2002. Proceedings. 22nd International Conference on*, pages 771–776. IEEE, 2002.

[9] Albrecht Schmidt, Antti Takaluoma, and Jani Mäntyjärvi. Context-Aware Telephony Over WAP. *Personal Technologies*, 4:225–229, 2000.

[10] I. Altman, A. Vinsel, and B.B. Brown. Dialectic conceptions in social psychology: an application to social penetration and privacy regulation. *Advances in Experimental Social Psychology*, 14:108–161, 1981.

[11] Charles Antaki, Rebecca Barnes, and Ivan Leudar. Self-disclosure as a situated interactional practice. *British Journal of Social Psychology*, 44:181–199, 2005.

[12] Paul M. Aoki and Allison Woodruff. 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*, pages 181–190, New York, NY, USA, 2005. ACM Press.

[13] Michael A. Baker and Alan F. Westin. *Databanks in a Free Society: Computers, Record-keeping, and Privacy.* Quadrangle Books, New York, 1972.

[14] J.E. Bardram and T.R. Hansen. The AWARE architecture: supporting context-mediated social awareness in mobile cooperation. In *Proceedings of the CSCW03*, pages 192–201, New York, NY, 2003. ACM Press.

[15] Louise Barkhuus and Paul Dourish. Everyday Encounters with Context-Aware Computing in a Campus Environment. In *Proceedings of the Sixth International Conference on Ubiquitous Computing (UBICOMP'04)*, Lecture Notes in Computer Science, pages 232–250, Berlin / Heidelberg, 2004. Springer.

[16] Philip Barnard, Jon May, and Daniel Salber. Deixis and points of view in media spaces: an empirical gesture. *Behaviour & Information Technology*, 15(1):37–50, January 1996.

[17] James "Bo" Begole, Nicholas E. Matsakis, and John C. Tang. Lilsys: Sensing unavailability. In *CSCW '04: Proceedings of the 2004 ACM conference on Computer supported cooperative work*, pages 511–514, New York, NY, USA, 2004. ACM Press.

[18] James "Bo" Begole, John C. Tang, and Rosco Hill. Rhythm modeling, visualizations and applications. In *UIST '03: Proceedings of the 16th annual ACM symposium on User interface software and technology*, pages 11–20, New York, NY, USA, 2003. ACM Press.

[19] V. Bellotti and A. Sellen. Design for Privacy in Ubiquitous Computing Environments. In *Proceedings of the Third European Conference on Computer Supported Cooperative Work (ECSCW'93)*, pages 77–92. Kluwer, 1993.

[20] A. R. Beresford and F. Stajano. Mix zones: user privacy in location-aware services. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004*, pages 127–131. IEEE, 2004.

[21] Alastair R. Beresford and Frank Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing* , 2:46–55, 2003.

[22] John H. Berg and Valerian J. Derlega. Themes in study of self-disclosure. In Valerian J. Derlega and John H. Berg, editors, *Self-Disclosure. Theory, Research and Therapy*, pages 1–8, New York, 1987. Plenum Press.

[23] Peter L. Berger and Thomas Luckman. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. Garden City, New York, NY, 1966.

[24] S. Bessler and O. Jorns. A privacy enhanced service architecture for mobile users. In *Third IEEE International Conference on Pervasive Computing and Communications Workshops, 2005. PerCom 2005 Workshops*, pages 125–129. IEEE, 2005.

[25] Sara A. Bly, Steve R. Harrison, and Susan Irwin. Media spaces: bringing people together in a video, audio, and computing environment. *Commun. ACM*, 36(1):28–46, 1993.

[26] Cristian Bogdan and Kerstin Severinson Eklundh. Fingerprint: supporting social awareness in a translucent sensor-mediated cue-based environment. In *CHI '04: CHI '04 extended abstracts on Human factors in computing systems*, pages 1263–1266, New York, NY, USA, 2004. ACM Press.

[27] Michael Boyle, Christopher Edwards, and Saul Greenberg. The effects of filtered video on awareness and privacy. In *CSCW '00: Proceedings*

of the 2000 ACM conference on Computer supported cooperative work, pages 1–10, New York, NY, USA, 2000. ACM Press.

[28] Robert Bridle and Eric McCreath. Inducing shortcuts on a mobile phone interface. In *IUI '06: Proceedings of the 11th international conference on Intelligent user interfaces*, pages 327–329, New York, NY, USA, 2006. ACM Press.

[29] Barry Brown and Rebecca Randell. Building a context sensitive telephone: Some hopes and pitfalls for context sensitive computing. *Computer Supported Cooperative Work*, 13(3-4):329–345, 2004.

[30] Commission of the Europena Communities. First report on the implementation of the data protection directive (95/46/ec). COM(2003) 265 final, 2003.

[31] comScore. Europe Surpasses North America In Instant Messenger Users, comScore Study Reveals. Online, `http://www.comscore.com/press/release.asp?press=800`, 2006.

[32] Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. Location disclosure to social relations: why, when, & what people want to share. In *CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 81–90, New York, NY, USA, 2005. ACM Press.

[33] Richard L. Daft and Robert H. Lengel. Organizational information requirements, media richness and structural design. *Management science*, 32:554–571, 1986.

[34] Nigel Davies and Hans-Werner Gellersen. Beyond prototypes: Challenges in deploying ubiquitous systems. *Pervasive Computing*, 1:26–35, 2002.

[35] Marc Davis, Nancy Van House, Jeffrey Towle, Simon King, Shane Ahern, Carrie Burgener, Dan Perkel, Megan Finn, Vijay Viswanathan, and Matthew Rothenberg. MMM2: mobile media metadata for media sharing. In *CHI '05: CHI '05 extended abstracts on Human factors in computing systems*, pages 1335–1338, New York, NY, USA, 2005. ACM Press.

[36] Judith Wagner DeCew. *In Pursuit of Privacy. Law, Ethics and the Rise of Technology*. Cornell University Press, New York, USA, 1997.

[37] Department for Constitutional Affairs. Response to the Consultation Paper, Data Protection Act 1998: Subject Access. Online, `http://www.dca.gov.uk/consult/foi/dpsaresp.htm`, July 2003.

[38] Bella M. DePaulo, Deborah A. Kashy, Susan E. Kirkendol, and Melissa M. Wyer. Lying in Everyday Life. *Journal of Personality and Social Psychology*, 70(5):979–995, 1996.

[39] Anind K. Dey and Gregory D. Abowd. Towards a better understanding of context and context-awareness. Technical Report GIT-GVU-99-22, College of Computing, Georgia Institute of Technology, 1999.

[40] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[41] Paul Dourish. Culture and Control in a Media Space. In Giorgio de Michelis and Carla Simone, editors, *European Conference on Computer-Supported Cooperative Work*, pages 133–146, Dordecht, Boston, London, 1993. Kluwer Academic Publishers.

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

[43] Paul Dourish and Sara Bly. Portholes: supporting awareness in a distributed work group. In *CHI '92: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 541–547, New York, NY, USA, 1992. ACM Press.

[44] Wenliang Du and Mikhail J. Atallah. Secure multi-party computation problems and their applications: a review and open problems. In *NSPW '01: Proceedings of the 2001 workshop on New security paradigms*, pages 13–22, New York, NY, USA, 2001. ACM Press.

[45] Matt Duckham and Lars Kulik. A Formal Model of Obfuscation and Negotiation for Location Privacy. In Hans W. Gellersen, Roy Want, and Albrecht Schmidt, editors, *Third International Conference, PERVASIVE 2005, Munich, Germany, May 8-13, 2005. Proceedings*, number 3468 in Lecture Notes in Computer Science, pages 152–170. Springer-Verlag, 2005.

[46] Nathan Eagle. *Machine Perception and Learning of Complex Social Systems*. PhD thesis, Program in Media Arts and Sciences, Massachusetts Institute of Technology, 2005.

[47] Ellen Frankel Paul (Ed.). The right to privacy. *Social Philosophy and Policy*, 17(2), 2000.

[48] C. Ellison and B. Schneier. Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure. *Computer Security Journal*, 16:1–7, 2000.

[49] Thomas Erickson and Wendy A. Kellogg. Social translucence: an approach to designing systems that support social processes. *ACM Trans. Comput.-Hum. Interact.*, 7(1):59–83, 2000.

[50] Thomas Erickson, David N. Smith, Wendy A. Kellogg, Mark Laff, John T. Richards, and Erin Bradner. Socially translucent systems: social proxies, persistent conversation, and the design of "babble". In *CHI '99: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 72–79, New York, NY, USA, 1999. ACM Press.

[51] European Commission Internal Market DG. Terms of reference of the technical workshop on privacy-enhancing technologies organised by dg internal market on the 4th of july in brussels. Online, `http://europa.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/pet/200304-pet-tor_en.pdf`, 2003.

[52] James Fogarty, Scott E. Hudson, Christopher G. Atkeson, Daniel Avrahami, Jodi Forlizzi, Sara Kiesler, Johnny C. Lee, and Jie Yang. Predicting human interruptibility with sensors. *ACM Trans. Comput.-Hum. Interact.*, 12(1):119–146, 2005.

[53] Susannah Fox and Mary Madden. Generations Online. Online, `http://www.pewinternet.org/pdfs/PIP_Generations_Memo.pdf`, 2006.

[54] Ludwin Fuchs, Uta Pankoke-Babatz, and Wolfgang Prinz. Supporting Cooperative Awareness with Local Event Mechanisms: The GroupDesk System. In *Proceedings of ECSCW'95*, pages 247–262. Kluwer Academic Publishers, 1995.

[55] William W. Gaver. The affordances of media spaces for collaboration. In *CSCW '92: Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 17–24, New York, NY, USA, 1992. ACM Press.

[56] GEOPRIV Working Group Archives. Georpiv and actively lying, 2003. Mailing list exchange, Online, `http://ecotroph.net/`

~anewton/hypermail/geopriv/0309/0846.html, referenced Jun 2006.

[57] Erving Goffman. *Interaction Ritual*, chapter On Face-Work, pages 5–45. Pantheon Books, New York, 1967.

[58] Erving Goffman. *The Presentation of Self in Everyday Life*. Penguin Books, London, UK, 1990. Reprinted, original 1959 Anchor Books.

[59] Ben Goldacre. How I stalked my girlfriend. *The Guardian*, (Wednesday Feb 1st), 2006.

[60] Adam Greenfield. *Everyware: The Dawning Age of Ubiquitous Computing*. New Riders Publishing, Indianapolis, IN, 2006.

[61] H. Grice. Logic and conversation. In P. Cole and J. L. Morgan, editors, *Syntax and semantics*, volume 3 Speech Acts, pages 43–58, New York, 1975. Academic Press.

[62] Rebecca E. Grinter and Leysia Palen. Instant messaging in teen life. In *CSCW '02: Proceedings of the 2002 ACM conference on Computer supported cooperative work*, pages 21–30, New York, NY, USA, 2002. ACM Press.

[63] W.G. Griswold, P. Shanahan, S.W. Brown, R. Boyer, M. Ratto, R.B. Shapiro, and T.M. Truong. ActiveCampus: experiments in community-oriented ubiquitous computing. *Computer*, 37:73–81, October 2004.

[64] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *MobiSys '03: Proceedings of the 1st international conference on Mobile systems, applications and services*, pages 31–42, New York, NY, USA, 2003. ACM Press.

[65] Göta Hovrätt. Bodil Lindqvist mot Åklagarkammaren i Jönköping. Mål nr. B 747-00, 2004.

[66] R. R. Harper and J. A. Hughes ad D. Z. Shapiro. Working in harmony: An examination of computer technology in air traffic control. In *Proceedings of the First European Conference on Computer-Supported Cooperative Work*, pages 73–86, 1989.

[67] Richard H. R. Harper. Looking at ourselves: an examination of the social organisation of two research laboratories. In *CSCW '92: Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 330–337, New York, NY, USA, 1992. ACM Press.

[68] Christian Heath and Paul Luff. Collaborative Activity and Technological Design: Task Coordination in London Underground Control Rooms. In Liam Bannon, Mike Robinson, and Kjeld Schmidt, editors, *Proceedings of the Second European Conference on Computer-Supported Cooperative Work - ECSCW 91*, pages 65–80. Kluwer Academic Publishers, 1989.

[69] Lars Erik Holmquist, Jennica Falk, and Joakim Wigström. Supporting group collaboration with interpersonal awareness devices. *Personal Technologies*, 3(1–2):13–21, March 1999.

[70] Jason I. Hong and James A. Landay. An architecture for privacy-sensitive ubiquitous computing. In *MobiSys '04: Proceedings of the 2nd international conference on Mobile systems, applications, and services*, pages 177–189, New York, NY, USA, 2004. ACM Press.

[71] Scott E. Hudson and Ian Smith. Techniques for addressing fundamental privacy and disruption tradeoffs in awareness support systems. In *CSCW '96: Proceedings of the 1996 ACM conference on Computer supported cooperative work*, pages 248–257, New York, NY, USA, 1996. ACM Press.

[72] Giovanni Iachello and Gregory D. Abowd. Privacy and proportionality: adapting legal evaluation techniques to inform design in ubiquitous computing. In *CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 91–100, New York, NY, USA, 2005. ACM Press.

[73] E. Isaacs, S. Whittaker, D. Frohlich, and B. O'Conaill. Informal communication re-examined: New functions for video in supporting opportunistic encounters. In Kathleen E. Finn, Abigail J. Sellen, and Sylvia B. Wilbur, editors, *Video-Mediated Communication*. Lawrence Erlbaum, 1997.

[74] Ellen Isaacs, Alan Walendowski, and Dipti Ranganthan. Hubbub: a sound-enhanced mobile instant messenger that supports awareness and opportunistic interactions. In *CHI '02: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 179–186. ACM Press, 2002.

[75] L. Kagal, T. Finin, and A. Joshi. Trust-based security in pervasive computing environments. *Computer*, 34:154–157, 2001.

[76] Kjeld Schmidt. The Problem with 'Awareness': Introductory Remarks on 'Awareness in CSCW'. *Computer Supported Cooperative Work (CSCW)*, 11(3–4):285–298, September 2002.

[77] Douwe Korff. EC study on implementation of data protection directive. Comparative summary of national laws. Online, `http://www.eu.int/comm/justice_home/fsj/privacy/docs/lawreport/consultation/univessex-comparativestudy_en.pdf`, september 2002.

[78] Marc Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In Gregory D. Abowd, Barry Brumitt, and Steven A. Shafer, editors, *Proceedings of the Third International Conference on Ubiquitous Computing (UbiComp 2001)*, number 2201 in Lecture Notes in Computer Science, pages 273–291, Atlanta, USA, 2001. Springer-Verlag.

[79] Mark R Leary and Robin M Kowalski. Impression Management: A literature review and a two-component model. *Psychological bulletin*, 107(1), 1990.

[80] Scott Lederer, Jennifer Mankoff, and Anind K. Dey. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03: CHI '03 extended abstracts on Human factors in computing systems*, pages 724–725, New York, NY, USA, 2003. ACM Press.

[81] Alison Lee, Andreas Girgensohn, and Kevin Schlueter. Nynex portholes: initial user reactions and redesign implications. In *GROUP '97: Proceedings of the international ACM SIGGROUP conference on Supporting group work*, pages 385–394, New York, NY, USA, 1997. ACM Press.

[82] Christian Licoppe and Jean-Philippe Heurtin. France: preserving the image. In J. Katz and M. Aakhus, editors, *Perpetual Contact: Mobile communication, private talk, public performance*, pages 94–109. Cambridge University Press, Cambridge, MA, 2002.

[83] Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. *Journal of Cryptology*, 15:177–206, 2002.

[84] R. Ling. *The Mobile Connection: The Cell Phones Impact on Society.* Morgan Kaufmann, 2004.

[85] Enid Mante. The Netherlands and the USA compared. In J. Katz and M. Aakhus, editors, *Perpetual Contact: Mobile communication, private talk, public performance*, pages 110–125. Cambridge University Press, Cambridge, MA, 2002.

[86] Marilyn M. Mantei, Ronald M. Baecker, Abigail J. Sellen, William A. S. Buxton, Thomas Milligan, and Barry Wellman. Experiences in the use of a media space. In *CHI '91: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 203–208, New York, NY, USA, 1991. ACM Press.

[87] Marilyn M. Mantei, Ronald M. Baecker, Abigail J. Sellen, William A. S. Buxton, Thomas Milligan, and Barry Wellman. Experiences in the use of a media space. In *CHI '91: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 203–208, New York, NY, USA, 1991. ACM Press.

[88] Stephen T. Margulis. On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, 59(2):411–429, 2003.

[89] Matthew Chalmers. Historical view of context. *Computer Supported Cooperative Work (CSCW)*, V13:223–247, 2004.

[90] Oleksiy Mazhelis, Seppo Puuronen, and Mika Raento. Evaluating classifiers for mobile-masquerader detection. In *Proceedings of the Security and Privacy in Dynamic Environments (SEC2006), 21st IFIP TC-11 International Information Security Conference*, pages 271–283, Berlin, Heidelberg, 2006. Springer Verlag.

[91] Joseph F. McCarthy and Eric S. Meidel. ACTIVEMAP: A Visualization Tool for Location Awareness to Support Informal Interactions. In *Handheld and Ubiquitous Computing: First International Symposium, HUC'99, Karlsruhe, Germany, September 1999. Proceedings*, volume 1707 of *Lecture Notes in Computer Science*, pages 158–170, Berlin / Heidelberg, 1999. Springer-Verlag.

[92] Judi Beinstein Miller and Amy Stubblefield. Parental disclosure from the perspective of late adolescent. *Journal of Adolescence*, 16:439–455, December 1993.

[93] Thomas P. Moran and R. J. Anderson. The workaday world as a paradigm for CSCW design. In *CSCW '90: Proceedings of the 1990 ACM conference on Computer-supported cooperative work*, pages 381–393, New York, NY, USA, 1990. ACM Press.

[94] Bonnie A. Nardi, Steve Whittaker, and Erin Bradner. Interaction and outeraction: instant messaging in action. In *CSCW '00: Proceedings of the 2000 ACM conference on Computer supported cooperative work*, pages 79–88, New York, NY, USA, 2000. ACM Press.

[95] OECD. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. OECD, 2002.

[96] Gary M. Olson and Judith S. Olson. Distance Matters. *Human-Computer Interaction*, 15(2&3):139–178, 2000.

[97] Robert J. Orr and Gregory D. Abowd. The smart floor: a mechanism for natural user identification and tracking. In *CHI '00: CHI '00 extended abstracts on Human factors in computing systems*, pages 275–276, New York, NY, USA, 2000. ACM Press.

[98] Antti Oulasvirta. *Studies of working memory in interrupted human-computer interaction*. PhD thesis, University of Helsinki, 2006.

[99] Antti Oulasvirta, Renaud Petit, Mika Raento, and Sauli Tiitta. On how users interpret and act upon mobile awareness cues. *Human-Computer Interaction*, 2006. in press.

[100] Antti Oulasvirta, Mika Raento, and Sauli Tiitta. 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*, pages 167–174. ACM, 2005.

[101] Leysia Palen. Social, individual and technological issues for groupware calendar systems. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 17–24. ACM Press, 1999.

[102] Leysia Palen and Paul Dourish. Unpacking "privacy" for a networked world. In *CHI '03: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 129–136, New York, NY, USA, 2003. ACM Press.

[103] Elin Rønby Pedersen and Tomas Sokoler. Aroma: abstract representation of presence supporting mutual awareness. In *CHI '97: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 51–58, New York, NY, USA, 1997. ACM Press.

[104] Sandra Petronio. *Boundaries of Privacy, Dialectics of Disclosure*. State University of New York Press, 2002.

[105] W. Prinz. NESSIE: An awareness environment for cooperative settings. In *Proceedings of the Sixth European Conference on Computer Supported Cooperative Work — ECSCW99*, pages 391–410. Kluwer Academic Publishers, 1999.

[106] Jukka-Pekka Puro. Finland: a mobile culture. In J. Katz and M. Aakhus, editors, *Perpetual Contact: Mobile communication, private talk, public performance*, pages 19–29. Cambridge University Press, Cambridge, MA, 2002.

[107] Mika Raento and Antti Oulasvirta. Privacy management for social awareness applications. In *Proceedings of the workshop on Context Awareness for Proactive Systems, CAPS 2005*, pages 105–114. Helsinki University Press, 2005.

[108] Anand Ranganathan, Roy H. Campbell, Arathi Ravi, and Anupama Mahajan. Conchat: A context-aware chat program. *IEEE*, 1(3):51–57, 2002.

[109] Yvonne Rogers. Moving on from Weiser's Vision of Calm Computing: engaging UbiComp experiences. In Paul Dourish and Adrian Friday, editors, *UbiComp 2006: Ubiquitous Computing: 8th International Conference, UbiComp 2006 Orange County, CA, USA, September 17-21, 2006 Proceedings*, number 4206 in Lecture Notes in Computer Science, pages 404–421. Springer-Verlag, 2006.

[110] Antti Salovaara, Antti Oulasvirta, and Giulio Jacucci. "The panoption": a method for observing inter-group interactions. A position paper presented in CHI'06 workshop on Reality testing: HCI challenges in non-traditional environments, available online at `http://www.cs.indiana.edu/surg/CHI2006/RealityTesting/RealityTesting_Salovaara-et-al.pdf`, 2006.

[111] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman. Role-based access control models. *Computer*, 29:38–47, February 1996.

[112] Emanuel A. Schegloff. Notes on a conversational practice: Formulating place. In David Sudnow, editor, *Studies in social interaction*, pages 75–119, New York, USA, 1972. The Free Press.

[113] Albrecht Schmidt, Michael Beigl, and Hans-W. Gellersen. There is more to context than location. *Computers and Graphics*, 23(6):893–901, 1999.

[114] Jean-Marc Seigneur and Christian Damsgaard Jensen. Trust enhanced ubiquitous payment without too much privacy loss. In *SAC '04: Proceedings of the 2004 ACM symposium on Applied computing*, pages 1593–1599, New York, NY, USA, 2004. ACM Press.

[115] Chia Shen, Katherine Everitt, and Kathleen Ryall. UbiTable: Impromptu Face-to-Face Collaboration on Horizontal Interactive Surfaces. In Anind K. Dey, Albrecht Schmidt, and Joseph F. McCarthy, editors, *UbiComp 2003: Ubiquitous Computing*, volume 2864 of *Lecture Notes in Computer Science*, pages 281–288, Berlin / Heidelberg, 2003. Springer.

[116] Leonard Sloane. Orwellian Dream Come True: A Badge That Pinpoints You. *The New York Times*, September 12th 1992.

[117] Ian Smith and Scott E. Hudson. Low disturbance audio for awareness and privacy in media space applications. In *MULTIMEDIA '95: Proceedings of the third ACM international conference on Multimedia*, pages 91–97, New York, NY, USA, 1995. ACM Press.

[118] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*, pages 38–47. ACM Press, 2001.

[119] Michael Spreitzer and Marvin Theimer. Scalable, secure, mobile computing with location information. *Commun. ACM*, 36(7):27, 1993.

[120] Mike Spreitzer and Marvin Theimer. Providing location information in a ubiquitous computing environment (panel session). In *SOSP '93: Proceedings of the fourteenth ACM symposium on Operating systems principles*, pages 270–283, New York, NY, USA, 1993. ACM Press.

[121] Latanya Sweeney. k-anonymity: a model for protecting privacy. *Int. J. Uncertain. Fuzziness Knowl.-Based Syst.*, 10(5):557–570, 2002.

[122] John C. Tang, Ellen A. Isaacs, and Monica Rua. Supporting distributed groups with a montage of lightweight interactions. In *CSCW '94: Proceedings of the 1994 ACM conference on Computer supported cooperative work*, pages 23–34, New York, NY, USA, 1994. ACM Press.

[123] John C. Tang, Nicole Yankelovich, James Begole, Max Van Kleek, Francis Li, and Janak Bhalodia. ConNexus to awarenex: extending awareness to mobile users. In *CHI '01: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 221–228, New York, NY, USA, 2001. ACM Press.

[124] The European Commission. 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. *Official Journal of the European Communities*, (L 281):31–50, 1995.

[125] Konrad Tollmar, Ovidiu Sandor, and Anna Schomer. Supporting social awareness @ work design and experience. In *CSCW '96: Proceedings of the 1996 ACM conference on Computer supported cooperative work*, pages 298–307, New York, NY, USA, 1996. ACM Press.

[126] Lea Viljanen. Towards an Ontology of Trust. In Sokratis Katsikas, Javier López, and Günther Pernul, editors, *Trust, Privacy and Security in Digital Business. Second International Conference, TrustBus 2005, Copenhagen, Denmark, August 22-26, 2005. Proceedings*, pages 175–184, Berlin Heidelberg, 2005. Springer-Verlag.

[127] Jeffrey R. Vittengl and Craig S. Holt. Getting acquainted: The relationship of self-disclosure and social attraction to positive affect. *Journal of Social and Personal Relationships*, 17(1):53–66, 2002.

[128] W3C. Platform for Privacy Preferences (P3P) Project, 2005. Online, `http://www.w3.org/P3P/`, referenced Jun 2006.

[129] Joseph B. Walther. Interpersonal Effects in Computer-Mediated Interaction: A Relational Perspective. *Communication Research*, 19(1), 1992.

[130] Roy Want, Andy Hopper, Veronica Falcao, and Jonathan Gibbons. The active badge location system. *ACM Transactions on Information Systems*, 10(1):91–102, 1992.

[131] Roy Want, Bill N. Schilit, Norman I. Adams, Rich Gold, Karin Petersen, David Goldberg, John R. Ellis, and Mark Weiser. An overview of the PARCTAB ubiquitous computing experiment. *IEEE Personal Communications*, 2:28–43, December 1995.

[132] Warren and Brandeis. The Right to Privacy. *Harvard Law Review*, IV, December 1890.

[133] Mark Weiser. The Computer for the Twenty-First Century. *Scientific American*, 265:94–104, September 1991.

[134] Melora Zaner, EK Chung, and Tammy Savage. 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, 2003. Online, `http://berkeley.intel-research.net/paulos/lab/ubicomp03/Workshop/index.htm`, referenced Jun 2006.

xxx